Closed Circuit Television (CCTV) Policy

Version	**0.1**
Date	**August 2021**

Document Control Information

Document Control

Policy Domain Expert	Policy Owner	Distribution Controller
ITPWG	Support Department	ORSG Unit

Modification History

Version	Modification Date	Comments	Authors
0.2	September 2021		Risk Committee
0.2	August 2021	Minor amendment & Approval	EXCO
0.1	August 2021	Approval	ITPWG
0.1	May 2021	First Draft version	Glen Simpson

Table of Contents

1. Overview

APS Bank plc. ("the Bank") operates a closed-circuit television ("CCTV") surveillance system ("the CCTV System") in its Offices and Branch network, including any other premises belonging to the bank, primarily to ensure the safety and security of staff members, customers, visitors and contractors at all times.

2. Purpose

This policy sets out the use and management of the CCTV System in compliance with the relevant data protection and privacy laws including but not limited to the Data Protection Regulation (EU) 2016/679 ("GDPR") and the Data Protection Act, Chapter 586 of the Laws of Malta and subsidiary legislation thereto, as may be amended from time to time (hereinafter collectively referred to as the 'Data Protection Laws'). The Bank has also produced this policy in line with the Guidelines on processing of personal data through video devices as published by the European Data Protection Board (Guidelines 3/2019) and adopted on 10 July 2019. Such Guidelines reflect the principles enshrined in the Data Protection Laws.

3. Scope

This policy applies to all of the Bank's CCTV Systems including closed circuit television ("CCTV"), Automatic Number Plate Recognition ("ANPR"), Licence Plate Recognition cameras ("LPR"), temporary CCTV arrangements and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. The Bank's CCTV System may capture images and audio recordings. CCTV recordings are monitored and retained in accordance with the Malta Bankers' Association guidelines.

4. Objectives

The Bank's objectives for processing of personal data through use of the CCTV System are the following (as may be applicable):

- Ensure the safety of staff members, clients, visitors & contractors
- Detect, prevent or reduce the incidence of crime
- Prevent and respond effectively to all forms of possible harassment and disorder
- Reduce the fear of crime
- Create a safer environment
- Provide emergency services assistance
- Investigate legal or insurance claims
- Investigate and manage internal incidents

5. Ownership

The CCTV System is owned, managed and operated by the Bank's Support Department with the assistance of the Security Services Company engaged by the Bank, particularly in certain locations.

The Head of Support or his delegate are responsible for the maintenance of the CCTV system.

The Support Department must liaise with the Operational Risk & Security Governance Unit (ORSG) that is responsible for the Security Governance.

6. Coverage

6.1 Permanent CCTV Cameras Coverage

Cameras are strategically located in sensitive areas throughout the premises of the Bank, particularly covering the perimeters, entrance and exit points, cash processing and other areas that the Bank may deem important to cover from time to time both in public and non-public areas.

The exact location of the cameras is confidential and restricted information due to security reasons. However, where ever there is a CCTV camera, clearly visible and legible signage is prominently placed at strategic points to inform staff members, visitors and members of the public that a CCTV System is in operation in that area.

6.2 Temporary CCTV Coverage

CCTV cameras can be positioned temporarily in strategic positions in a covert way under a limited number of circumstances. Such temporary placements may only be carried out in cases of suspected specific criminal activity or where the security of ("the Bank") is likely to be compromised and shall only be conducted where informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there is reasonable ground to suspect that illegal or unauthorised activity is taking place.

The placement of cameras in temporary arrangements requires the written authorisation of the Chief Risk Officer and the Head of Support and, where this may involve members of staff, the Head of Human Resources.

Any authorisation to use temporary CCTV arrangements must include a justification of the need to use such methods to obtain evidence of suspected criminal activity in a specific case; an assessment of alternative methods of obtaining such evidence and a statement of how

long the arrangement should remain in place. The authorisation must be reviewed every 15 calendar days in view of whether the arrangement should continue or otherwise.

Any decision to use temporary CCTV arrangements for any reason must be fully documented and records of such decision retained securely by the ORSG Unit.

7. Data Controller

APS Bank p.l.c., a Bank registered under the laws of Malta with registration number C2192 and having its registered address at APS Centre, Tower Street, B'Kara BKR 4012, Malta, is the data controller and responsible for any personal data collected, stored or processed under this policy.

The Bank has appointed a Data Protection Officer ("DPO"), who is responsible for ensuring compliance with data protection legislation. The DPO may be contacted via:

- Email on: **DataProtectionOfficer@apsbank.com.mt** or
- Mail to: **The Data Protection Officer**,
  APS Bank plc,
  APS Centre,
  Tower Street,
  Birkirkara BKR 4012

8. Processing of Personal Data

8.1 Access to Recordings by the Bank

Access to CCTV recordings is restricted to those who need to have access in accordance with this policy and any governing legislation.

Locations in which monitoring takes place include, but are not limited to, the Bank's Control Room, Designated Branch Staff Members and offsite at Security Service Providers.

Access to viewing of CCTV coverage shall be strictly limited to authorised personnel. Images displayed on monitors in these locations shall not be visible from outside the above mentioned rooms and locations.

All staff who have access to the CCTV System shall be made aware of the sensitivity of handling CCTV images and recordings and are obliged to sign a confidentiality agreement. The Security Services Company engaged by the Bank will ensure that authorised staff members are fully briefed and trained in all aspects of the operational and administrative functions of the CCTV System. All persons, be they APS staff or Security Services Company staff, authorized to access CCTV recordings shall do so in a judicious manner and related to

specific work exigencies. Every access to CCTV recordings is justified and a record (audit trail) including the reason for accessing such recordings is kept.

On removing the medium on which the images have been recorded for use in legal proceedings, should the need arise, the Bank ensures that there is documentation of:

- The reason why they were removed from the system;
- The date on which the images were removed from the general system for use in legal proceedings;
- Any crime incident number to which the images may be relevant;
- The location of the images;
- The signature of the collecting Police Officer or other Government agent where relevant.

8.2 Categories of Personal Data

The information processed may include visual images, licence plates, personal appearance and behaviours. This information may be about staff members, clients, visitors, suppliers, business partners and contractors, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Any monitoring in particular that of staff members will be carried out in accordance with applicable legislation and internal Policies and Procedures.

8.3 Lawful Basis of Processing

The Bank's legitimate interest for processing such personal data stems from the following: CCTV is used for maintaining safety, the security of property and premises and for preventing and investigating crime and safety related incidents, it may also be used to ensure the safety of staff, clients, visitors and contractors to ensure the quality of staff conduct and performance when carrying out work duties. The Bank recognises the effect of such a CCTV System on the individual and the right to privacy and protection of personal data.

8.4 Data Retention

No images and information shall be stored for longer than is required for the stated purpose. CCTV recordings will be kept for the period of time that is necessary for the Bank. In certain instances, the retention period of images captured by some cameras may be extended further for the purpose of security or according to legal obligations imposed on the Bank by law. In line with the special concessions given to banks within the 'Data Protection Guidelines for Banks' issued by the Malta Bankers' Association in collaboration with the Information and Data Protection Commissioner ('IDPC') and additional internal measures, any footage capturing customer/client images may be kept for 30 days, while any footage capturing

images of the employee's hands and the cash handling process may be kept for up to 90 days. Images will be deleted once their purpose has been discharged.

8.5 Disclosures of Personal Data

The Bank will share personal data with third parties only if there is a legal obligation imposed on it to do so.

8.6 Technical and Organisational Security Measures

The Bank shall implement and maintain appropriate and sufficient technical and organisational security measures, taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to protect personal data against any unauthorised accidental or unlawful destruction or loss, damage, alteration, disclosure or access to personal data transmitted, stored or otherwise processed and shall be solely responsible to implement such measures.

The Bank shall ensure that its staff members who process personal data are aware of such technical and organisational security measures. The Bank shall ensure that such staff members are bound by a duty to keep personal data confidential.

The technical and organisational security measures in this clause shall mean the particular security measures intended to protect personal data of individuals in accordance with the Data Protection Laws.

9. Rights of Data Subjects

9.1 Right of Access

Anyone who believes that they have been recorded by the CCTV System can request a copy of the recording, subject to any restrictions covered by applicable Data Protection Laws, security considerations and Freedom of Information Act. Such request will be evaluated by the person(s) within the Bank responsible for data protection who will provide without excessive delay and without expense, written information as required by law. Where required to be provided, the information shall indicate, in particular:

- The actual personal data which are processed;
- The source of the information;
- The purpose of the processing;
- Any recipients or categories of recipients of the data;
- The applicable retention period;

- The various rights to which the data subject is entitled under the GDPR (including the right to rectification, erasure and restriction - where applicable as well as the right to lodge a complaint with the Maltese Office of the Information and Data Protection Commissioner);
- As well as any other information to which the data subject is entitled under Article 15 of the GDPR (Right of Access).

In such cases, only information concerning the individual specifically making the request may be provided. Other information revealing the identity of other persons shall not be disclosed. In the case of an ongoing investigation, whereby providing information may be prejudicial to the investigation itself or to the rights and freedoms of others, such information could be withheld.

Although the law does not specifically entitle the individual to have an extract of the images being recorded, or to view directly the images, in the case of CCTV systems, the most practical approach is to invite individuals for direct viewing of the images, provided that the identity of third parties is obscured. If an individual is not satisfied with the reply provided, or with the manner by which access is granted, the matter may be referred to the Information and Data Protection Commissioner who will investigate the case and ascertain that the right of access is properly granted.

9.2 Right to Rectification

Data subjects also have the right to request that inaccurate data be corrected or erased; and to seek redress for any damage caused. Procedures are in place to ensure all such requests are dealt with effectively and within the law.

9.3 Right to Lodge a Complaint

Data subjects have the right to lodge a complaint regarding the processing of their personal data with the supervisory authority for data protection matters. In Malta this is the Information and Data Protection Commissioner (“IDPC”), with whom a complaint can be lodged on the IDPC’s website via this link. https://idpc.org.mt

9.4 Right to Erasure

In certain circumstances data subjects may request the Bank to delete the Personal Data that is held about them;

9.5 Right to Object

Data subjects have a right to object and request that the Bank ceases the processing of their personal data where the Bank relies on its own, or a third party's legitimate interest for processing personal data;

9.6 Right to Portability

Data subjects may request the Bank to provide personal data of the data subject in a structured, commonly used and machine-readable format. Where technically feasible, data subjects may also request that the Bank transmits their personal data to a third party controller indicated by the data subjects;

9.7 Right to Restriction

Data subjects have the right to request the Bank to stop using their personal data in certain circumstances, including if they believe that the Bank is unlawfully processing their data;

Data subjects' rights are not absolute and the Bank may not be able to entertain the above requests if it is prevented from doing so in terms of the applicable law.

10. Third-Party Access to Personal Data

Access to recorded images is only granted to third parties that are eligible to it by law.

The Bank may release recordings to the Malta Police Force or other authorities empowered by law to request the information, for the purposes of prevention or detection of crime, the apprehension or prosecution of offenders, or in the interests of national security, or in other circumstances where the Bank is legally obliged to do so, or in accordance with the specified purposes of the CCTV system. Access to recorded images by the Malta Police Force or other authorities are made via an official request and is recorded accordingly by the Bank. Disclosure of CCTV recordings to third parties will only be made in accordance with the purposes of the CCTV System and in compliance with applicable Data Protection Laws.

11. Deviations from the Policy

Deviations can be a result of instances where it may not be technically, operationally possible or cost-effective to comply with the policy statements hence it is to be reported to the Policy Owner. This is done in order to evaluate the security, operational and other risks anticipated as a result from the deviation and to identify additional compensating controls required to mitigate these risks or when this is not possible, to formally acknowledge any residual risk and assign appropriate responsibility for further monitoring.

When all options have been exhausted, a request for exemption shall be forwarded to the Policy Owner and Chief Risk Officer or delegate for assessment.

12. Breach of Policy

Breaches of this policy including accidental or unintentional activity is to be reported to the Policy Owner, who will in turn escalate to the Chief Risk Officer or delegate in order to determine appropriate corrective action.

Any employee or contractor found to have violated any statement/s of this policy may be subject to disciplinary action, which may also result to termination of employment, or termination of contractual agreements, denial of access and/or penalties both criminal and civil.

The Breach could also be reported to the Internal Audit Unit for further investigation and for potential internal control improvements.

13. Document Information

13.1 Related Documents

Name	Location

13.2 References

Name	Location
Malta Bankers' Association Archival Material Retention Periods	*https://idpc.org.mt/wp-content/uploads/2020/07/Data-Protection-guidelines-for-banking.pdf*
Information Commissioner's Office	https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

13.3 Issuing Authority

This CCTV policy has been compiled by the Support Department.

Technical review and maintenance of this document is under the direction and authority of the IT Policy and Standard Working Group. The policy document will be escalated in line with the process as outlined in ITPWG terms of reference document.

This CCTV policy has been approved by Risk Committee (RC).

13.4 Contact Information

APS Bank IT Policies, Standards, Procedures and associated publications can be found on Insight.

13.5 Policy Review

This policy will be reviewed every two years or earlier in case of changes in regulations/directive.

14. Further Information

For more detailed information on how the data subjects' personal data are processed, be it with regard to this CCTV policy or otherwise, including information on data subject rights, please read the APS Privacy Policy which can be accessed on https://www.apsbank.com.mt/en/gdpr or ask for a printed copy at the address cited below.

For further information relating to this policy and the procedures concerning the use of CCTV cameras, employees and other individuals are to contact: csc@apsbank.com.mt.

In addition, for matters or enquiries relating to data protection, individuals may wish to contact the DPO at the address specified above in Clause 7, or else the Information and Data Protection Commissioner using the details provided below:

Office of the Information and Data Protection Commissioner

2, Airways House

High Street

Sliema, SLM 16

Tel: (356) 2328 7100

Fax: (356) 2328 7198