CCTV Camera Surveillance Policy

Why is this a topic for Van Loon Group?

Within the Van Loon Group locations, cameras are used for the security of people, buildings, the grounds, affairs and production processes. This is done in the areas of property law, food safety (food defence), process optimisation and occupational safety.
Because this camera footage is stored, it has an impact on the privacy of our employees and other persons operating in our buildings and grounds. With this policy, Van Loon Group wants to clearly indicate how they deal with this.

Scope

Use, storage and processing of CCTV footage at Van Loon Group sites.

Ambition

Van Loon Group is committed to ensuring that the processing of CCTV footage is done in the proper legal manner.

1. General

1.1. Van Loon Group believes that CCTV systems and other surveillance systems play a legitimate role in helping maintain a safe environment for all our employees and visitors. We realise that this may raise concerns about the privacy of individuals. The images recorded by surveillance systems are personal data that must be handled in accordance with the requirements of applicable laws and regulations, in particular the General Data Protection Regulation 2016/679 (GDPR) and the Dutch Personal Data Protection Act (PDPA).

1.2. This policy describes Van Loon Group's use of camera surveillance and the precautions taken by Van Loon Group to protect the personal data, privacy and other fundamental rights of those seen in the footage. We make every effort to comply with our legal obligations, and to ensure that the legal rights of our employees and visitors with respect to their personal data are recognised and respected.

1.3. This policy applies to all employees and flex workers of Van Loon Group, as well as visitors to the sites, including subcontractors, suppliers and self-employed persons.

1.4. A violation of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a violation of this policy may be considered misconduct resulting in disciplinary action, including dismissal.

2. Definitions

2.1. For the purposes of this policy, the following definitions are explained in more detail:

CCTV (Closed Circuit TeleVision): This means that there is an image connection over a closed circuit and/or network.
As a result, the recorded and captured camera footage is not publicly broadcast, nor can it be received.

Data: Information stored electronically or in certain paper filing systems. Regarding camera surveillance, this generally means video footage. It may also contain static images, such as printed screenshots.

People concerned: All persons about whom we have personal information as a result of using CCTV or other surveillance systems.

Personal data: Data relating to an individual who can be identified from that data (or other data in our possession). This data also includes video footage of individuals

Processing manager: Individuals or organisations who determine the manner in which personal data is processed. They are responsible for establishing procedures and policies so that the company is compliant with laws and regulations.

Data users: Employees whose work involves the processing of personal data. This includes operating CCTV cameras and other surveillance systems and recording, monitoring, storing, retrieving and deleting camera footage. Data users must protect the data they process in accordance with this policy.

Data processors: Individuals or organisations who are not data users (or employees of a processing manager), but who process data on our behalf and in accordance with our instructions (for example, a supplier who processes camera footage on our behalf).

Processing: Any activity that involves the use of data. This includes obtaining, recording or storing data, or performing any operation on the data, including organising, modifying, retrieving, using, disclosing or destroying it. Processing also includes the transfer of personal data to third parties.

Surveillance systems: Any device or system designed to monitor or record footage of people. The term includes CCTV systems as well as all technologies that may be introduced in the future, such as automatic license plate recognition, body-worn cameras, drones and other systems that capture information from individuals, or that capture information related to identification of individuals.

3. Responsible employees

3.1. The Executive Board has overall responsibility for compliance with relevant legislation and the effective implementation of this policy.
The day-to-day responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed is delegated to the Managing Directors of the operating companies.
Daily operational responsibility for CCTV cameras and storage of recorded data is the responsibility of the Site Manager.

3.2. The Data Protection Officer is responsible for keeping this policy up to date.

4. Reasons for using CCTV

4.1. The purpose of camera surveillance is to secure people, buildings, premises, affairs and production processes, both in terms of property rights, food safety (food defence), process optimisation and occupational safety. Specifically, this includes:

a) Protecting buildings and affairs from damage, disruption, vandalism and other crimes;
b) Monitoring the personal safety of employees and visitors;
c) Supporting judicial authorities in the prevention, detection and prosecution of crimes;
d) Assisting in the resolution of disciplinary or employment disputes or complaints;

This list is not exhaustive and other purposes may be, or may become relevant.

5. Supervision

5.1. The CCTV system monitors and continuously records all relevant areas on the inside and outside of our buildings and grounds 24 hours a day.

5.2. Camera locations are chosen so that surveillance of irrelevant areas is minimised. As far as practical, CCTV cameras will not focus on private homes, gardens, or other private areas.

5.3. Verification of footage is performed by authorised personnel Staff using surveillance systems receive appropriate training to ensure that they understand and take into account the legal requirements relating to the processing of relevant data.

6. Handling the CCTV system

6.1. Where CCTV cameras are placed in the workplace, we will use signs to clearly indicate that camera surveillance is taking place.

6.2. Live feeds from CCTV cameras are monitored only when necessary, such as for access control, or to protect the health and safety of employees.

6.3. We will ensure that live feeds from cameras and recorded footage are viewed only by employees whose position requires them to have access to this data. This may include HR personnel involved in disciplinary matters or complaints.

7. Use of data collected by CCTV

7.1. To ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data collected from CCTV cameras is stored in a manner that safeguards integrity and security. This applies to both on-premises servers and cloud computing systems.

7.2. We may engage data processors to process data on our behalf. In this case, clear agreements will be made, and safeguards put in place to protect the security and integrity of the data.

8. Storage and deleting of data collected by CCTV

8.1. Data recorded by the CCTV system is stored. Data from CCTV cameras is not kept indefinitely but is permanently deleted once there is no longer any reason to keep the recorded information. Footage will not be retained for more than 30 days.

8.2. After footage is no longer usable, all footage stored in any format is permanently and securely erased. All physical items, such as tapes or disks, are discarded as confidential waste. Any still images and prints are disposed of as confidential waste.

9. Extension of surveillance systems

9.1. Prior to the introduction of a new surveillance system, including the installation of a new CCTV camera, a Data Protection Impact Assessment (DPIA) is carried out.

9.2. A DPIA is intended to help us decide whether new surveillance cameras are necessary and proportionate given the circumstances, whether they should be used at all, and whether restrictions should be placed on their use.

9.3. Each DPIA will take into account the nature of the problem we are trying to address at the time, whether the surveillance camera is an effective solution, and whether there is a better solution.

9.4. No surveillance cameras will be placed in areas where privacy is expected (e.g., locker rooms) unless, in very exceptional circumstances, it is deemed necessary by us.

9.5. Each DPIA shall be submitted to the Joint Works Council for approval.

10. Hidden surveillance

10.1. We will never conduct covert surveillance (i.e., when individuals do not know that surveillance is taking place) unless, in very exceptional circumstances, there are reasonable grounds to suspect criminal activity or very serious malpractices. In these cases, we will always coordinate this in advance with the Joint Works Council.

10.2. In the event that covert surveillance is deemed justified, it will only be carried out with the express consent of the Data Protection Officer. The decision to conduct covert surveillance will be fully documented, and it will be recorded how and by whom the decision to use covert resources was made. The risk of invading the privacy of innocent employees will always be a primary consideration when making such a decision. Only a limited number of people will be involved in hidden surveillance.

10.3. Hidden surveillance will only be conducted for a limited and reasonable period of time consistent with the purposes of making the recording, and will only relate to the specific suspected illegal or unauthorised activity.

11. Ongoing assessment of using CCTV

11.1. We will ensure that the ongoing use of existing CCTV cameras in the workplace is periodically reviewed to ensure that their use remains necessary and appropriate, and that each surveillance system continues to meet the needs that justified its introduction.

Requests for disclosure of footage

11.2. We may share data with, for example, other operating companies or organisations, where we believe it is reasonably necessary to do so for one of the legitimate purposes set out in paragraph 4.1.

11.3. No images from our CCTV cameras will be released to third parties without the express permission of the Data Protection Officer. Data will not normally be released unless there is sufficient evidence that it is required for legal proceedings, or must be produced pursuant to a court order.

11.4. In other applicable circumstances, we may permit the judicial authorities to view or remove CCTV footage where required in the investigation or prosecution of criminal offenses.

11.5. We keep a record of all disclosures of CCTV footage.

11.6. CCTV footage will never be posted online or made public to the media.

12. Access requests by concerned parties

12.1. Concerned parties may request the release of their personal information. A request for inspection by a concerned party is subject to legal requirements, and must be made in writing.

12.2. In order to locate relevant footage, all requests for copies of recorded CCTV footage should include the following: date and time of the recording, the location where the footage was taken and, if necessary, information related to identifying the individual.

12.3. We reserve the right to make images of third-parties unreadable when they are released as part of an access request.

13. Complaints

13.1. If an employee has questions regarding this policy, or concerns about our use of CCTV, they should first contact their supervisor or the Data Protection Officer.

13.2. Where this is not appropriate, or matters cannot be resolved informally, employees should follow our formal complaints procedure.

.

Signed by Van Loon Group

Name: Robert van Ballegooijen
Position: CEO Van Loon Group
Date: 06-06-2024