CCTV Camera Surveillance - Policy

Why is this a theme for Van Loon Group?

Within Van Loon Group locations, cameras are used for the security of people, buildings, grounds, assets, and production processes. This is done in the areas of property rights, food safety (food defense), process optimization, and occupational safety.

Since these camera images are stored, this has an impact on the privacy of our employees and other persons active in our buildings and on our premises.

With this policy, Van Loon Group wants to clearly indicate how it deals with this.

Scope

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

Our policy

Van Loon Group strives to ensure that the processing of CCTV images takes place in the correct legal manner.

1. General

1.1. Van Loon Group believes that CCTV systems and other surveillance systems play a legitimate role in helping to maintain a safe environment for all our employees and visitors. We realize that this may raise concerns regarding the privacy of individuals. 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 Data Protection Act (Wbp).

1.2. This policy describes the use of camera surveillance by Van Loon Group, as well as the precautions taken by Van Loon Group to protect the personal data, privacy, and other fundamental rights of those visible in the images. We make every effort to comply with our legal obligations and to ensure that the legal rights of our employees and visitors regarding their personal data are acknowledged and respected.

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

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

2. Definitions

2.1. For the purposes of this policy, the definitions below are further explained:

CCTV (Closed Circuit Television): This means that there is a video connection over a closed circuit and/or network. This implies that the recorded and captured camera images are not broadcast publicly and cannot be received.

Data: information stored electronically or in certain paper archiving systems. With regard to camera surveillance, this generally means video images. It may also include static images, such as printed screenshots.

Data subjects: all persons about whom we hold personal information as a result of the use of CCTV or other surveillance systems.

Personal data: data relating to a person who can be identified on the basis of that data (or other data in our possession). This data also includes video images of persons.

Controllers: persons or organisations that determine how personal data is processed. They are responsible for establishing procedures and policies to ensure 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: persons or organizations who are not data users (or employees of a controller) 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 involving the use of data. It includes obtaining, recording, or storing data or performing any operation on the data, including organizing, modifying, retrieving, using, disclosing, or destroying. Processing also includes the transfer of personal data to third parties.

Surveillance systems: all devices or systems designed to monitor or record images of persons. The term includes both CCTV systems and all technologies that may be introduced in the future, such as automatic license plate recognition, body cameras, drones, and other systems that capture information about persons or record information relating to the identification of persons.

3. Responsible employees

3.1. The Executive Board has overall responsibility for compliance with the relevant legislation and the effective implementation of this policy.
The day-to-day responsibility to decide which 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 the storage of recorded data is the responsibility of the Location Manager.

3.2. The Data Protection Officer is responsible for the current
like this policy.

4. Reasons for the use of CCTV

4.1. The purpose of the camera surveillance is the security of persons, buildings, premises, property, and production processes, regarding property rights, food safety (food defense), process optimization, and occupational safety. Specifically, this includes:

a) Protect buildings and property against damage, disruption, vandalism and others crimes;

b) Monitoring the personal safety of employees and visitors;

c) Assisting the justice system in the prevention, detection and prosecution of crimes;

d) Assisting in the settlement of disciplinary or employment disputes or complaints; This list is not exhaustive and other purposes may be or become relevant.

5. Supervision

5.1. The CCTV system monitors all relevant areas inside and outside our buildings and grounds 24 hours a day, and the data is continuously recorded.

5.2. Camera locations have been chosen so that surveillance of irrelevant areas is minimized. As far as practically possible, CCTV cameras will not focus on private homes, gardens, or other private property.

5.3. The verification of the images is carried out by authorized personnel.

5.4. Personnel using surveillance systems receive appropriate training to ensure that they understand and take into account the legal requirements regarding the processing of relevant data.

6. Handling the CCTV system

6.1. We will clearly indicate where CCTV cameras are placed in the workplace.
by means of signs indicating that camera surveillance is taking place.

6.2. Live feeds from CCTV cameras are only monitored if necessary,
for example, 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 only
are viewed by employees whose position requires them to have access to this data. This may include HR personnel involved in disciplinary or complaint matters.

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 guarantees integrity and security. This applies to both on-premise servers and cloud computing systems.

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

8. Storage and deletion of data collected by CCTV

8.1. Data recorded by the CCTV system is stored. Data from CCTV cameras is not retained indefinitely but is permanently deleted as soon as there is no longer a reason to retain the recorded information.

Images will not be stored for longer than 30 days.

8.2. Once images are no longer usable, all images stored in any format will be permanently and securely deleted. All physical items, such as tapes or discs, will be disposed of as confidential waste. Any still images and printed prints will be disposed of as confidential waste.

9. Extensions to surveillance systems

9.1. Prior to the introduction of a new surveillance system, including the When installing a new CCTV camera, a Data Protection Impact Assessment (DPIA) is conducted.

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

9.4. No surveillance cameras will be installed in areas where privacy is expected (for example, in changing rooms) unless in very exceptional circumstances, where we deem it necessary.

9.5. Every DPIA is submitted to the Joint for approval. Works Council

10. Covert surveillance

10.1. We will never conduct covert surveillance (that is to say, when persons are unaware that surveillance is taking place), unless in very exceptional circumstances there are reasonable grounds to suspect criminal activity or very serious malversations. In these cases, we will always consult with the Joint Works Council in advance.

10.2. In the event that covert surveillance is deemed justified, it shall only be carried out with the express consent of the Data Protection Officer. The decision to carry out covert surveillance shall be fully documented, and it shall be recorded how and by whom the decision to deploy covert means was taken. The risk of infringement of the privacy of innocent employees shall always be a primary consideration when making such a decision.

10.3. Only a limited number of people will be involved in covert surveillance.

10.4. Covert surveillance shall only be conducted for a limited and reasonable period in accordance with the purposes of making the recording and shall only relate to the specific suspected illegal or unauthorized activity.

11. Ongoing assessment of the use of CCTV

11.1. We will ensure that the continued 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 images

11.2. We may share data with, for example, other operating companies or organizations where we believe that this is reasonably necessary for one of the legitimate purposes set out in paragraph 4.1.

11.3. No footage from our CCTV cameras will be released to third parties without the express permission of the Officer for

Data protection. Data is normally not disclosed unless there is sufficient evidence that this is required for legal proceedings or must be submitted pursuant to a court order.

11.4. In other applicable circumstances, we may allow the Public Prosecution Service to view or delete CCTV footage where required for the investigation or prosecution of criminal offences.

11.5. We maintain a register 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 data subjects

12.1. Data subjects may submit a request to disclose their personal information. A request for access by a data subject is subject to statutory conditions and must be made in writing.

12.2. In order to locate relevant footage, all requests for copies of recorded CCTV footage must contain the following: the date and time of the recording, the location where the footage was taken and, if necessary, information regarding the identification of the individual.

12.3. We reserve the right to obscure third-party images when releasing them as part of an access request.

13. Complaints

13.1. If an employee has questions about 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 must follow our formal complaints procedure.

.

Signed for Van Loon Group

Name: Robert van Ballegooijen

Function: CEO

Date: 7-5-2026

DocuSigned by:

A266BC0366F0401...