ON-LINE DATA PROTECTION NOTICE OF VIDEO SURVEILLANCE AT THE OFFICE BUILDINGS OF THE EUROPEAN CENTRAL BANK

Table of Contents:

1 Purpose and scope of the ECB`s video surveillance policy

This video-surveillance policy details the video surveillance system of the ECB and the safeguards that the institution has in place to protect the personal data and privacy, as well as other fundamental rights and the legitimate interests of those entering into surveillance areas at the ECB premises in Frankfurt am Main.

This video-surveillance policy is based on the "Video-Surveillance Guidelines"[1] adopted by the European Data Protection Supervisor (EDPS) on 17 March 2010 (hereinafter referred to as the "**Guidelines**").

The ECB processes the images in accordance with both the Guidelines and Regulation (EC) No 45/ 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 Community institutions and bodies and of the free movement of such data (hereinafter referred to as the "**Regulation**").

This policy is part of the broader ECB general physical security framework. Physical security refers to all measures intended to deter, detect, delay, defeat or diminish the impact of threats against the ECB, the health and safety of the members of its decision-making bodies, all staff and other persons contracted to work for or at the ECB, as well as business and non-business visitors (all staff and other persons), the intangibility of its real assets, its continued ability to perform its business functions, and the integrity, intangibility, accessibility and usability of its premises.

This public version:

- provides you with basic information about the system;
- tells you how you can get hold of more detailed information;
- explains how you can exercise your rights as a data subject.

2 Which areas are under surveillance?

The ECB is currently renting three office buildings in the city centre of Frankfurt am Main and one external technical plant including an office area. The video surveillance system covers these four buildings. It consists of more than **600 cameras**. Out of this total amount 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 system.

The system includes standard door cameras. These images are transferred to **local secretaries' desks** organising the access to the respective office area.

There are no cameras monitoring any areas under heightened expectations of privacy such as offices and social facilities (see Guidelines, Section 6.8).

[1] The Guidelines are available on the EDPS website at http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Guidelines.

Camera locations have been carefully determined to minimise the monitoring of areas without relevance for the intended purposes of the video surveillance system (see Section 6.1 of the Guidelines).

The amounts of cameras reflect the complex architectural design of the locations. The vast majority of cameras are only activated during late evenings and weekends.

Each building contains a separate video crossbar system. Video is being displayed in **security control centres**. During out-of-business hours video is being transferred to the main security control centre located in the headquarter building. The ECB partly relies on third party infrastructure, components and auxiliaries. Clear boundaries to relevant external parties (landlords) were defined and quality of service is constantly monitored.

In addition to the main control centres additional **security check posts** are installed. The amount and quality of the installations are dependent on the architecture of the building and the criticality of the corresponding area to be supervised and protected.

The monitoring of areas beyond the boundary of the ECB Premises on the territory of Germany is kept to the absolute minimum that is necessary to meet the ECB`s security needs, as recommended in Section 6.5 of the Guidelines and has been discussed with the relevant German data protection authorities.

3 What personal information does the ECB collect and for what purpose?

3.1 Summary description and technical specifications for the system

The video surveillance system combines live video monitoring and video recording. All cameras activated within the system operate 24 hours a day, seven days a week; a small number, however, are only activated through a sensor alarm as described below.

The resolution and image quality produced by the cameras varies from location to location, subject to requirements. Where identification of individuals is not necessary, the camera/object lens combination is chosen in such a way that no recognisable features are captured.

As regards surveillance within the **boundary including driveways to the parking area** of the premises, a permanent recording takes place. The video surveillance through fixed camera units covers the façade of the office buildings, the corresponding walkway and – with the Eurotower building – gives additional protection to the perimeter system, namely the bollards and road blockers. Some video domes and pan/tilt/zoom cameras are used for live monitoring at the security control centre and may be recorded via a manual trigger within the alarm management system although the exact reason for the recording has to be stated for auditing purposes. Following the recommendation of the DATA PROTECTION OFFICER and the data protection authority of the state of Hesse a privacy function is implemented.

Entering the premises and proceeding to the office area, fixed camera units are live monitored and recorded triggered by the access control system.

Other business areas are live monitored on a case-by-case decision. Video is displayed in the corresponding security control centre or security desk dedicated to the respective area. A video recording may be manually triggered, corresponding to an audit trail. During out-of-business hours alarms will be displayed in the security control centre and a video recording of the alarm situation takes place together with time, date and location.

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 if an intercom connection is established. There is no standard video recording of these pictures.

Areas within the **highest security zone** are covered by fixed camera installations. Based on detailed operational requirements defined by the responsible business area, event triggered live monitoring and permanent video recording takes place. Storage intervals highly differ from the standard retrieval period. The intervals are up to 5 years for well-defined areas. All staff working within these areas is informed about this technical configuration.

The following surveillance methods are not employed:
- high-tech or intelligent video surveillance technology (Section 6.9 of the Guidelines)
- interconnection of our system with other systems (Section 6.10 of the Guidelines)
- covert surveillance (Section 6.11 of the Guidelines)
- sound recording and "talking CCTV" (Section 6.12 of the Guidelines).

3.2 Purpose of the surveillance

The video surveillance system forms an integral part of a range of technical, operational and organisational measures taken in accordance with the broader security policy for the ECB Premises as outlined under Section 1.

The ECB operates a video surveillance system for the sole purpose of ensuring the security and access control of the premises. The video surveillance system helps to control access to the ECB Premises and secured areas within the EC B Premises and helps to ensure the safety, security and integrity of the installations, the safety of the ECB staff and visitors, as well as the security of property and information located or stored on the site. It supplements other technical security systems, such as access control systems, intruder alarms and fire detectors. It helps to prevent, deter, detect and, if necessary, investigate instances of unauthorised access, including unauthorised access to secure premises and protected areas, the IT infrastructure or operational information. In addition, video surveillance helps to prevent, detect and investigate instances of theft of equipment or assets owned by the ECB and its contractors, staff or site visitors, as well as threats to the safety of visitors or personnel working on the ECB Premises (such as incidents of fire or physical assault).

3.3 Purpose limitation

The system is not used for any other purpose, such as to monitor the attendance or work of staff members or contractors. Neither is it used as an investigative tool, except in the event of a physical security incident, such as a theft or case of unauthorised access and, then, it is only

under the circumstances described in Section 5.5 below that images may be transferred or disclosed to investigatory bodies, within the framework of a formal administrative inquiry, disciplinary proceedings or a criminal investigation (see Sections 5.7, 5.8 and 10.3 of the Guidelines).

3.4 Ad hoc surveillance operations

At this time, the ECB does not foresee any ad hoc surveillance (see Guidelines, Section 3.6).

3.5 Webcams

No webcams are installed for video surveillance purposes.

3.6 Special categories of data

The ECB collects no special categories of data (Section 6.7 of the Guidelines).

4 What are the lawful grounds and legal basis for video surveillance?

The use of video surveillance equipment is necessary to ensure the proper management and functioning of the ECB Premises (i.e. for safety, security and access control purposes, as described in Section 3.2 above). Therefore, the ECB has lawful grounds to carry out the video surveillance (see Section 5.2 of the Guidelines). A more detailed and specific legal basis for the video surveillance is provided in the video surveillance policy which is adopted by the Executive Board. This policy, in turn, forms part of the broader security policies adopted by the ECB.

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

5.1 In-house security staff and security guards deployed by an external contractor.

Digitally recorded footage is accessible only to a restricted number of named ECB staff only. Live footage is additionally accessible to security guards on duty working for an external security provider.

5.2 Access rights.

The ECB`s Information security policy for the video surveillance system (see Section 6 below) clearly specifies and documents

- who has access to the video surveillance footage;

– the technical architecture of the video surveillance system;
– what constitutes sufficient justification for access rights;
– which privileges are granted under the access.

In particular, the document specifies who has the right to:

– view live footage;
– view recorded footage;
– copy, download, erase or alter footage;
– perform maintenance or programming activities on the system.

5.3 Data protection training

All individuals with access rights to video recordings and, in addition, the security guards employed by the external contractor, were all made aware of the data protection issues within their scheduled training sessions. A specific dedicated data protection training takes place. Training is provided for each new member of staff and any security guard employed by the external contractor and periodic workshops on data protection compliance issues are carried out at least once every two years for all staff with access rights (see Section 8.2 of the Guidelines).

5.4 Confidentiality undertakings

Following their training, staff members will have to sign a confidentiality undertaking; such undertaking shall also be signed by any security staff employed by the external contractor.

5.5 Transfers and disclosures

Images recorded by the video surveillance system may be disclosed outside of the Security Division of the ECB subject to a rigorous assessment of the necessity of such a disclosure and its compatibility with the intended security-related purpose (see Section 10 of the Guidelines). All disclosures are documented accordingly. The DATA PROTECTION OFFICER of the ECB is consulted in each case.

Access rights are not granted to ECB management (with the exception of Security Division's management) or the Directorate General HR, Budget and Organisation.

Local police may be granted access if this is needed for investigations or prosecutions relating to criminal offences.

If follow-up is required in response to a physical security-related incident (such as a case of physical assault, theft or damage to ECB property), it may be necessary to make any relevant footage accessible to the European Anti-fraud Office ('OLAF') in the framework of an investigation carried out by OLAF, or to any other relevant body in the context of a formal administrative inquiry or disciplinary procedure being conducted within the ECB under the rules set forth in the ECB statutory framework, on the condition that such a transfer is deemed

proportionate. In addition, under exceptional circumstances, access may also be granted to the aforementioned bodies if follow-up is required in response to illegal activities not relating to a physical security incident, provided that it can be reasonably expected that the transfer may help with the investigation of a sufficiently serious disciplinary or criminal offence.

No requests for data mining shall be accommodated.

6 How does the ECB protect and safeguard the data?

In order to protect the integrity of the video surveillance system including the security of the personal data it captures, a number of technical and organisational measures haven been put in place. These are explained in detail in a processing-specific security policy ("Information security policy for video-surveillance").

Among others, the following measures are taken:

- The video system units are mounted in locked cabinets with restricted access of technical staff members of the ECB and named external staff of the engaged service providers.
- Retrieval of stored video images is only possible within a dedicated internal network. No remote connections are available.
- Administrative measures include the obligation of any staff deployed by an external contractor who has access to the system (including those maintaining the equipment and the systems) to be bound by the confidentiality undertakings incorporated in the contract between the ECB and the external contractor rendering security related services.
- All staff with access to the system are bound by individually signed confidentiality agreements regarding the processing of personal data.
- System users are granted access rights strictly only to those parts of the system which are indispensable for the fulfilment of their respective tasks.
- Only the system administrator, appointed by the “data controller” (Head of the Security Division) specifically for the purpose of administering access rights, is able to grant, alter or annul any access rights of any person. Any granting, alteration or annulment of access rights is made pursuant to the criteria established in the ECB`s Information security policy for the video surveillance system.
- The Information security policy for the video surveillance system contains an up-to-date list of all persons with access to the system and describes their access rights in detail.

7 How long does the ECB keep the data?

Images are stored for a maximum period of one month (with the exception of the highest security zone as described in Section 3.1 above). Thereafter, all images are deleted. 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 witnessing a security incident, such footage shall be quarantined and retained for as long as necessary beyond the aforementioned retention periods. Their retention is documented rigorously and the need for retention is to be reviewed periodically.

The system is also monitored live 24 hours a day by security guards in the security control room.

Video recording is not standard for all cameras. Based on the service performance of the video systems and transforming the outcome of the risk analysis process four types of video recording were technically elaborated and implemented within the video surveillance system. The general specifications are listed as follows:

Event based (automatic) recording of individual cameras in case of an alarm

- use case: cameras installed adjacent to transition zones of different security zones or monitoring sensitive areas in order to observe and/or record malevolent, accidental or as directed actions.

Event based manual recording of video monitor scenes

- use case: manually selected cameras in order to observe and/or record planned actions or to monitor certain scenarios, which may lead to a malevolent or accidental action.

Permanent recording of dedicated cameras

- use case: selected cameras in order to observe and/or record actions or monitor certain scenarios, which can not be permanently monitored by security staff or do not have the technical feature of being alarm-/event triggered and which may lead to a malevolent or accidental action.

Permanent recording of video monitor scenes

- use case: Dedicated alarm monitors in the Security Control Centres in order to record alarm triggered video pictures / -streams

8 How does the ECB provide information to the public?

8.1 Multi-layered approach.

The ECB provides information to the public about its video surveillance practices in an effective and comprehensive manner (see Section 11 of the Guidelines). To this end, a multi-layered approach is pursued, consisting of a combination of the following two methods:

– the displaying of on-the-spot notices to alert the public to the fact that the site is under surveillance and provide them with essential information about the processing of data;
– the posting of this public version of the video surveillance policy (in English and German) on the ECB`s internet site, for those seeking further information.

Printouts of the public version of the video surveillance policy are also available from the ECB`s security desks in the ECB Premises and from the Security Division on request, and include a phone number and an e-mail address for any further enquiries.

An on-the-spot notice is displayed adjacent to all areas under surveillance. Notices are also displayed near all entry points.

8.2 Specific individual notice

Individuals are notified that they have been 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 incriminates the individual;
– the file is intended to be kept beyond standard retention period;
– the recording has been disclosed outside the Security Division;
– the identity of the individual is disclosed to anyone outside the Security Division.

Notification may sometimes be delayed temporarily, for example, if a delay is necessary for the prevention, investigation or detection of criminal offences or the prosecution of individuals. Other exceptions under Article 20 of the Regulation may also apply.

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

9 How can members of the public verify, modify or delete their personal data?

Every individual has the right to access the personal data the ECB holds about them and to correct and complete such data. Any request to access, rectify, block and/or erase personal data should be directed to the controller, the Head of the Security Division (email: MB-Service_Center@ecb.europa.eu, tel.: 069-1344 7000). The ECB DATA PROTECTION OFFICER may also be contacted in relation to any other questions regarding the processing of personal data (dpo@ecb.europa.eu; tel.: 069-1344 0).

In principle, the Security Division will respond definitely to a request within 15 calendar days. If this is not possible, the applicant is informed of the next steps and the reasons for the delay within 15 calendar days. Even in the most complex of cases access must be granted, or a reasoned response providing the ultimate grounds for refusal, within three months of the request at the latest. The Security Division endeavours to respond earlier, especially if the applicant establishes the urgency of their request.

If specifically requested, a viewing of the images may be arranged or the applicant may obtain a copy of the recorded images either on a DVD or any other medium. In the case of such a request, the applicant must establish their identity beyond all doubt (e.g. they should present a form of identity at the viewing). In addition, they should give the date, time, location and circumstances of when they were captured on camera. They must also provide a recent photograph that will allow security staff to identify them from the recorded material.

At this time, the ECB does not charge applicants to view recordings or for digital copies of material. However, the ECB reserves the right to charge a reasonable fee to cover the costs of the provision of such services should demand increase.

A request for access may be refused if an exemption under Article 20(1) of the Regulation applies. For example, following an evaluation, the ECB may conclude that restricting access is necessary in order to safeguard the investigation of a sufficiently serious disciplinary or criminal offence. A restriction may also be necessary to protect the rights and freedoms of individuals, for example, if other people are identifiable on the images recording and it is not possible to secure

their consent to disclosure their personal data or to edit images in order to remedy this lack of consent.

10 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 have been infringed as a result of the processing of their personal data by the ECB. However, before doing so it is recommended that individuals first liaise with the relevant parties of the ECB. These are:

- the Head of the Security Division (see above for contact details),
- the ECB DATA PROTECTION OFFICER (see above for contact details).

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