

Wat moet ik doen in mijn winkel als ik camera's gebruik (ook AI-camera's)?

Cameratoezicht kan helpen bij veiligheid en diefstalpreventie.

Informeer je klanten duidelijk

- Hang **goed zichtbare borden** bij de ingang en in de winkel.
- Vermeld dat er cameratoezicht is.
- Geef aan **waarom** je camera's gebruikt (bijv. veiligheid of diefstalpreventie).
- Vermeld wie verantwoordelijk is (naam winkel/bedrijf).

Heb een geldige reden (doel)

Je mag camera's alleen gebruiken als je een **gerechtvaardigd doel** hebt, zoals:

- Voorkomen van diefstal
- Bescherming van medewerkers en klanten
- Beveiliging van eigendommen

Gebruik je AI-camera's

AI-camera's kunnen bijvoorbeeld tellen, gedrag analyseren of patronen herkennen. Dan geldt:

- Verzamel **niet meer gegevens dan nodig**.
- Gebruik bij voorkeur **anonieme of geanonimiseerde data**.
- Gebruik geen gezichtsherkenning.
- Vraag aan je leverancier indien nodig een kopie van de DPIA
- Een DPIA is verplicht bij AI camera's

AI-specifieke afbakening

- Geen emotieherkenning.
- Geen profilering van individuele klanten.
- Geen koppeling met andere databronnen (zoals loyaliteitsapps).

Wanneer is een DPIA verplicht?

Systematische en grootschalige monitoring

Bijvoorbeeld:

- Cameratoezicht in openbare of semi-openbare ruimtes
- Online tracking of profilering van gebruikers
- Structurele monitoring van werknemers

Grootschalige verwerking van bijzondere persoonsgegevens

- Gezondheidsgegevens
 - Biometrische gegevens (vingerafdruk, gezichtsherkenning)
 - Strafrechtelijke gegevens
- Voorals het om **veel mensen** of **structureel gebruik** gaat.

Geautomatiseerde besluitvorming met grote gevolgen

- Kredietbeoordeling zonder menselijke tussenkomst
- Selectie of uitsluiting van personen (bijv. sollicitaties, verzekeringen)

Nieuwe technologieën

- AI-toepassingen
- Gezichtsherkenning
- Grootschalige data-koppelingen

Combinatie van meerdere risicofactoren

De Autoriteit Persoonsgegevens noemt o.a.:

- Profileren
- Grote aantallen betrokkenen
- Kwetsbare personen (kinderen, patiënten, werknemers)
- Gegevens uit verschillende bronnen combineren

Beperk de camerabeelden

- Richt camera's alleen op noodzakelijke plekken.
- **Geen camera's** in paskamers, toiletten of personeelsruimtes.
- Zorg dat beelden niet onnodig lang worden bewaard (meestal max. **28 dagen**, tenzij er een incident is)

Beveilig de beelden goed

- Alleen bevoegde personen mogen toegang hebben.
- Gebruik sterke wachtwoorden en beveiligde systemen.
- Deel beelden alleen als dat wettelijk verplicht is (bijv. politie)

Respecteer privacyrechten

Klanten en medewerkers hebben rechten:

- Ze mogen vragen of ze zijn gefilmd.
- Ze mogen inzage vragen in beelden waar zij op staan.
- Ze mogen bezwaar maken tegen cameratoezicht.

Privacyverklaring

- Vermelden dat cameragebruik moet worden toegelicht in de privacyverklaring (op de website of in de winkel).
- Met name relevant bij AI-toepassingen zoals tellen, heatmaps of gedragsanalyse.

Verwerkersovereenkomst

- Indien de cameraleverancier beelden opslaat of analyseert, is een verwerkersovereenkomst vereist.

Cameratoezicht opnemen in het verwerkingsregister, inclusief:

- doel,
- type camera (AI / geen AI),
- bewaartermijn,
- wie toegang heeft.

Medewerkers

- Personeel schriftelijk informeren.
- Cameratoezicht niet gebruiken voor prestatiecontrole.
- Betrokkenheid van OR/personeelsvertegenwoordiging(indien van toepassing)

De winkelier blijft altijd verantwoordelijk voor de juiste toepassingen van de bovenstaande zaken.