

CCTV Cameratoezicht Beleid

Waarom is dit een thema voor Van Loon Group?

Binnen de locaties van Van Loon Group worden camera's gebruikt voor de beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen. Dit gebeurt op het gebied van eigendomsrecht, voedselveiligheid (fooddefense), procesoptimalisatie en arbeidsveiligheid. Aangezien deze camerabeelden opgeslagen worden, heeft dit impact op de privacy van onze medewerkers en andere personen die in onze gebouwen en op terreinen actief zijn. Met dit beleid wil Van Loon Group duidelijk aangeven hoe zij met hier mee omgaat.

Afbakening

Gebruik, opslag en verwerking van CCTV-beelden op de locaties van Van Loon Group.

Ambitie

Van Loon Group streeft ernaar dat de verwerking van CCTV-beelden op de juiste wettelijke manier plaatsvindt.

1. Algemeen

- 1.1. Van Loon Group is van mening dat CCTV-systemen en andere surveillancesystemen een legitieme rol spelen bij het helpen handhaven van een veilige omgeving voor al onze medewerkers en bezoekers. We realiseren ons dat dit tot bezorgdheid kan leiden over de privacy van personen. Beelden geregistreerd door surveillancesystemen zijn persoonsgegevens waar mee om moet worden gegaan in overeenstemming met de vereisten van toepasselijke wet- en regelgeving, met name de algemene verordening gegevensbescherming 2016/679 ("AVG") en de Wet bescherming persoonsgegevens (Wbp).
- 1.2. In dit beleid wordt het gebruik van cameratoezicht door Van Loon Group beschreven, alsmede de door Van Loon Group genomen voorzorgsmaatregelen ter bescherming van de persoonsgegevens, privacy en andere grondrechten van diegenen die op de beelden te zien zijn. We doen er alles aan om te voldoen aan onze wettelijke verplichtingen en ervoor te zorgen dat de wettelijke rechten van onze medewerkers en bezoekers met betrekking tot hun persoonlijke gegevens, worden erkend en gerespecteerd.
- 1.3. Dit beleid is van toepassing op alle medewerkers en flexmedewerkers van Van Loon Group alsmede bezoekers van de locaties waaronder onderaannemers, leveranciers en ZZP'ers.
- 1.4. Een overtreding van dit beleid kan, in passende omstandigheden, worden behandeld als een disciplinaire kwestie. Volgend op onderzoek kan een overtreding van dit beleid worden beschouwd als wangedrag dat leidt tot disciplinaire maatregelen waaronder ontslag.

2. Definities

- 2.1. Ten behoeve van dit beleid worden onderstaande definities nader toegelicht:

CCTV (Closed Circuit TeleVision): Dit betekent dat er beeldverbinding is over een gesloten circuit en/of netwerk. Hiermee wordt bedoeld dat de opgenomen en vastgelegde camerabeelden niet publiekelijk uitgezonden worden en ook niet te ontvangen zijn.

Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 1 van 6

Data: informatie die elektronisch of in bepaalde papieren archiefsystemen wordt opgeslagen. Met betrekking tot cameratoezicht betekent dit over het algemeen videobeelden. Het kan ook statische afbeeldingen bevatten, zoals afgedrukte schermafbeeldingen.

Betrokkenen: alle personen over wie we persoonlijke informatie hebben als gevolg van gebruik van CCTV of andere bewakingssystemen.

Persoonsgegevens: gegevens met betrekking tot een persoon die aan de hand van die gegevens (of andere gegevens in ons bezit) kan worden geïdentificeerd. Deze gegevens omvat eveneens videobeelden van personen.

Verwerkingsverantwoordelijken: personen of organisaties die bepalen op welke wijze persoonlijke gegevens worden verwerkt. Zij zijn verantwoordelijk voor het vaststellen van procedures en beleid zodat het bedrijf compliant is met wet- en regelgeving.

Gegevensgebruikers: medewerkers wiens werk de verwerking van persoonsgegevens betreft. Dit omvat het bedienen van CCTV-camera's en andere bewakingssystemen en het opnemen, bewaken, opslaan, terughalen en verwijderen van camerabeelden. Gegevensgebruikers moeten de gegevens die ze verwerken beschermen in overeenstemming met dit beleid.

Gegevensverwerkers: personen of organisaties die geen gegevensgebruiker zijn (of medewerker van een verwerkingsverantwoordelijke) maar die namens ons en in overeenstemming met onze instructies gegevens verwerkt (bijvoorbeeld een leverancier die camerabeelden namens ons verwerkt).

Verwerking: elke activiteit waarbij gegevens worden gebruikt. Het omvat het verkrijgen, vastleggen of bewaren van gegevens of het uitvoeren van enige bewerking op de gegevens, waaronder het organiseren, wijzigen, opvragen, gebruiken, openbaar maken of vernietigen. Onder verwerking wordt ook verstaan het doorgeven van persoonsgegevens aan derden.

Surveillancesystemen: alle apparaten of systemen die zijn ontworpen om beelden van personen te bewaken of op te nemen. De term omvat zowel CCTV-systemen als alle technologieën die mogelijk in de toekomst worden geïntroduceerd zoals automatische kentekenherkenning, camera's op het lichaam, drones en andere systemen die informatie vastleggen van personen of informatie vastleggen met betrekking tot identificatie van personen.

3. Verantwoordelijke medewerkers

3.1. De Executive Board heeft de algehele verantwoordelijkheid voor de naleving van de relevante wetgeving en de effectieve uitvoering van dit beleid.

De dagelijkse verantwoordelijkheid om te beslissen welke informatie wordt geregistreerd, hoe deze zal worden gebruikt en aan wie het kan worden bekendgemaakt, is gedelegeerd aan de Managing Directors van de werkmaatschappijen.

Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 2 van 6

Dagelijkse operationele verantwoordelijkheid voor CCTV-camera's en de opslag van opgenomen gegevens is de verantwoordelijkheid van de Locatiemanager.

- 3.2. De functionaris voor gegevensbescherming is verantwoordelijk voor het actueel houden van dit beleid.

4. Redenen voor het gebruik van CCTV

- 4.1. Doel van het cameratoezicht is beveiliging van personen, gebouwen, terreinen, zaken en productieprocessen, zowel op gebied van eigendomsrecht, voedselveiligheid (fooddefense), procesoptimalisatie als arbeidsveiligheid. Specifiek valt daaronder:
- Gebouwen en zaken beschermen tegen schade, verstoring, vandalisme en andere misdrijven;
 - Bewaken van de persoonlijke veiligheid van medewerkers en bezoekers;
 - Ondersteunen van justitie bij het voorkomen, opsporen en vervolgen van misdrijven;
 - Helpen bij het beslechten van disciplinaire of arbeidsrechtelijke geschillen of klachten;
- Deze lijst is niet uitputtend en andere doeleinden kunnen relevant zijn of worden.

5. Toezicht

- 5.1. Het CCTV-systeem bewaakt alle relevante ruimtes aan de binnen- en buitenzijde van onze gebouwen en terreinen 24 uur per dag en de gegevens worden continu vastgelegd.
- 5.2. Cameralocaties zijn zo gekozen dat toezicht op niet relevante ruimtes geminimaliseerd wordt. Voor zover praktisch mogelijk, zullen CCTV-camera's zich niet concentreren op particuliere huizen, tuinen of andere privéterreinen.
- 5.3. Controle van de beelden wordt uitgevoerd door bevoegd personeel.
- 5.4. Personeel dat surveillancesystemen gebruikt, krijgt passende training om ervoor te zorgen dat ze de wettelijke vereisten met betrekking tot de verwerking van relevante gegevens begrijpen en hiermee rekening houden.

6. Omgang met CCTV-systeem

- 6.1. Waar CCTV-camera's op de werkplek worden geplaatst, zullen we duidelijk aangeven middels borden dat cameratoezicht plaatsvindt.
- 6.2. Live feeds van CCTV-camera's worden alleen gecontroleerd als dit noodzakelijk is, bijvoorbeeld voor toegangscontrole of om de gezondheid en veiligheid van medewerkers te beschermen.
- 6.3. We zullen ervoor zorgen dat live feeds van camera's en opgenomen beelden alleen worden bekeken door medewerkers wiens functie vereist dat zij toegang hebben tot deze gegevens. Dit kan onder meer HR-personeel zijn dat betrokken is bij disciplinaire of klachtenkwesties.

7. Gebruik van door CCTV verzamelde gegevens

- 7.1. Om ervoor te zorgen dat de rechten van personen die door het CCTV-systeem zijn geregistreerd, worden beschermd, zullen we ervoor zorgen dat gegevens die zijn verzameld van CCTV-camera's worden opgeslagen op een manier die de integriteit en veiligheid garandeert. Dit geldt zowel voor on-premise servers als voor cloud computersystemen.
- 7.2. We kunnen gegevensverwerkers inschakelen om namens ons gegevens te verwerken. In dat geval zullen er duidelijke afspraken gemaakt worden en waarborgen getroffen worden om de veiligheid en integriteit van de gegevens te beschermen.

Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 3 van 6

8. Opslag en wissen van door CCTV verzamelde gegevens

- 8.1. Door het CCTV-systeem geregistreerde gegevens worden opgeslagen. Gegevens van CCTV-camera's worden niet voor onbepaalde tijd bewaard maar worden permanent verwijderd zodra er geen reden meer is om de geregistreerde informatie te bewaren. Beelden zullen niet langer dan 30 dagen worden bewaard.
- 8.2. Nadat beelden niet meer bruikbaar zijn worden alle beeld die in welk formaat dan ook zijn opgeslagen, permanent en veilig gewist. Alle fysieke zaken, zoals banden of schijven, worden als vertrouwelijk afval weggegooid. Eventuele stilstaande foto's en gedrukte afdrukken worden als vertrouwelijk afval weggegooid.

9. Uitbreidingen op surveillancesystemen

- 9.1. Voorafgaand aan de introductie van een nieuw bewakingsstelsel, inclusief het plaatsen van een nieuwe CCTV-camera wordt een Data Protection Impact Assessment (DPIA) uitgevoerd.
- 9.2. Een DPIA is bedoeld om ons te helpen beslissen of nieuwe surveillancecamera's noodzakelijk en proportioneel zijn gezien de omstandigheden, of ze überhaupt moeten worden gebruikt en of er beperkingen moeten worden gesteld aan hun gebruik.
- 9.3. Elke DPIA zal rekening houden met de aard van het probleem dat we op dat moment proberen aan te pakken, of de bewakingscamera een effectieve oplossing is en of er een betere oplossing bestaat.
- 9.4. Er worden geen bewakingscamera's geplaatst in ruimtes waar privacy wordt verwacht (bijvoorbeeld in kleedkamers) tenzij in zeer uitzonderlijke omstandigheden, het door ons noodzakelijk wordt geacht.
- 9.5. Iedere DPIA wordt voorgelegd voor instemming aan de Gemeenschappelijke Ondernemingsraad.

10. Verborgene toezicht

- 10.1. We zullen nooit verborgen toezicht houden (dat wil zeggen, wanneer personen niet weten dat toezicht plaatsvindt), tenzij er in zeer uitzonderlijke omstandigheden redelijke gronden zijn om te vermoeden dat er sprake is van criminele activiteiten of zeer ernstige malversaties. In deze gevallen zullen we dat altijd vooraf afstemmen met de Gemeenschappelijke Ondernemingsraad.
- 10.2. In het geval dat verborgen toezicht gerechtvaardigd wordt geacht, zal deze alleen worden uitgevoerd met de uitdrukkelijke toestemming van de Functionaris voor gegevensbescherming. De beslissing om verborgen toezicht uit te voeren zal volledig worden gedocumenteerd en er zal vastgelegd worden hoe en door wie het besluit om verborgen middelen in te zetten is genomen. Het risico van inbreuk op de privacy van onschuldige werknemers zal altijd een eerste overweging zijn bij het nemen van een dergelijke beslissing.
- 10.3. Slechts een beperkt aantal mensen zal betrokken zijn bij verborgen toezicht.
- 10.4. Verborgene toezicht zal alleen worden uitgevoerd voor een beperkte en redelijke periode in overeenstemming met de doeleinden van het maken van de opname en hebben alleen betrekking op de specifieke vermoedelijke illegale of ongeoorloofde activiteit.

Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 4 van 6

11. Doorlopende beoordeling van het gebruik van CCTV

11.1. We zullen ervoor zorgen dat het doorlopende gebruik van bestaande CCTV-camera's op de werkplek periodiek wordt beoordeeld om ervoor te zorgen dat het gebruik ervan noodzakelijk en gepast blijft, en dat elk bewakingssysteem tegemoet blijft komen aan de behoeften die de invoering ervan rechtvaardigde.

Verzoeken om openbaarmaking van beelden

- 11.2. We kunnen gegevens delen met bijvoorbeeld andere werkmaatschappijen of organisaties waar we van mening zijn dat dit redelijkerwijs noodzakelijk is voor een van de legitieme doeleinden uiteengezet in paragraaf 4.1.
- 11.3. Er zullen geen beelden van onze CCTV-camera's worden vrijgegeven aan derden, zonder dat hiervoor uitdrukkelijke toestemming is gegeven door de Functionaris voor gegevensbescherming. Gegevens worden normaal gesproken niet vrijgegeven tenzij er voldoende bewijs is dat dit vereist is voor een gerechtelijke procedure of op grond van een gerechtelijk bevel moet worden overgelegd.
- 11.4. In andere toepasselijke omstandigheden kunnen we Justitie toestaan CCTV-beelden te bekijken of te verwijderen waar dit vereist is bij de opsporing of vervolging van strafbare feiten.
- 11.5. We houden een register bij van alle openbaarmakingen van CCTV-beelden.
- 11.6. CCTV-beelden zullen nooit online worden geplaatst of openbaar worden gemaakt aan de media.

12. Toegangsverzoeken door betrokkenen

- 12.1. Betrokkenen kunnen een verzoek indienen om hun persoonlijke informatie vrij te geven. Een inzageverzoek van een betrokkene is onderworpen aan de wettelijke voorwaarden en moet schriftelijk worden gedaan.
- 12.2. Om relevante beelden te kunnen lokaliseren, moeten alle verzoeken om kopieën van opgenomen CCTV-beelden het volgende bevatten: datum en tijd van de opname, de locatie waar de beelden zijn gemaakt en, indien nodig, informatie met betrekking tot het identificeren van het individu.
- 12.3. We behouden ons het recht voor om afbeeldingen van derden onleesbaar te maken bij het vrijgeven als onderdeel van een toegangsverzoek.

13. Klachten

- 13.1. Als een medewerker vragen heeft over dit beleid of zich zorgen maakt over ons gebruik van CCTV, dan moeten ze in eerste instantie contact opnemen met hun leidinggevende of de functionaris voor gegevensbescherming.
- 13.2. Waar dit niet gepast is of zaken niet informeel kunnen worden opgelost, moeten medewerkers onze formele klachtenprocedure volgen.

Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 5 van 6

Getekend voor gelezen en akkoord

Naam: Robert van Ballegooijen

Functie: CEO Van Loon Group

Datum: 12-06-2024



Documentcode: BEL 505	Auteur: Manager IT Services Van Loon Group	Versiedatum: 06-06-2024
Code: 3044	Verificateur: CTO Van Loon Group	Pagina 6 van 6