10 Richtlijn: Protocol cameratoezicht

10.1 Doel protocol:

In dit protocol worden de afspraken met betrekking tot de omgang met cameratoezicht binnen thyssenkrupp Materials Nederland B.V. weergegeven. Deze afspraken zorgen ervoor dat er conform Algemene Verordening Gegevensbescherming (AVG) en de voorwaarden van de Autoriteit Persoonsgegevens (AP) wordt gehandeld. De hieronder vernoemde richtlijn is van toepassing op werknemers en toegelaten externe natuurlijke personen, welke zich op of binnen (al dan niet in eigendom), thyssenkrupp Materials Nederland B.V. locaties bevinden. Deze richtlijn treedt per 1 september 2025 in werking. Per datum ingang vervallen hiermee alle voorgaande richtlijnen en regelingen betreffende protocol cameratoezicht.

10.2 Algemeen:

Cameratoezicht binnen thyssenkrupp Materials Nederland B.V. wordt niet gebruikt om eigen medewerkers te controleren op aanwezigheid en/of prestaties. Derhalve wordt in alle gevallen bij cameratoezicht gebruik gemaakt van zichtbaar opgehangen camera's.

Echter, in geval van vermogensdelicten als diefstal, fraude of verduistering en andere criminele handelingen (waaronder vernieling e.d.) kan er besloten worden om in het kader van het gerechtvaardigd belang, onder bepaalde voorwaarden, conform artikel 139f van het Wetboek van Strafrecht, heimelijk cameratoezicht toe te passen.

10.3 Doel cameratoezicht:

A. verhogen veiligheid en gezondheid van onze werknemers en toegelaten externe natuurlijke personen welke zich op of binnen onze (al dan niet in eigendom) locaties bevinden tegen o.a. mogelijke bedreigingen zoals geweld, andere criminele activiteiten en ongeoorloofde of ongewenste activiteiten;
B. voorkomen van diefstal, fraude, verduistering en andere vermogensdelicten, waaronder vernieling, etc.;
C. bescherming van onze bedrijfseigendommen tegen beschadiging, diefstal, vandalisme en calamiteiten (o.a. brandbeveiliging);
D. bewaking van de procesflow (machines in werking zonder toezicht);
E. kwaliteit- en kwantiteitscontrole bij ingaande en uitgaande goederenstromen. (eventuele bewijslast richting derden);
F. ondersteuning bij incidentonderzoek op de werkvloer, zoals ongelukken, onveilige situaties, conflicten of calamiteiten, alsmede gebruik voor trainingsdoeleinden ter bevordering van de veiligheid.

10.3.1 Verwerking cameratoezicht:

In het kader van deze verwerking worden mogelijk gegevens verwerkt van personen waarvan opnamen gemaakt zijn als gevolg van:

- Voor doel A: gerichte opnamen van de toegangsmogelijkheden tot gebouwen, terreinen en de magazijnhallen, voor zover noodzakelijk voor het doel, alsmede gerichte opnamen van betrokken persoon of personen, voor zover noodzakelijk voor het doel;
- Voor doel B: gerichte opnamen van zaken die zich in gebouwen of op terreinen bevinden, voor zover noodzakelijk voor het doel;
- Voor doel C: gerichte opnamen van bedrijfseigendom, terreinen en potentiële brand oorzakelijke hotspots, voor zover noodzakelijk voor het doel;
- Voor doel D: gerichte opnamen van machines, voor zover noodzakelijk voor het doel;

- Voor doel E: gerichte opnamen van ontlading en belading van vrachtwagens, voor zover noodzakelijk voor het doel;
- Voor doel F: alle beschikbare opnamen betreffende incidenten, voor zover noodzakelijk voor het doel.

10.4 Kenbaar maken van cameratoezicht:

Conform wet- en regelgeving zijn alle ingangen van thyssenkrupp Materials Nederland B.V. locaties voorzien van stickers of borden met daarop de tekst en een pictogram “camerabewaking”.

10.5 Beveiliging van data:

Data (beeldopnames) worden online verstuurd vanuit het beveiligde tk netwerk (waarbinnen via separaat VLAN) versleuteld naar een certificeerde service provider in de Cloud. Wettelijke data bewaartermijnen worden aldaar bewaakt.

10.6 Toegang tot data en autorisatieniveaus:

Er zijn twee soorten toegang tot de data te onderscheiden:

1. Systeemgebruikers: Dit zijn werkplekken waarop aldaar benodigde data live gestreamd wordt. (bijvoorbeeld werkplekken waar toegang tot onze locaties moet worden verleend). Deze systeemgebruikers worden door de systembeheerder naar behoefte geautoriseerd voor live data streams van individuele camera’s. Systeemgebruikers hebben geen toegang tot historische data. Toegang wordt verleend via separaat geconfigureerde fysieke hardware.
2. Individuele gebruikers: dit zijn individuele gebruikers die door de systeembeheerder worden geautoriseerd op: toegang per individuele camera, en daarbinnen op: live streaming ja/nee, bekijken historische data ja/nee, mogelijkheid tot downloaden data ja/nee en maximale tijdsduur toegang systeem. Deze gebruikers beschikken over een persoonlijk gebruikers ID en wachtwoord.

De systeembeheerder is een lid van de directie van thyssenkrupp Materials Nederland B.V.
Wijzigen, verwijderen of toevoegen van formeel geautoriseerde functionarissen, alsmede bijbehorende autorisaties worden door de directie met motivatie aan de OR gecommuniceerd. Formeel geautoriseerde functionarissen kunnen zich in voorkomende gevallen door anderen hierbij laten bijstaan, mits dit met toestemming van de directie geschiedt. Ter voorkoming en bewaking van onnodige toegang wordt elke toegang en actie van de systeembeheerder en door hem formeel geautoriseerde functionarissen door het systeem gelogd.

10.7 Bewaking van zichtlijnen:

De OR zal één persoon binnen haar leden aanwijzen die geautoriseerd wordt om periodiek de camerazichtlijnen te kunnen verifiëren, ter waarborging van de gemaakte afspraken.

10.8 Overdracht van data intern binnen de organisatie:

Data kan ten hoogste worden verstrekt aan de volgende functionarissen, en allen voor zover strikt noodzakelijk voor de onderscheiden doelen binnen de organisatie, zoals vermeld in paragraaf 10.3.1. aan:

- die functionarissen, die belast zijn met of leiding geven aan de in artikel 10.3.1 bedoelde activiteiten of daarbij zijn betrokken;
- de leidinggevende van de betrokkene(n);
- de directie;
- de betrokkene(n);

10.9 Overdracht van data buiten de organisatie (derden):

Data kan ten hoogste worden verstrekt aan de volgende instanties of rechtspersonen echter enkel en alleen binnen de Europese Unie:

- externe service provider voor data opslag (Data beheerder);
- politieambtenaren;
- justitie en gerechtelijke autoriteiten;
- andere ambtenaren en/of functionarissen die als bevoegd gezag kunnen worden beschouwd en uit dien hoofde kennis mogen nemen van de gegevens;
- advocaten en verzekeringsmaatschappijen in dienst van thyssenkrupp Materials Nederland B.V.;
- klanten en/of leveranciers, enkel in het kader van bewijslast;
- moederconcern, enkel in het kader van ongeval analyses.

Het overdragen van data aan derden is enkel en alleen ter discretie van de directie. De directie zal van geval tot geval beoordelen of overdracht gerechtvaardigd en/of geoorloofd is. Dit ter bescherming van de organisatie en haar medewerkers. Waar nodig zal zij zich juridisch laten bijstaan en/of data anonimiseren en/of individuele werknemers om toestemming verzoeken.

10.10 Bijzonderheden:

In het geval dat geconstateerde incidenten leiden tot sancties tegen een medewerker, dan zal de betreffende medewerker de gelegenheid geboden worden om de beelden die hebben geleid tot deze sanctie in te zien.

Overige actuele informatie

Aantal camera's geïnstalleerd:	Locatie Veghel Locatie Zwijndrecht	36 25
Externe Service provider:	Eagle Eye Networks	
Privacy en GDPR (AVG) policy externe service provider:	https://www.een.com/privacy-policy/ https://www.een.com/blog/seven-ways-eagle-eye-networks-supports-organizations-with-gdpr/	
Bewaartermijn data:	7 dagen	
Technisch onderhoud camera's:	Van der Linden, Eisenhowerweg 39, 5466 AB Veghel	
Systeembeheerder:	Lid directie	
Systeemgebruikers:	Receptie balie, locatie Veghel	
Autorisatie systeem gebruikers:	Via geconfigureerde hardware, Live stream (24 uur).	
Individuele gebruikers:	Manager Logistiek Medewerker Technische Dienst	
Autorisaties individuele gebruikers:	Alle camera's: Live stream (max 30 minuten), bekijken historische data, mogelijkheid tot downloaden maximale tijdsduur per dag toegang systeem: 24 uur.	

10 Guideline: CCTV Surveillance Protocol

10.1 Purpose of the protocol:

This protocol sets out the agreements regarding the use of CCTV surveillance within thyssenkrupp Materials Nederland B.V. These agreements ensure that actions are taken in accordance with the General Data Protection Regulation (GDPR) and the requirements of the Dutch Data Protection Authority (AP). The policy set out below applies to employees and authorised external individuals who are present on or within (whether owned or not) thyssenkrupp Materials Nederland B.V. locations. This policy comes into effect on 1 September 2025. Upon this date, all previous policies and regulations concerning the CCTV Surveillance Protocol will cease to apply.

10.2 General:

CCTV surveillance within thyssenkrupp Materials Nederland B.V. is not used to monitor the presence and/or performance of its own employees. Consequently, in all cases where CCTV surveillance is used, cameras are mounted in a visible manner.

However, in the event of property offences such as theft, fraud or embezzlement and other criminal acts (including vandalism, etc.), it may be decided, in the context of legitimate interest and subject to certain conditions, to use covert CCTV surveillance in accordance with Section 139f of the Criminal Code.

10.3 Purpose of CCTV surveillance:

A. to enhance the safety and health of our employees and authorised external individuals who are on or within our premises (whether owned by us or not) against, amongst other things, potential threats such as violence, other criminal activities and unauthorised or undesirable activities;
B. to prevent theft, fraud, embezzlement and other property offences, including vandalism, etc.;
C. to protect our company property against damage, theft, vandalism and emergencies (including fire safety);
D. monitoring of the process flow (machines operating without supervision);
E. quality and quantity control of incoming and outgoing goods flows (potential burden of proof vis-à-vis third parties);
F. support for incident investigations in the workplace, such as accidents, unsafe situations, conflicts or emergencies, as well as use for training purposes to promote safety.

10.3.1 Processing of CCTV footage:

In the context of this processing, data may be processed relating to individuals who have been recorded as a result of:

- For purpose A: targeted recordings of access points to buildings, premises and warehouse halls, to the extent necessary for the purpose, as well as targeted recordings of the person or persons concerned, to the extent necessary for the purpose;
- For purpose B: targeted recordings of items located in buildings or on premises, to the extent necessary for the purpose;
- For purpose C: targeted recordings of company property, premises and potential fire-causing hotspots, to the extent necessary for the purpose;
- For purpose D: targeted images of machinery, to the extent necessary for the purpose;
- For purpose E: targeted footage of the unloading and loading of lorries, to the extent necessary for the purpose;
- For purpose F: all available footage relating to incidents, to the extent necessary for the purpose.

10.4 Notification of CCTV surveillance:

In accordance with legislation and regulations, all entrances to thyssenkrupp Materials Nederland B.V. locations are fitted with stickers or signs bearing the text and a 'CCTV' pictogram.

10.5 Data security:

Data (video recordings) are transmitted online from the secure tk network (within which a separate VLAN is used) in encrypted form to a certified service provider in the Cloud. Statutory data retention periods are observed there.

10.6 Access to data and authorisation levels:

There are two distinct types of access to the data:

1. System users: These are workstations where the necessary data is streamed live. (For example, workstations where access to our sites must be granted.) These system users are authorised by the system administrator as required for live data streams from individual cameras. System users do not have access to historical data. Access is granted via separately configured physical hardware.
2. Individual users: these are individual users authorised by the system administrator for: access per individual camera, and within that: live streaming yes/no, viewing historical data yes/no, ability to download data yes/no, and maximum duration of system access. These users have a personal user ID and password.

The system administrator is a member of the management board of thyssenkrupp Materials Nederland B.V. Changes to, removal of, or addition of formally authorised officers, as well as associated authorisations, are communicated by the management to the Works Council with justification. Formally authorised officers may, where necessary, be assisted in this by others, provided this is done with the consent of the management. To prevent and monitor unauthorised access, every access and action by the system administrator and by officials formally authorised by him is logged by the system.

10.7 Monitoring of sightlines:

The Works Council shall designate one person from among its members who is authorised to periodically verify the camera sightlines, in order to ensure compliance with the agreements made.

10.8 Transfer of data internally within the organisation:

Data may be provided to the following officials at most, and only to the extent strictly necessary for the respective purposes within the organisation, as stated in paragraph 10.3.1:

- those officials who are responsible for or manage the activities referred to in Article 10.3.1 or are involved in them;
- the supervisor of the data subject(s);
- the management;
- the data subject(s);

10.9 Transfer of data outside the organisation (third parties):

Data may be disclosed to the following bodies or legal entities, but only within the European Union:

- external data storage service provider (Data Controller);
- police officers;
- judicial and legal authorities;
- other officials and/or officers who may be regarded as competent authorities and who, in that capacity, are authorised to access the data;
- solicitors and insurance companies acting on behalf of thyssenkrupp Materials Nederland B.V.;
- customers and/or suppliers, solely in the context of the burden of proof;
- the parent company, solely in the context of accident analyses.

The transfer of data to third parties is solely at the discretion of the management. The management will assess on a case-by-case basis whether such transfer is justified and/or permissible. This is to protect the organisation and its employees. Where necessary, it will seek legal advice and/or anonymise data and/or request consent from individual employees.

10.10 Details:

In the event that identified incidents lead to sanctions against an employee, the employee in question will be given the opportunity to view the footage that led to this sanction.

Other current information

Number of cameras installed:	Location: Veghel Location: Zwijndrecht	36 25
External service provider:	Eagle Eye Networks	
External service provider's privacy and GDPR (AVG) policy:	https://www.een.com/privacy-policy/ https://www.een.com/blog/seven-ways-eagle-eye-networks-supports-organizations-with-gdpr/	
Data retention period:	7 days	
Technical maintenance of cameras:	Van der Linden, Eisenhowerweg 39, 5466 AB Veghel	
System administrator:	Member of the management board	
System users:	Reception desk, location Veghel	
System user authorisation:	Via configured hardware, Live stream (24 hours).	
Individual users:	Logistics Manager Technical Services Staff	
Individual user authorisations:	All cameras: Live stream (max. 30 minutes), view historical data, option to download; maximum daily system access duration: 24 hours.	