

POLICY ON PERSONAL DATA PROCESSING

for video surveillance of the premises and facilities of the Central Bank of San Marino,

issued in accordance with Article 13 and Article 14 of Law No. 171 of December 21, 2018, "Protection of individuals with regard to the processing of Personal Data"

Preamble

This document is drawn up by the Central Bank of the Republic of San Marino, in the capacity of the Data Controller (hereinafter "**CBSM**" or "**Data Controller**") and in compliance with the current legislation on the protection of Personal Data, particularly Article 13 and 14 of Law No. 171 of December 21, 2018, titled "Protection of individuals with regard to the processing of Personal Data" and subsequent amendments (hereinafter "**Law**"), and Article 13 and Article 14 of the EU Regulation 2016/679 (hereinafter "**GDPR**").

This privacy policy (hereinafter "**Policy**") is provided in addition to the information that is made publicly available through the signs displayed within CBSM premises and provided directly by CBSM or collected from third parties (hereinafter also "**Data Subjects**") and relates to the processing of Personal Data carried out by CBSM for video surveillance purposes.

"**Personal Data**" refers to each of the categories indicated above, considered as a whole. Personal Data is therefore defined as any information concerning an identified or identifiable natural person.

An identifiable person is one who can be identified, either directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more physical, physiological, genetic, mental, economic, cultural, or social factor.

SECTION 1

CONTACT DETAILS OF THE DATA CONTROLLER

Pursuant to Article 2 of the Law, the Data Controller for the purposes set out below is the Central Bank of the Republic of San Marino, whose headquarters and General Directorate is located at Via Del Voltone n. 120, 47890 – San Marino (Republic of San Marino).

For additional information, the Data Controller may be contacted via email at privacy.titolare@bcsm.sm or by written request to Banca Centrale della Repubblica di San Marino, Via del Voltone n. 120, 47890 – San Marino (RSM). Alternatively, the Data Controller can be contacted by phone at +378 0549 981010 or by fax at +378 0549 981019.

SECTION 2

CONTACT DETAILS OF THE DATA PROTECTION OFFICERS (DPOs)

The Controller has appointed Ms Valentina Rabitti and Mr Nathaniel Casadei as “Data Protection Officers” (hereinafter, “**DPOs**” or “**RPDs**”), in accordance with Chapter 4 of the Law. For all issues relating to the processing of Personal Data and/or to exercise the rights envisaged by the Law itself, listed in Section 11 of this Policy, please, send an email to privacy.dpo@bcsm.sm, or a letter to “Nova Poesis, Via Pomposa no. 43/l, 47924 – Rimini (IT)”, addressed to the RPDs.

SECTION 3

TYPE AND SOURCE OF THE PERSONAL DATA SUBJECT TO PROCESSING

In carrying out its functions, CBSM processes Personal Data in the form of images through video surveillance systems, as described below.

Each video surveillance system consists of multiple cameras that only record the passage areas within the bank premises and near the technical facilities of the Data Controller, and they capture images – considered as Personal Data under the relevant laws on data protection and GDPR – of individuals (such as visitors, employees, etc.) passing within the field of view of each camera (hereinafter “**Images**”).

An operational 24/7 video surveillance system is in place around each of the bank relevant area. Cameras are positioned in a way that they comply with the following standards:

- a) they must be located around duly signposted sensitive areas.
- b) they must not capture private staff areas – e.g., changing rooms, toilets, rest areas.
- c) they must not capture workstations continuously.

In relation to points b) and c), reference is made to the provisions of employment contracts for all categories – managers, employees, auxiliaries, and management personnel – stating as follows: “Audio/video recordings revealing the ordinary work activities of employees are not allowed, not even for security reasons, unless the RSA (Employee Representative Union) and all employees have been previously informed.”

The CBSM video surveillance system is configured and positioned so that the cameras primarily capture the areas relevant to CBSM and avoid surrounding areas. All video-monitored areas are duly signposted.

SECTION 4

PURPOSES AND LEGAL BASIS FOR THE PROCESSING

The processing of Personal Data for video surveillance purposes is carried out in accordance with Law no.171/2018 (and subsequent amendments), Article 5, paragraph 1, letter d) ("Processing is necessary for the protection of the vital interests of the Data Subject or any other natural person, only when none of the other legal grounds provided by that article is applicable.") and letter f) ("Processing is necessary for the pursuit of the legitimate interests of the Data Subject or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, particularly if the Data Subject is a minor. This provision shall not apply to processing carried out by public authorities in the performance of their tasks").

CBSM shall process the images for the pursuit of the Data Controller's legitimate interests and for video surveillance purposes, such as:

- Protecting corporate assets.
- Ensuring safety in work environments with the aim to safeguard employees, visitors, and all individuals accessing the premises, even in case of emergencies.
- Preventing, investigating, and repressing crimes and offenses, such as acts of vandalism, theft, robbery, damage, or other crimes against the premises and/or property of the Data Controller or under their management and/or custody, and against the Data Subjects in and outside the company premises.

SECTION 5

DATA PROCESSING METHODS

In view of the aforementioned purposes, image processing is carried out electronically through the following operations: collection, recording, organization, storage, consultation, processing, selection, extraction, use, blocking, transmission, and deletion.

Images can be processed exclusively by a limited number of employees of the Data Controller, acting as data processors and/or internal Data Controllers and/or system administrators, and by the authorized external provider during system maintenance interventions. All the aforementioned parties shall process images based on specific written instructions provided by the Data Controller.

Consent to image acquisition is automatically given by the Data Subject upon crossing the surveillance notice sign displayed nearby the recording cone. In the event that the Data Subject does not wish to be recorded, the Data Controller will not be able to grant them access to the company premises.

Suitable technical and organizational measures shall be adopted to ensure an adequate level of security against risks, specifically the destruction, loss, alteration, and unauthorized disclosure or access, whether accidental or unlawful, to the Personal Data being processed.

Access to recordings is password-protected and may be granted only in the presence of authorized security personnel. Police forces are allowed to access any recordings received by competent authorities for criminal investigation. The recordings acquired may only be used as judicial evidence.

The processing of data obtained from the video surveillance system may be carried out by the Security Manager and the Deputy Security Manager exclusively. Any other individual is prohibited from accessing or obtaining the Images and data collected by the system.

In case of the processing of information already provided upon previous access to the CBSM premises, visitors do not have to renew their written consent (when required), provided that the subsequent processing occurs within the time period outlined in Section 8. However, it is always within the Data Subject's rights to request new copies of this policy.

SECTION 6

DISCLOSURE OF DATA

Images shall not be disclosed to third parties except to Public Authorities acting upon request of third parties or, when necessary, acting as autonomous Data Controllers for the prevention, investigation, and suppression of crimes and offenses, workplace security, as well as for the protection of corporate assets.

Personal data shall not be disclosed or transferred to non-EU countries.

For the pursuit of the purposes outlined in the previous Section 4, Personal Data shall be processed by specifically designated employees of the Central Bank of the Republic of San Marino, who are authorized to process such data.

Additionally, CBSM may occasionally need to share Personal Data with third parties belonging to the following categories:

- External data processors, particularly IT service and product providers
- Authorities, judicial bodies, supervisory and control bodies, and the Police

The entities belonging to the aforementioned categories may operate as Data Controllers, completely independent from CBSM, or as Data Processors formally designated by the latter through written notice. The list of external entities designated as Data Processors for specific processing activities will be kept up-to-date at CBSM's headquarters and made available for consultation at the address of the Data Controller indicated in Section 1.

SECTION 7

TRANSFER OF DATA TO THIRD COUNTRIES

Personal Data is stored within the territory of the Republic of San Marino. The Data Controller does not transfer Personal Data to third countries or international organizations.

SECTION 8

DATA RETENTION

As a general practice, images are stored for a minimum of approximately 7 days to a maximum of 18 days. After this period, images will be automatically overwritten, unless there is a need to extend their retention due to specific requests from the Authorities.

CBSM might be required to retain your data for a longer period in compliance with legal obligations, for public interest, or by order of an authority.

At the end of the retention period, Personal Data will be deleted.

Henceforth, the right to access, erasure, rectification, and the right to data portability cannot be exercised anymore.

SECTION 9

AUTOMATED DECISION-MAKING PROCESS

CBSM does not process Personal Data through any automated decision-making processes, including profiling as mentioned in Article 22 of the Law.

SECTION 10

RIGHTS OF THE DATA SUBJECT

The Data Subject may exercise the following rights granted by the legislation on Personal Data Protection against CBSM at any time. To do so, the Data Subject must submit a specific written request to the Central Bank of the Republic of San Marino using one of the following means:

- recorded delivery letter addressed to Banca Centrale della Repubblica di San Marino, Via del Voltone no. 120 – 47890 San Marino (RSM)
- email to privacy.titolare@bcm.sm
- fax to + 378 0549 981019

1. Right of access

The Data Subject shall have the right to obtain confirmation from CBSM of whether its Personal Data is being processed, and, if so, request access to the Personal Data and information envisaged by Article 15 of the Law. This includes obtaining information about the purposes pursued by the Data Controller, the categories of data involved, the recipients to whom the data may be disclosed, the applicable retention period, and the existence of automated decision-making processes, among others.

2. Right to rectification

The Data Subject has the right to obtain from CBSM, without undue delay, the rectification of their Personal Data, in case of inaccuracies. Additionally, considering the purposes of the processing, the Data Subject may request the completion of their data, if it is found incomplete, by providing a supplementary statement.

3. Right to erasure

The Data Subject has the right to request the erasure of their Personal Data from the Controller, if one of the reasons set forth by Article 17 of the Law applies. The Data Subject may exercise such right if their Personal Data is no longer necessary for the purposes for which it was collected or otherwise processed or if consent to the processing has been revoked and there is no other legal basis for processing their Personal Data. However, the revocation of consent shall not affect the lawfulness of any processing carried out prior to such revocation. Please, note that CBSM may not be able to erase your Personal Data if its processing proves necessary to comply with a legal obligation, for reasons of public interest, or for legal purposes such as establishing, exercising, or defending legal claims.

4. Right to restricted processing

The Data Subject may request that the processing of their Personal Data be restricted where one of the circumstances envisaged by Article 18 of the Law applies. This may include circumstances in which the Subject deems their data incorrect, or when the data is necessary for legal purposes such as establishing, exercising, or defending legal claims, even though CBSM no longer needs it for its original processing purposes.

5. Right to data portability

In accordance with the provisions of Article 20 of the Law, if the processing of Personal Data is consensual or essential for the execution of a contract or pre-contractual measures, and the processing is carried out using automated means, you may:

- request to receive the Personal Data you provided in a structured, commonly used, and in a computer or tablet format.

6. Right to object

The Data Subject may object to the processing of their Personal Data at any time, especially if the processing is carried out for the performance of an activity in the public interest or for the pursuit of the Data Controller's legitimate interests, including profiling, as specified in Article 21 of the Law. Should the Data Subject decide to exercise their right to object, CBSM shall refrain from processing their Personal Data any further, unless there are compelling legitimate reasons for the processing which outweigh the interests, rights and freedoms of the Data Subject or for the establishment, exercise, or defence of legal claims.

7. Right to lodge a complaint with the Data Protection Authority

Without prejudice to your right to resort to any other administrative or judicial remedies, if you believe that the processing of your Personal Data by the Data Controller violates the Law and/or applicable regulations, you may lodge a complaint with the competent Supervisory Authority for Personal Data Protection.