GIBRALTAR ELECTRICITY AUTHORITY

CCTV POLICY

25th September 2023

Version 2

Contents

1. Policy Statement

1.1 CCTV and other surveillance systems have a crucial and legitimate role to play in helping the Gibraltar Electricity Authority ('The Authority') perform our statutory functions of supplying electricity to the general public, as well as ensuring we adhere to our duty of care towards our staff by maintaining a safe and secure environment.

1.2 However, we recognise that the use of CCTV may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns. Images recorded by surveillance systems are Personal Data, which must be processed in accordance with the Applicable Data Protection Law.

1.3 This policy applies only to the CCTV used by The Authority and will inform you what to expect when we collect Personal Data about you, in this case static or moving imagery captured via CCTV or surveillance systems in or around our offices and at our depots at the North Mole Power Station, Rosia Road Electricity Centre, Admiral Rooke Road, and Distribution Centres.

1.4 If you have any questions about this policy or our privacy practices, please contact us on privacy@gea.gi.

1.5 You have the right to make a complaint at any time to the office of the Gibraltar Regulatory Authority (GRA), the supervisory authority for data protection issues in Gibraltar, by contacting them on privacy@gra.gi or via their website www.gra.gi. We would, however, appreciate the chance to deal with your concerns before you approach the GRA so please contact us in the first instance.

2. Definitions

2.1 For the purposes of this policy, the following terms have the following meanings:

Applicable Data Protection Law: means the Gibraltar General Data Protection Regulation 2016/679 (the "Gibraltar GDPR") and the Data Protection Act 2004, as revised and superseded from time to time, and any other laws and regulations relating to the processing of Personal Data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the GRA;

Authorised Personnel: means an Authority employee who is included within Appendix 1.

CCTV: means fixed and domed cameras designed to capture and record images of individuals and property.

Data Controller: means a person or organisation who, either alone, or jointly, or in common with other persons determines the purposes for which and the manner in which any Personal Data are to be processed.

Data Processor: means any person or organisation that Processes Personal Data on the Data Controllers' behalf and in accordance with their instructions.

Data Subjects: means all living individuals about whom we hold Personal Data as a result of the operation of The Authority CCTV.

Department CCTV: means our CCTV cameras operated in or around our offices and sites, and at our depots at the North Mole Power Station, Rosia Road Electricity Centre, Admiral Rooke Road, and Distribution Centres.

DSAR: means the enforcement of a Data Subjects' right to access under the Gibraltar GDPR by way of a Data Subject Access Request.

Personal Data: means data relating to a living individual who can be identified from that data (or other data in our possession). In respect of CCTV, this generally means video images and it may also include static pictures such as printed screen shots.

Processing: means any activity that involves the use of Personal Data. It includes obtaining, recording or holding Personal Data, or carrying out any operation on the Personal Data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring Personal Data to third parties.

Senior Management Team: means The Authority's senior officers, from time to time consisting of; the Chief Executive Officer and the Deputy Chief Executive Officer.

3. About this Policy

3.1 The CCTV system is owned and operated by The Authority, and its deployment is determined by the Senior Management Team.

3.2 This policy outlines why we as Data Controller use the CCTV and the lawful basis which we rely on, how we will use it and how we will process your Personal Data to ensure we are compliant with the Applicable Data Protection Law and best practice. This policy also explains how to make a DSAR in respect of Personal Data created by CCTV in addition to other data protection rights.

3.3 This policy applies to all of The Authority's members of staff, including contracted workers.

3.4 This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract you may have with us.

4. Personnel Responsible

4.1 The Senior Management Team have overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy.

4.2 The responsibility of the Senior Management Team includes:

- Ensuring that the use of The Authority CCTV is implemented in accordance with this policy.
- Keeping this policy updated.
- Overseeing and co-ordinating the use of CCTV monitoring for safety and security purposes within areas under their responsibilities.
- Ensuring that the existing Authority CCTV is evaluated for compliance with this policy.
- Ensuring that the CCTV monitoring is consistent with the highest standards and protections, including consideration of expectations of privacy.
- Reviewing camera locations and be responsible for the release of any information or materials stored in compliance with this policy.
- Maintaining a record of access to, and release of Personal Data.
- Giving consideration to both staff and general public feedback/complaints regarding possible invasion of privacy due to the location of a particular CCTV camera.
- Ensuring that appropriate CCTV signage is conspicuously placed at every location where The Authority is operating CCTV.
- Ensuring that internal/external cameras are non-intrusive in terms of their positions and views of residential housing.
- Ensuring that images and monitoring footage are stored in a secure place

with access by Authorised Personnel only.

- Ensuring that recorded images/footage are stored for a period not longer than 30 days and are then erased unless required as part of a disciplinary, criminal investigation or court proceedings (criminal or civil).

5. Reasons for the use of CCTV

5.1 We currently use The Authority CCTV as outlined below:

(a) Protecting the buildings, sites and assets internally and externally, both during and after site opening hours.

(b) For the safety and security of our staff and visitors.

(c) For the proper accounting of personnel during incidents of fire or any other emergency events which require immediate evacuation of premises.

(d) Deterring and reducing the incidence of crime and anti-social behaviour (including theft and vandalism).

(e) Supporting law enforcement bodies in the prevention, investigation, detection and prosecution of criminal offences.

(f) For investigative purposes, or as evidence to support, any formal follow-up to office/site incidents.

(g) To assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.

5.2 CCTV systems will not be used to monitor normal working procedures (for example; time keeping).

6. Data Protection Impact Assessments

6.1 Where new CCTV systems or cameras are to be installed, the Senior Management Team will carry out a full Data Protection Impact Assessment (DPIA) and identify risks related to the installation and ensure compliance with the Applicable Data Protection Law. This may, in some circumstances, involve the need for consultation with staff.

6.2 Where existing CCTV systems or cameras are in operation as of September 2022, The Authority will endeavour to carry out a full DPIA of the CCTV system or cameras within a 2-year period.

7. Monitoring and Recording

7.1 CCTV cameras will be sited so that they only capture images relevant to the purposes for which they are installed. Due consideration will be taken to ensure that reasonable privacy expectations are not violated.

7.2 The Senior Management Team will ensure that the location of the CCTV cameras and equipment are carefully considered to ensure that images captured comply with the Applicable Data Protection Law.

7.3 CCTV cameras will not be used in private areas such as toilets and showers.

7.4 CCTV cameras placed so as to record internal and external areas are positioned, in so far as possible, in such a way as to prevent or minimise recording of passers-by or of another person's private property.

7.5 The Authority does not engage in covert surveillance.

7.6 Images and recorded footage, and the monitoring equipment will be securely stored onsite. Unauthorised access to these areas will not be permitted at any time. These areas will be locked and a log of access to the images and footage will be maintained as per Appendix 2.

7.7 Access will be limited to officers listed in Appendix 1. When accessing the CCTV footage/images two Authorised Personnel must be present. The log access of CCTV monitoring can be found at Appendix 2. Every instance must be recorded.

7.8 Authorised Personnel must be reviewed on a yearly basis, and additionally whenever any Authorised Personnel leaves The Authority.

7.9 Images are recorded centrally on secure servers located onsite. Recorded images will only be viewed in designated, secure offices.

7.10 Mobile phones and other recording devices are not allowed within these secure offices whenever CCTV footage is being reviewed.

7.11 The CCTV cameras installed provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

7.12 All images recorded by The Authority CCTV System remain the property and copyright of The Authority.

7.13 CCTV monitoring will not take place unless such footage forms part of a security or other incident, or as part of random quality controls conducted by the Senior

Management Team, including as a result of consultation with the Human Resources Departments and/or the Government's Audit Department.

7.14 We may engage Data Processors to process Personal Data on our behalf. If we do this, we will ensure reasonable contractual safeguards are in place to protect the security and integrity of the Personal Data.

7.15 All staff involved in the operation of the CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained herein.

8. Transfers of Personal Data outside of Gibraltar

8.1 We do not usually transfer any Personal Data outside of Gibraltar. However, where this is necessary, we will only do so in compliance with the additional rules applicable under the Applicable Data Protection Law and ensuring that all information is secure.

9. Storage Retention of Personal Data

9.1 The Authority will ensure that any recorded images to which we have access are stored in a way that maintains its integrity and security. This may include encrypting the Personal Data, where it is possible to do so.

9.2 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images/footage will be retained for no longer than 30 days from the date of recording. The footage will be automatically overwritten after this point.

9.3 Where an image/footage is required to be held in excess of the retention period referred to in 9.2, the Chief Executive Officer or their nominated deputy, will be responsible for authorising such a request.

9.4 When image/footage is required to be kept for longer than 30 days a log must be kept specifying the reasons why it is being kept and who is in possession of the information. This log must be reviewed once per month to ensure it is kept updated.

9.5 If after review, any image/footage that has been held in excess of their retention period is no longer required, it must be safely deleted with all appropriate safeguards in relation to privacy matters.

9.6 At the end of their useful life, all images/footage stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be

disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

10. Access and Requests for Disclosure

10.1 Access will be restricted to Authorised Personnel as noted in Appendix 1.

10.2 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, in relation to the prevention, investigation, detection or prosecution of criminal offences, or in other circumstances where an exemption applies under relevant legislation.

10.3 Disclosures as per 10.2 will be made at the discretion of the Chief Executive Officer or their nominated deputy, with reference to relevant legislation.

10.4 We may share Personal Data with the Human Resources Departments, Gibraltar Law Offices, the Audit Department, law enforcement bodies and our professional advisors when we consider that this is reasonably necessary for any of our legitimate purposes.

10.5 Extracted images/footage will be stored in a secure environment with a log of access. Access will be restricted to Authorised Personnel.

10.6 A record of the date of any disclosure request along with details of whom the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept for accountability purposes.

10.7 Personal Data will be provided to those requests authorised in a permanent format where possible. If this is not possible, we will offer the opportunity to view the footage.

11. Data Subject Access Requests ("DSARs")

11.1 Data subjects may make a request for disclosure of their Personal Data and this may include CCTV images/footage. A DSAR is subject to the statutory conditions from time to time in place and should be made in writing to our Senior Management Team on privacy@gea.gi.

11.2 In order for us to locate relevant footage, any requests for copies of recorded CCTV images should include the date and time of the recording, the location where the footage was captured and, if necessary, Personal Data identifying the individual.

11.3 Where possible The Authority must respond to the request without undue delay. If the response is to take one calendar month, The Authority must ensure that the requested image/footage is extracted as soon as reasonably possible, so as to avoid the requested data from being accidentally erased after the request has been made.

11.4 In giving a person a copy of their Personal Data, The Authority provides a still/series of still pictures, a tape or a disk with relevant images/footage. However, other images of other individuals will be obscured before the Personal Data is released.

11.5 Notwithstanding 11.4, The Authority reserves the right to not provide images/footage in a permanent format and instead offer the Data Subject the opportunity to view the image/footage at their offices accompanied by Authorised Personnel.

11.6 Data Subjects may be asked to provide proof of identity for comparison with the images/footage prior to searching and disclosing any information.

11.7 A record of the date of the DSAR (including details of who the information has been provided to) will be kept for accountability purposes.

12. Staff Training

12.1 Staff authorised to access The Authority CCTV system will be trained to comply with this policy.

12.2 Staff will understand that all information relating to The Authority CCTV is confidential and must be handled securely.

12.3 Staff will receive appropriate training to enable them to identify and handle different requests for access and disclosure of Personal Data.

12.4 Any misuse or unauthorised access of The Authority CCTV will lead to disciplinary proceedings.

13. Policy Review

13.1 The Authority's use of CCTV and the content of this policy shall be reviewed every two years with reference to the Applicable Data Protection Law. Further reviews will take place as required.

Appendix 2

CCTV MONITORING LOG

CCTV images/video footage review needs to be carried out by two authorised persons and the following form completed prior to its review.

Date	Time	Name of 1st officer	Name of 2nd officer	Reason for review
(a)	(b)	(c)	(d)	(e)