Bank of Valletta p.l.c.

CCTV POLICY

BOV
Bank of Valletta

Table of Contents

1. Who are we?

1.1. Bank of Valletta p.l.c. (hereinafter as the 'Bank', 'us', 'our', 'we'), is the Data Controller as defined by relevant data protection laws and regulations.

1.2. The Bank has appointed a Data Protection Officer who is responsible for ensuring compliance with data protection legislation. The Data Protection Officer may be contacted via email on *dpo@bov.com*.

2. Ownership

2.1. The Closed-Circuit Television System ('CCTV') (hereinafter also referred to as 'the System') is owned and managed by the Bank.

2.2. The System, all recorded material and copyright are owned by the Bank.

3. Introduction

3.1. This Policy aims to ensure that the use and management of the System complies with the applicable data protection and privacy laws, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the Data Protection Act (Chapter 586 of the Laws of Malta) and subsidiary legislation thereto, as may be amended from time to time. Photographic and visual material obtained from the system which includes recognisable individuals constitute personal data and are covered by data protection laws.

3.2. Should members of staff or external individuals/entities have any difficulties with understanding any aspect of this Policy, or require further information in respect to accessibility, interpretation or application of the Policy, they may contact the Bank's Data Protection Officer at *dpo@bov.com*.

4. Scope

4.1. The scope of this Policy is restricted to the CCTV System operated by the Bank only. This 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 or the governing body. CCTV recordings are monitored and retained in strict accordance with this Policy.

5. Entry in force and application of this Policy

5.1. This Policy shall enter into force on 18 May 2022.

5.2. The Bank shall review this Policy biennially, or earlier, if so, required by amendments made to the respective laws or if requested by the Office of the Information and Data Protection Commissioner and/or other relevant authorities.

6. Principles

6.1. Data collected from CCTV system will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the data protection laws in order to safeguard the rights and freedoms

of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Purposes of Processing

7.1. The CCTV system is intended to provide an increased level of security at the workplace for the benefit of those who work in or visit the Bank premises. The CCTV system will be used to respond to the following key objectives which will be subject to regular assessment:

- To detect, prevent or reduce the incidence of crime;
- To prevent and respond effectively to all forms of harassment and disorder;
- To prevent damage to property and assets of the Bank;
- To create a safer environment;
- To provide emergency service assistance; and
- To ensure the safety of staff, customers and visitors.

7.2. Footage will only be used for the stipulated purposes.

7.3. Processing for a distinct activity that is not compatible with the original reason for which the System was installed will only be performed if prior notice is given to the affected data subjects, and consent is attained, if required by law.

8. Legal Basis for Processing

8.1. The Bank justifies the use of a CCTV system for its legitimate business interests (Article 6 (1) (f) of the GDPR) such as maintaining security of property and premises, prevention and investigation of crime, safety of staff, customers, suppliers and visitors and quality control.

8.2. It is also within the affected data subjects' legitimate interest to monitor and consequently keep them safe and secure by preventing crime, preventing employee misconduct, ensuring compliance with health and safety procedures, monitoring and improving productivity, and comply with regulatory requirements.

9. Personal Data Captured

9.1. The Personal Data processed involves visual material which may include the following categories of data subjects: staff, customers, visitors, suppliers, offenders and suspected offenders, members of the public and any individual inside, entering or in the immediate vicinity of the area under surveillance.

10. CCTV System Details

10.1. The CCTV system installed in and around the Bank's premises is comprised of a mixture of visible fixed cameras located at various business facilities including:

- Exterior surfaces of the Bank's façade.
- Entrance to the interior premise/hall/meeting room.
- Customer area, counter and the tellers' area.
- Area where the cash is stored and administered (entrance and indoor premise).
- Area where the documents are stored and administered (entrance and indoor premise).
- Area where information technology systems are located (entrance and indoor premise).
- Area around generators.
- Area around ATMs.
- Parking
- Elevators
- Cash escort route (CASH route

The System continuously record images in real time and time lapse mode but will not record sound. The images are stored in digital video recorders which are kept in secure, locked areas accessible only by authorised staff.

10.2. Some of the rules for installing cameras in the Bank premises are as follows:

- The System should not violate the fundamental rights of the individual by interfering in his/her private life;
- Security measures must be complete to protect the data obtained from the recording, processing and storage of such data;
- Cameras shall not be hidden from view and warning signs are prominently placed before entering any area which is monitored. The signs will indicate the presence of monitoring and recording; and
- It is the Bank's policy not to use video surveillance in areas under "high expectations of privacy" e.g. canteens and toilets, except where the Bank feels it is necessary to deter and prevent illicit activities including but not limited to theft, voyeurism or sexual harassment. In any such cases of video surveillance, the Bank shall implement security measures to minimise the viewing of spaces/individuals which are not relevant to the legitimate purpose of monitoring, for example, by mounting the cameras in a particular position or using 'privacy masks' i.e. blocking/removing certain areas of a scene from the camera's view.

11. Access to, including viewing and/or disclosure of footage

11.1. Access to the CCTV footage is restricted to authorised personnel only. The Bank may authorise further access to footage if so required when relevant to purpose/s specified above.

11.2. Staff who are provided with access to the CCTV System are made aware of the sensitivity of handling CCTV images and recordings and are bound by strict confidentiality agreements.

11.3. The Bank may authorise access to footage if required, when relevant to the purpose/s specified above to:

- Law enforcement authorities with after filing a Police report;
- Any regulatory body or authorised entity, against a reasonable justification in writing;
- Legal representatives subject to court orders;

11.4. The extracted footage will be stored on a Hard Disk which is to be retained by the Bank. A Copy of the Disk will be made and is released to the requesting party upon signing the relevant Data Release Form and presenting an identification document. The Hard Disk and the Copy will be marked with an identical identification number, are sealed in their own case, and are securely kept.

11.5. The Bank shall maintain a record documenting all requests received for access to CCTV footage.

12. Data Subject Rights

12.1. CCTV footage, if sufficiently clear, are considered to be the personal data of the individuals whose images have been recorded by the CCTV System.

12.2. Data subjects have a right to access to their personal data under the data protection legislation. They also have other rights, in certain circumstances, including the right to have their data erased, rectified, and to restrict processing and object to processing. They can ask to exercise these rights by emailing the DPO at dpo@bov.com.

12.3. On receipt of a request – which needs to include the date and approximate time of the recording – the DPO will liaise with the Security Department regarding compliance with the request and communicate the decision to the data subject. This should be done without undue delay and at the latest within one month of receiving the request unless an extension of the period is justified.

12.4. If a request is to view footage, and the footage only contains the individual concerned, then the individual may view the footage. The authorised person accessing the footage must ensure that the footage available for viewing is restricted to the footage containing only the individual concerned.

12.5. If the footage requested contains images of other people, the DPO must consider:

- whether the images of the other people can be distorted so as not to identify them;
- seeking consent from the third parties to their images being disclosed to the requester; or
- if these options are not possible, whether it is reasonable in the circumstances to disclose the images to the individual making the request in any case.

13. Retention Periods

13.1. The CCTV footage shall not be stored for longer than is required for the stated purposes and in accordance with the Bank's data retention policy and procedures.

13.2. All active CCTV Systems within the Bank shall have a retention period of a maximum of Thirty (30) days.

13.3. Images will be automatically overwritten after the retention period elapses.

13.4. If required for evidential or other specific purposes, any recorded material and/or still photograph produced from the System will normally be retained for maximum period of three (3) months unless otherwise dictated by the enforcement agencies and law courts for evidential or other specific purposes.

13.5. Data Release Forms and other ancillary documents shall be kept in a secure location with access restricted to authorised personnel and will be retained for a period of five (5) years.

14. Complaints & Information

14.1. Any complaints or requests for information about the Bank's CCTV system should be addressed to the Data Protection Officer at *dpo@bov.com*.

14.2. Data subjects are also hereby informed of their right to lodge a complaint with the Office of the Information and Data Protection Commissioner ('IDPC'). The IDPC may be contacted as follows:

Address:
Information and Data Protection Commissioner
Level 2, Airways House
Triq il-Kbira
Tas-Sliema SLM 1549
Malta

Email: idpc.info@gov.mt