

CCTV Policy

Geberit Sales Ltd

Contents

1. Policy Statement and Scope of Policy	3
2. Principles	3
3. CCTV System Overview	4
4. Objectives of the CCTV System	4
5. Monitoring and Recording	5
6. Data Protection	5
7. Application for disclosure of images	6
8. Retention of images	7
9. Documentation & Review	7
10. Feedback	7

1. Policy Statement and Scope of Policy

- 1.1 This policy applies to Geberit Sales Ltd known throughout this policy as the “Company”, “we”, “We”, “Our” or “our”.
- 1.2 In this policy, when we refer to “you” or “your”, we are referring to employees, workers, agency workers or contractors employed or engaged by the Company.
- 1.3 We are committed to the safety of our staff and all those working or visiting our facility. As such we have invested in systems to support the prevention of crime and to aid the security of our buildings and facilities. This policy details how we will regulate the management, operation and use of the closed-circuit television (CCTV) system.
- 1.4 This policy seeks to comply with the **General Data Protection Regulation (GDPR)** and the **Data Protection Act 2018 (DPA)** and any other regulations that govern the processing of personal data from time to time (“the Data Protection Laws”).
- 1.5 Any breach of this policy by an employee, worker, agency worker or consultant will be taken seriously and may result in disciplinary action in relation to employees and other action in relation to non-employees. Serious or repeated breaches of this policy may be considered as an act of gross misconduct (if you are an employee) and will be managed accordingly in line with the Disciplinary Policy. If you are a contractor, worker or agency worker, a serious or repeated breach may result in the immediate termination of any agreement or engagement.
- 1.6 This policy does not form part of an employee’s contract of employment and the Company can amend this policy at its sole discretion. The Company will always consider a best practice approach when making changes to its policy.
- 1.7 This Policy should be read in conjunction with Geberit’s Security Policy.

2. Principles

- 2.1 We are committed to ensuring that the use of personal data throughout the Company is in accordance with legal requirements and that the integrity and protection of data are maintained at all times. As such we will have due regard to the Data Protection Act (2018) and the General Data Protection Regulation (GDPR), as well as having due regard to the 12 guiding principles issued under the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (amended in 2021).
- 2.2 This Policy has been drawn up in a accordance with advisory guidance contained within the Information Commissioner’s CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

- 2.3 The operators of the CCTV system recognise the effect of such systems on the individual and the right to privacy.
- 2.4 Jana Lenzen from KREMER Rechtsanwälte is assigned as the Data Protection Officer for all Geberit companies and is responsible for ensuring compliance with the Act. Ashley Anderson and Louise Rigden are Data Protection Coordinators for Warwick.

3. CCTV System Overview

- 3.1 We operate CCTV on all external doors, the car park and the garage with images being monitored and recorded centrally on the server. No camera fitted on our premises has the ability to record sound.
- 3.2 We are registered with the Information Commissioners Office and have declared the use of CCTV on our premises.
- 3.3 The Facilities and Compliance Manager is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing and monitoring of the system.
- 3.4 Signage is prominently placed at strategic points to inform staff, visitors and members of the public that a CCTV installation is in use.
- 3.5 Any tampering of Company surveillance equipment is not permitted and will be considered as a Gross Misconduct offence. Only authorised personnel are permitted to amend, change, remove, or otherwise adjust any element of the equipment. Any persistent malfunctions of recording devices, such as non-recording, adjusting camera angles, placement and general tampering will be investigated in line with the disciplinary policy.

4. Objectives of the CCTV System

- 4.1 The principle purposes of the CCTV system are as follows:
 - 4.1.1 Protect the Company's buildings, its assets and to ensure that they are free from intrusion, vandalism, damage, disruption, either from its own staff or those with no connection to the Company.
 - 4.1.2 To ensure the safety of all employees, contractors and visitors to site.
 - 4.1.3 To assist in the investigation of suspected breaches of the Company's policies and rules. If an act of Misconduct becomes apparent the system will be reviewed and can be used as evidence during a formal disciplinary or grievance procedure. You will be given the opportunity to view any relevant footage referred to during the process. *Please refer to the Disciplinary Policy.*

4.1.4 To assist in the investigation of suspected Health and Safety breaches.

5. Monitoring and Recording

- 5.1 CCTV is not routinely monitored but will be reviewed where a crime, potential crime, or suspected violation of Company policy, practice or Health and Safety infringement has taken place and the CCTV may be used as evidential support.
- 5.2 Data recorded from the cameras located on or in Company buildings will be routinely stored for 30 days, or if required for evidence, as detailed in section 7 of this policy.
- 5.3 Images from the cameras located in and around the Company's premises will be stored on a recording device, within a secure, locked room, accessible only to a limited number of people. Access to the recording system is password protected and will not be disclosed to unauthorised individuals. General access is not available.
- 5.4 This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those entering, exiting or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the data subjects themselves, employees, service providers, police forces, court or tribunal, security organisations and persons making an enquiry.
- 5.5 The camera's installed provide images that are of suitable quality for the specific purposes for which they are installed.
- 5.6 All images remain the property of the Company.
- 5.7 CCTV will be kept to public areas and will not be used in areas reasonably considered to be private or such an area that the Company feels would breach an individual's right to privacy.

6. Data Protection

- 6.1 The Company complies with principles relating to the protection of personal data as detailed within the GDPR, Data Protection Act (2018) and guiding principles of the Surveillance Camera Code of Practice. Information obtained will be:
 - 6.1.1 Collected only for specified, explicit and legitimate purposes;
 - 6.1.2 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
 - 6.1.3 Accurate and where necessary kept up to date;

- 6.1.4 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the Data is processed; and
- 6.1.5 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 6.2 The Company is responsible for and will seek to demonstrate compliance with the above principles.

7. Application for disclosure of images

- 7.1 We will process, under our legitimate interest, any evidence obtained from the CCTV systems if deemed applicable for disciplinary, grievance or other formal process. We are able to process this personal data as we have a legitimate interest in maintaining levels of conduct, and protecting the welfare and safety of our employees, contractors and visitors to our site.
- 7.2 Where a suspicion of misconduct arises and at the formal request of the investigation officer or HR/ MD the Facilities and Compliance Manager may provide access to CCTV images. Any request will be recorded, clearly stating the reason and date of the request and will be stored in the individuals' personnel file.
- 7.3 Requests by individual data subjects for images relating to themselves should be made via the Company's dedicated request form *Site - CCTV Subject Access Request*, available on the GIN. The Company will process any such request in line with the relevant law adopted by the UK at that point in time.
- 7.4 Where the company is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the identifiable individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.
- 7.5 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 of crime or to assist government bodies in formal investigations, or in other circumstances where an exemption applies under relevant legislation. Such disclosures will be authorised by the Managing Director.

8. Retention of images

- 8.1 Data obtained from the CCTV cameras located on site will be retained for 30 days before being automatically overwritten. Data will be retained for longer periods where it is required for the investigation of or as evidence during any formal process, such as disciplinary, grievance or criminal matter. Where data has been retained due to an Employee Relations concern, where a sanction has been issued, evidence will be retained in line with the Retention Policy for Employee Information and Data Protection Policy.
- 8.2 Any further installation of CCTV equipment will be subject to a Privacy Impact Assessment.

9. Documentation & Review

- 9.1 All documentation referred to in this policy can be found on GIN. The Facilities and Compliance Manager will review the policy annually to ensure the purpose still applies. The system will be reviewed annually to ensure that the system remains necessary, proportionate and effective in meeting its stated purpose.

10. Feedback

- 10.1 Any concerns or complaints over the use of Geberit’s CCTV system should be addressed to louise.rigden@geberit.com.

Document Name	Version/Issue Date	Change
CCTV Policy	October 2023	Policy reviewed and small updates made, checking alignment to laws and best practice. Included within this policy that CCTV can be used as evidence in disciplinary proceedings. Introduced Subject Access Request form and information on auditing security and access to the system