EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

ECB Video Surveillance Policy

15 September 2020

Table of contents

ECB Video Surveillance Policy

1. Purpose and Scope of the ECB's Video-Surveillance Policy

For the safety and security of its staff, visitors, buildings, assets and information, the ECB is operating a video surveillance system on its sites in Frankfurt am Main, Germany. The scope of this policy is restricted to the video-surveillance system operated by the ECB only and on ECB sites located in Frankfurt am Main, Germany, where the ECB is the controller of the data.

The ECB video-surveillance policy does not apply to the recordings or broadcasting of events for the purposes of the press conference and public communication of the Executive Board, the Governing Council, or the Single Supervisory Mechanism.

This video-surveillance policy, along with its attachments, (i) describes the video surveillance system of the ECB and the safeguards the ECB has in place to protect the personal data of those viewed by the cameras; (ii) tells you how you can get hold of more detailed information; (iii) explains how you can exercise your rights as a data subject.

2. How do 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

This document consists in version 2.0 of the ECB video-surveillance policy and replaces version 1.0 from 2012. This version extends its scope to the new ECB building and organizational changes, and has been reviewed to incorporate the requirements from Regulation (EU) 2018/1725 and the recommendations set forth in the EDPS Video-Surveillance Guidelines.

2.2 Compliance status

The ECB processes video-surveillance images in accordance with ECB Decision 2007/1, repealed by ECB Decision (EU) 2020/655 that enters into force on 1 November 2020, and Regulation (EU) No 2018/1725 on the protection of personal data by the Community institutions and bodies and takes into account the EDPS Video-Surveillance Guidelines.

2.3 Self-audit

The ECB video-surveillance system was subject to an assessment by the ECB Data Protection Officer (hereinafter "ECB DPO") in order to align compliance of the processing of video-surveillance with the EDPS Video-Surveillance Guidelines.

The current video-surveillance system merges the video-surveillance policy previously approved by the ECB Executive Board (on 31 January 2012), the changes adopted for the new building constructed (2015), the changes in organizational needs (that required two prior checks from the EDPS and implementation of consequent mitigation measures) and the new Regulation (EU) 2018/1725.

Within two years after the adoption of this video-surveillance policy by the ECB Executive Board, the ECB video-surveillance policy will be externally audited based on the EDPS recommendations. The External Audit will have mainly 2 objectives:

- To verify the ECB video-surveillance policy adequacy: to verify that there is a documented and up-to-date video-surveillance policy in place and that this policy complies with Regulation (EU) 2018/1725 and EDPS Video-Surveillance Guidelines; and,
- To verify the policy compliance: to check that the ECB is in fact operating in accordance with its video-surveillance policy.

2.4 Notification of compliance status to the EDPS

The ECB has submitted to the EDPS two Prior Checks and this video-surveillance policy takes into account the adoption of the mitigation measures proposed by the EDPS. The prior checks submitted by the ECB were:

- **EDPS Prior Checking Opinion Ref.** C 2015-0938 on the use of thermal imaging cameras and the auto-track functionality of pan-tilt cameras – ECB; and,
- **EDPS Prior Checking Opinion Ref.** C 2016-0695 regarding automated vehicle license plate recognition at the European Central Bank.

Both EDPS Prior Checking Opinions are published on the EDPS site and are publicly available through the links provided above, and are available in three EU Official Languages: French, English and German.

This version of the video-surveillance policy was reviewed the ECB DPO and the ECB DPO has notified the EDPS of this policy together with a compliance status.

2.5 Contacts with the relevant data protection authority in the Member State

The competent data protection authorities of the German State of Hesse were made aware of the video surveillance policy regarding the Main Building and the city locations (as defined under section 3). In particular, the policy was discussed with the Hessian Officer for Data Protection and Freedom of Information.

The recommendations were taken into account by the ECB.

2.6 Director's decision and consultation

The decision to implement the current video surveillance system, and to put in place the relevant data protection safeguards as described in this video surveillance policy, was taken by the Executive Board after consultation with:

- the ECB's Security and Safety Division (DG-CS/A/SET);
- the ECB's Data Protection Officer (ECB DPO) and;
- the ECB's Staff Committee and the recognised trade union IPSO.

During the consultation process, the ECB demonstrated and documented the need for a video surveillance system for the scope mentioned in this policy, discussed possible alternatives and concluded that the installation of a video surveillance system continues to be necessary and proportionate for the ECB security, safety and access control purposes.

2.7 Transparency

The ECB Video-Surveillance policy is available on the ECB's Internet site and on the ECB's Intranet site, under Security Page.

Two versions of the video surveillance policy are available: a version for restricted internal use and this public version for the general public.

The public version of the Video-Surveillance policy may contain summarized information with respect to particular topics or annexes. Information is only omitted from the public version when the preservation of confidentiality is absolutely necessary for compelling - security reasons and to preserve the confidentiality of business sensitive information.

2.8 Periodic reviews

A periodic data protection review will be undertaken by the ECB Security and Safety Division with the ECB DPO every two years, the first by 2022, re-assessing that:

- there continues to be a need for the video-surveillance system;
- the video-surveillance system continues to serve its declared purpose, and that;
- it remains the adequate system for its intended purpose.

The periodic reviews will also cover all other issues noted in the former reviews, in particular, whether the ECB's Video-Surveillance policy continues to comply with Regulation (EU) 2018/1725 and the EDPS video-surveillance Guidelines (adequacy audit), and whether it is followed in practice (compliance audit).

2.9 Privacy-friendly technological solutions

To protect privacy, the ECB has implemented the following privacy-friendly technological solutions:

- the operating units of the video surveillance system are configured and restricted to select only those cameras necessary to fulfil the dedicated operations;
- live video monitoring is secured by means of access control;
- the camera lens selection is geared towards the surveillance task, reducing the degree of personal recognition possibilities to the degree necessary;
- masking images (privacy function) helps eliminate the surveillance of areas irrelevant to the surveillance target. This is especially relevant for video dome cameras or pan/tilt cameras which could possibly be used to target neighbouring houses and major public areas around the ECB buildings premises. Masking technologies are in place to ensure privacy for standard situations (like windows and balconies on opposite side of the road or walkways on the opposite side of a road). Only in well-defined alarm situations which are event-triggered via technical devices, the masking function can exceptionally be deactivated automatically to perform the security function of the devices. The zoom factor is taken into account while defining the degree of masking;
- limitation of the view on public and or recreational areas, both internal and external to the ECB's premises;
- limitation of storage times in line with security requirements (see this policy Section 8);
- the access to the recorded data is password protected and is available only to the specific people designated by the ECB Security and Safety Division;

- strict management of operator's physical and logical rights regarding access to the video-surveillance System, and;
- the access to areas where the video-surveillance streaming are processed (Security guards rooms) is restricted to the designated Security personnel; the video streams for the video-surveillance systems are not visible from the outside.

3. What areas are under surveillance?

The ECB premises are located as follows: the main premises are located in the city district of Frankfurt am Main called "Ostend" and three other office buildings are located in the city centre of Frankfurt am Main. The video surveillance system covers these buildings and premises. It consists of more than 1600 cameras among which some pan/tilt/zoom camera units are used for aerial surveillance. The amount of cameras is limited to the number necessary to achieve the purpose of the video-surveillance system.

Cameras are located at various points of ECB premises including: main entries, exits and emergency exit points, entrance to secured areas, lobbies, corridors, parking facilities, and around the buildings to protect the outer perimeters. There are also technical cameras installed to perform empty space recognition.

The video-surveillance system includes standard door intercom cameras. These images are transferred to local secretaries' desks in charge of organising access to the respective office area.

The monitoring of areas beyond the boundaries of the ECB's premises is kept to the absolute minimum necessary to meet the ECB's security needs and was discussed with the relevant German data protection authorities, the Hessian Officer for Data Protection and Freedom of Information(see this policy Section 2.5).[1] Based on a contract with the city of Frankfurt the following areas are under video surveillance on public grounds:

- three transition areas for vehicle access;
- public grounds on the immediate vicinity of the ECB buildings;
- two security installations within a privately run railroad line.

[1] In line with the *EDPB Guidelines 3/2019 on processing of personal data through video devices* adopted on 29 January 2020 there are cases "*where the surveillance of the property is not sufficient for an effective protection. In some individual cases it might be necessary to exceed the video surveillance to the immediate surroundings of the premises*".

The location of the cameras has been carefully reviewed to ensure that they minimise the monitoring of areas that are not relevant for the intended purposes.

Cameras using thermal imaging technology, as well as the auto-track functionality of pan-tilt cameras, are integrated into the video-surveillance system. The operation of these cameras has been subject of a data privacy impact assessment and prior checked with the EDPS, as mentioned in this policy section 2.4.

There are no cameras monitoring any areas under heightened expectations of privacy such as offices and social facilities.

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

4.1 Summary description and detailed technical specifications for the system

The video surveillance system combines fixed, domes and pan/tilt/zoom cameras and live video monitoring takes place. It records digital images and is equipped with motion detection. It records any movement detected by the cameras in the areas under surveillance, indicated in this policy Section 3, as well as the corresponding time, date and location. All cameras activated within the system operate 24 hours a day, seven days a week. The resolution and image quality produced by the cameras in most cases allows identification of the movement of persons/vehicles in the cameras' area of coverage, allowing the prevention of any intrusion or incidents. Where no identification of individuals is necessary, the camera/object lens combination is chosen in a way that no recognisable features are captured. The potential use of pan/tilt/zoom cameras for the purposes of following externals is restricted to the immediate surroundings of the external perimeter.

The video-surveillance system uses license plate recognition system to allow the vehicle license plate recognition system for use within the access control system.

Permanent recordings take place and after the defined retention period are overwritten as indicated in chapter 8. The ECB is not using any non-digitally recorded footage.

The video-surveillance system may accept inbound alerts/messages from other systems (eg. intrusion detection system), and these alarm event recordings are blocked for the normal retention schedule, being later disposed manually. However the video-surveillance system is not connected to external systems, but it interconnects its video protection systems operating in the buildings listed in Section 3 of this policy.

The cameras in use do not record any sound.

In order to establish effective access management, all entrances to office areas with further restricted access are equipped with a video-based intercom station. Pictures are transmitted to the secretaries' desk or to the security control centre for technical areas if an intercom connection is established. These pictures are not recorded.

The following surveillance methods are not used

- interconnection of our system with other systems outside the ECB;
- covert surveillance;
- sound recording and "talking CCTV".

4.2 Purpose of the surveillance

The ECB operates its video surveillance system for the sole purpose of security, safety and access control. The video surveillance system helps to control accesses to ECB Premises and helps to ensure the safety, security and integrity of our buildings, ECB staff and visitors, as well as the security of property and information located or stored on the premises, as well as support investigations, either in the case of an administrative enquiry or for witnessing a security incident.

When necessary, it complements other physical security systems, such as access control systems, physical intrusion control systems and fire detection systems. It forms part of the measures to support the ECB broader security policies as established by the Executive Board on the security rules and helps prevent, deter, and if necessary, investigate unauthorized physical access, including unauthorized access to secure premises, protected rooms, IT infrastructure or operational information. In addition, video surveillance helps prevent, detect and investigate theft of equipment or assets owned by the ECB, staff, contractors or visitors, as well as threats to the safety of visitors or personnel working on the ECB Premises (e.g. incidents of fire or physical assault).

4.3 Purpose limitation

The video-surveillance system is not used for any other purpose, for example, it is not used to monitor the work of staff members or contractors or to monitor attendance. Neither is the video-surveillance system used as an investigative tool or evidence, except for the purposes of investigating physical security incidents, such as thefts or unauthorized access, or if requested for cooperation with the competent authorities. It is only in exceptional circumstances that the images may be transferred to

the competent authorities, within the framework of a formal administrative inquiry, disciplinary proceedings or criminal investigation, either pro-actively or upon request, following consultation with the ECB DPO, on a case-by-case basis.

4.4 Ad hoc video use

Where there is a duly justified security need for *ad hoc* video protection, such operations are planned beforehand.

4.5 Webcams

The ECB does not use webcams for video-surveillance purposes.

4.6 No special categories of data collected

The ECB collects no special categories of data.

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

The legal basis of the processing operations which the use of ECB video-surveillance system entails is Article 5(1)(a) of Regulation (EU) 2018/1725 read in the light of recital 22. The processing operations are necessary for the management and functioning of the ECB, for the sole purpose of security, safety and access control (as described in Section 4.2 above). Therefore, the ECB has a lawful ground for the use of a video-surveillance system. This policy, in turn, forms part of the broader security policies adopted by the ECB.

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

6.1 In-house security staff and outsourced security providers

Access to the recorded and live video is limited to a small number of clearly identifiable individuals on a need-to-know basis (as specified in section 6.2).

Live monitoring is additionally accessible to the security guards on duty, working at defined locations with qualified staff. These security guards work for an external security provider. Dedicated contractual obligations ensure the enforcement of rules defined in this video surveillance policy.

The maintenance, remediation and administration of the video surveillance system is performed by an external company, in a defined and controlled environment, that might have access to the system, for the necessary time to perform system' maintenance, trouble-shooting and administration activities. Dedicated contractual obligations ensure the enforcement of rules defined in this video surveillance policy.

6.2 Access rights

The ECB specifies the purpose and extent of access rights to the video-surveillance system. In particular, it limits who has the right to view the footage in real-time; view the recorded footage; access to the technical infrastructure, perform maintenance or programming activities on the system, copy, download, delete or alter any footage.

The data from the video-surveillance system (recorded and live) is only accessed by personnel tasked by the ECB Security and Safety Division (ECB staff and contracted personnel).

External providers' tasked with the maintenance and administration of the video-surveillance system, might have access to the system, for the necessary time to perform system' maintenance, remediation and administration activities.

6.3 Data protection training

All personnel with access rights, including external subcontracted security guards and system maintenance and administrators, are given initial data protection training.

6.4 Confidentiality undertakings

Each staff member also signs a confidentiality undertaking; such undertaking has also to be signed by external staff employed by external contractors.

6.5 Transfers and disclosures

All transfers and disclosures outside the ECB Security and Safety Division are documented and subject to an assessment of the lawfulness and the necessity of such transfer and the compatibility of the purposes of the transfer with the initial security, safety and access control purpose of the processing. The ECB DPO is consulted in each case. A register of the retention and transfer is kept under the responsibility of the ECB Security and Safety Division. The registers of the retention and transfers may be consulted by the ECB DPO and audit services.

The following principles apply for any transfer or disclosure of data obtained through the video-surveillance system:

I. No access is given to the ECB management (except Security Management) or to the Directorate General Human Resources personnel;

II. Local law enforcement authorities may be given access if needed to investigate or prosecute criminal offenses;

III. Under exceptional circumstances, access may also be given to:

- the competent authorities either pro-actively or upon request, in case of a security incident, following consultation with the ECB DPO, on a case-by-case basis;
- the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF;
- any other recognised competent and/or judicial authorities in the framework of, or if needed, to investigate or prosecute criminal offenses;
- those carrying out a formal internal ECB Investigation or disciplinary procedure, in the context of a formal administrative inquiry or disciplinary procedure conducted within the ECB under the rules set forth in the ECB statutory framework.

IV. 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, the following technical and organisational measures have been put in place:

- The video-surveillance system units are mounted in locked cabinets with restricted access of technical staff members of the ECB and named external staff of the ECB Security and Safety Division service providers.
- Secure premises, protected by physical security measures, host the servers storing the images recorded; network firewalls or physical segregation protect the logic perimeter of the IT infrastructure, and the main computer systems holding the data are security hardened.

- Retrieval of stored video images is only possible within a dedicated internal network. 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 external staff 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 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 section 6.2. of this policy.
- The ECB DPO will be consulted prior to the acquisition or installation of any new video-surveillance system, or any significant changes to the existing one.

The ECB Security and Safety Division "*IT Security Policy"* has been drawn up in accordance with the Section 9 of the EDPS video-surveillance Guidelines.

8. How long do we keep the data?

The images covering the public or semi-public areas are stored for a maximum period of 21 days and then overwritten.

If any image needs to be stored longer as part of a wider investigation (e.g. in the case of an administrative inquiry) or for serving as evidence regarding a security incident, the relevant footage is quarantined and retained for as long as necessary for the specific investigation in line with the applicable retention periods. Their retention is documented and the need for retention is to be reviewed periodically.

9. How do we provide information to the public?

9.1 Multi-layered approach

The ECB provides information to the public about its video surveillance practices 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 close to all areas under surveillance and all entry points, including car park entrances, in order to alert the public of the site surveillance and provide essential information about the data processing . The ECB's on-the-spot data protection notice is attached as appendix.
- the posting of this public version of the video surveillance policy on the ECB's intranet and internet sites, for those seeking further information about the video-surveillance practices of the ECB.

Print-outs of this video-surveillance policy are also available from the ECB Security and Safety Division upon request. These include a phone number and an e-mail address for any further enquiries.

Notices are affixed adjacent to the following monitored areas among others:

Near the main entrances, the lifts in the car park and at the entrances to the car parks, both in English and German Languages, in all ECB Buildings that are part of the scope of this video-surveillance policy.

9.2 Specific individual notice

In addition, individuals are also notified that they were identified on camera (for example, by security staff during a security investigation), if 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 file is kept beyond standard retention period;
- the recording has been disclosed outside the ECB Security and Safety Division; or
- the identity of the individual is disclosed to anyone outside the ECB Security and Safety Division.

Notifications may sometimes be delayed temporarily, for example, if it is necessary for the prevention, investigation, detection and prosecution of criminal offences. Other exceptions under Article 25 of the Regulation (EU) No 2018/1725 may also apply.

The ECB DPO is consulted in all such cases to ensure that the individual's rights are respected. In addition, the ECB DPO is notified of any decision to delay the above notification.

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

Members of the public and EBC Staff Members have the right to access the personal data the ECB holds about them and to correct and complete such data. Any request for access, rectification, blocking and/or erasing personal data should be directed to the ECB Head of the ECB Security and Safety Division, mb-service_center@ecb.europa.eu.

In the case of a request for viewing images, ECB Staff Members are entitled to seek the assistance of a Staff Representative, in line with ECB rules. Such assistance shall be provided taking into account the Data Protection Principles, in line with the relevant provisions of Regulation (EU) 2018/1725, and the ECB Legal Framework.

Regarding any other question relating to the processing of personal data members of the public can contact the ECB DPO dpo@ecb.europa.eu;

According to Article 14(3) Regulation (EU) No 2018/1725, the ECB Security and Safety Division responds to data subjects' access request in substance within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The ECB Security and Safety Division inform the requestor of any such extension within one month of receipt of the request, together with the reasons for the delay.

The ECB Security and Safety Division endeavours to respond earlier, especially if the applicant establishes the urgency of the request.

If specifically requested, a viewing of the images may be arranged. In case of such a request, the applicant must establish their identity beyond all doubt (e.g. bring identity cards when attending the viewing) and also specify the date, time, location and circumstances when they were caught on cameras. They must also provide a recent photograph that will allow security staff to identify them from the images reviewed. In case the person was indeed recorded he/she may obtain a copy of the recorded images either on a DVD or any other media.

The ECB provides the requested information to applicants in accordance with the New Regulation (EU) 2018/1725 under article 14(5), therefore the access to information shall be given free of charge; however, as stated in the same article, the ECB may refuse to provide such information where requests are manifestly unfounded or excessive, in particular because of their repetitive character.

A request for access may be refused if an exemption under Article 25(1) of the Regulation (EU) No 2018/1725 applies in a specific case. For example, following a case-by-case evaluation, the ECB may have to conclude that restricting access may be necessary in order to safeguard the investigation of a

sufficiently serious disciplinary process or criminal offence. A restriction may also be necessary to protect the rights and freedoms of others, for example, when other people are also identifiable on the images, and it is not possible to acquire their consent to the disclosure of their personal data or to edit images in order to remedy the lack of consent.

11. Right of recourse

Every individual has the right of recourse to the European Data Protection Supervisor (edps@edps.europa.eu) if they consider that their rights under the Regulation (EU) 2018/1725 have been infringed as a result of the processing of their personal data by the ECB. However, before doing so, we recommend that individuals first try to obtain recourse by contacting:

- the Head of ECB Security and Safety Division (see above for contact details), and/or
- the ECB Data Protection Officer (see above for contact details).

Staff members may also request a review of their appointing authority under the ECB's internal recourse procedures.

Annex: On-the-spot-notice

In line with the EDPS Guidelines the notice includes the following information:

- a pictogram (according to DIN/ISO 33450),
- contact information on how to address the "controller" and the data protection officer,
- statement of the purpose of the surveillance,
- statement that the images are recorded,
- statement on data subject rights

The signs are placed at such locations and are large enough that data subjects can recognise them before entering the monitored zone and can read them without difficulty. The signs are mounted both in English and German language.