EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB-PUBLIC

RECORD OF PROCESSING ACTIVITY

THE USE OF THERMAL IMAGING CAMERAS AND THE AUTO-TRACK FUNCTIONALITY OF PAN-TILT CAMERAS

1. Controller(s) of data processing activities

Controller: European Central Bank (ECB)

Organisational unit responsible for the processing activity: *Directorate General Corporate Services / Directorate Administration / Security and Safety Division* (DG-CS/DA/SET)

Data Protection Officer (DPO): DPO@ecb.europa.eu

2. Who is actually conducting the processing activity?

☐ The data is processed by the ECB itself

The organisational unit conducting the processing activity is:

☒ The data is processed together with an external third party.

In addition to internal staff, an external company providing physical security services (guarding services) monitors the video surveillance system at defined locations with qualified staff. The maintenance and administration of the video surveillance system is performed by an external company in a defined and controlled environment.

3. Purpose of the processing

The use of thermal imaging cameras and the auto-tracking functionality of pan-tilt cameras are tools to ensure the physical security on and access control to the ECB premises, by serving as alarm detectors within the perimeter of the ECB Main Building and by enabling the security guards to locate and follow a potential intruder approaching the building from the fence via the images displayed in the security control room. These cameras functionalities also support investigations, either in the case of an administrative enquiry or for witnessing a security incident.

For further details, please read the ECB Video Surveillance Policy and *the EDPS Prior Checking Opinion.*

4. Description of the categories of data subjects

Whose personal data are being processed?

- ☒ ECB staff
- ☒ Externals (agency staff, consultants, trainees or secondees)
- ☒ NCB or NCA counterparts (in the ESCB or SSM context)
- ☒ Visitors to the ECB, including conference participants and speakers
- ☒ Contractors providing goods or services
- ☐ Complainants, correspondents and enquirers
- ☐ Relatives of the data subject
- ☒ Other (please specify): *All persons on premises and in direct vicinity of premises*

5. Description of the categories of personal data processed

(a) **General personal data:**

The personal data contains:

- ☐ Personal details (name, address etc)
- ☐ Education & Training details
- ☐ Employment details
- ☐ Financial details
- ☐ Family, lifestyle and social circumstances
- ☐ Goods or services provided
- ☒ Other (please give details): *Images of individuals; licence plates of vehicles*

(b) **Special categories of personal data**

The personal data reveals:

- ☐ Racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health
- ☐ Data regarding a natural person's sex life or sexual orientation

6. The categories of recipients to whom the personal data have been or will be disclosed, including the recipients of the data in Member States, third countries or international organisations

- ☐ Data subjects themselves
- ☐ Managers of data subjects
- ☒ Designated ECB staff members
- ☐ Designated NCB or NCA staff members in the ESCB or SSM context
- ☒ Other (please specify): *In case of a security incident video footage may be transferred to the competent authorities either pro-actively or upon request, following consultation with the DPO, on a case-by-case basis*.

7. Transfers to/Access from third countries or an international organisation

Data are processed by third country entities:

- ☐ Yes

  Specify to which countries:

  Specify under which safeguards:

  - ☐ Adequacy Decision of the European Commission
  - ☐ Standard Contractual Clauses
  - ☐ Binding Corporate Rules
  - ☐ Administrative arrangement containing enforceable and effective data subject rights

If the third country's legislation and/or practices impinge on the effectiveness of appropriate safeguards, the personal data can only be transferred to, accessed from or processed in such third country when sufficient 'supplementary measures' are taken to ensure an essentially equivalent level of protection to that guaranteed within the EEA. These supplementary measures are implemented on a case-by case basis and may be technical (such as encryption), organisational and/or contractual.

☒ No

8. Retention time

Refer to ECB's Filing and Retention Plan

The data obtained will be stored for a maximum period of 21 days. 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 seven day retention period.