AUTORITEIT
PERSOONSGEGEVENS

Gezichtsherkenning

Antwoord op vragen over verwerkingen van persoonsgegevens bij de inzet van gezichtsherkenning

Inleiding

Gezichtsherkenning is het inzetten van technologie om automatisch gezichten en/of gezichtskenmerken te herkennen. Bij gezichtsherkenning worden vaak zogeheten biometrische gegevens verwerkt zoals bedoeld in de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg)[1]. Het gebruik van gezichtsherkenning is sterk in opkomst. De Autoriteit Persoonsgegevens (AP) ontvangt dan ook steeds vaker vragen en signalen over de inzet van deze techniek.

In dit document beantwoordt de AP een aantal veelgestelde vragen over de inzet van gezichtsherkenning om verwerkingsverantwoordelijken en juridische professionals op weg te helpen. De antwoorden zijn vooral bedoeld voor organisaties die gezichtsherkenning willen gaan toepassen. Het document geeft deze organisaties een indicatie van hoe de AP uitleg geeft aan relevante begrippen en hoe de AP toezicht houdt op gezichtsherkenning.

Grotere risico's

Het waarborgen van de bescherming van persoonsgegevens van betrokkenen is van groot belang bij het verwerken van biometrische gegevens. Het biometrisch gegeven is namelijk een uniek lichaamskenmerk dat is te herleiden naar een individu. Bij diefstal kunnen zulke gegevens niet worden gewijzigd (in tegenstelling tot bijvoorbeeld een wachtwoord) en daarom is het risico van de verwerking van biometrische gegevens voor betrokkenen ook groter.

Op basis van één enkele foto is het technisch heel gemakkelijk om alles van iemand te weten te komen: adres, salaris, zoekgeschiedenis en nog veel meer.[2] Deze foto hoeft nu ook niet meer – zoals in het verleden – onder unieke omstandigheden genomen te zijn. De gezichtsherkenningstechnologie anno 2024 kan iemand (uniek) identificeren, zelfs als iemand bijvoorbeeld een mondkapje op heeft of ouder is geworden. Het is bovendien een relatief laagdrempelige toepassing die gemakkelijk gebruikt kan worden door iedereen die dat wil: een app downloaden is vaak genoeg. Om gezichtsherkenning toe te passen hoeft iemand dus geen deskundige te zijn. Dat deze technologie zo laagdrempelig is, vormt een aanzienlijk risico. Individuen kunnen zo op grote schaal worden geïdentificeerd en gevolgd. De uitkomsten van gezichtsherkenning kunnen bovendien vooringenomen en/of discriminerend zijn en de gezichtsherkenning kan minder goed werken bij bepaalde groepen.

DPIA

Vanwege het risico van het verwerken van biometrische gegevens is het zeer waarschijnlijk dat u een data protection impact assessment (DPIA) moet uitvoeren voordat u start met een grootschalige verwerking door middel van gezichtsherkenning.[3] Ook bij pilots, testen of proefprojecten waarbij een eindproduct nog niet is opgeleverd, is de AVG van toepassing en moet u kijken of het noodzakelijk is om een DPIA uit te voeren. Daarnaast is er een grote kans dat uit de DPIA een hoog restrisico komt, waardoor u als verwerkingsverantwoordelijke ook verplicht bent om een voorafgaande raadpleging (VR) aan te vragen bij de AP.

[1] De Wpg en Wjsg in samenhang gelezen met het Wetboek van Strafvordering.
[2] Zie ook: "Je gezicht is nu van ons. Een real-life thriller over een ontwrichtende technologie" van Kashmir Hill, gepubliceerd op 26 september 2023.
[3] Zie ook: Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens, 27 november 2019 (Stcrt. 2019,64418).

Eerdere acties van de AP

Gezichtsherkenning is al langer een aandachtspunt voor de AP. Eerder heeft de AP in het kader van gezichtsherkenning onder andere een formele waarschuwing aan een supermarkt gegeven vanwege de inzet van gezichtsherkenning[4], een verkennend onderzoek uitgevoerd bij leveranciers en producenten van camera's met gezichtsherkenning[5] en de supermarktbranche via branchevereniging Centraal Bureau Levensmiddelenhandel (CBL) gewezen op de regels voor de inzet van gezichtsherkenningscamera's.[6]

Hoe gebruikt u dit document?

Overweegt u een vorm van gezichtsherkenning in te zetten? Een verwerkingsverantwoordelijke moet altijd verschillende stappen doorlopen om te bepalen wanneer gezichtsherkenningstechnologie is toegestaan, en onder welke voorwaarden van de AVG. Dit document helpt u op weg, maar biedt geen alomvattend toetsingskader voor de inzet van gezichtsherkenningstechnologie.

De AP legt in dit document de focus op de AVG. Afhankelijk van de aard van de gegevens en het doel waarvoor de gegevens verzameld worden, kan (ook) de Wpg of de Wjsg van toepassing zijn.[7] Bij nieuwe ontwikkelingen, zoals de inwerkingtreding van de AI-verordening, bekijkt de AP of er aanpassingen nodig zijn.

Dit juridisch kader begint met een korte introductie over de techniek achter gezichtsherkenning. Daarna volgen 4 veelgestelde vragen over het gebruik van gezichtsherkenning en het antwoord van de AP daarop.

Afbakening

De AP beperkt dit juridisch kader bewust tot de gegevens die verwerkt worden bij gezichtsherkenning, dus biometrische gegevens, die in de AVG ook wel bijzondere persoonsgegevens worden genoemd. De antwoorden in dit document gaan dus niet over de toepassing van biometrische categorisatie, deepfakes, emotieherkenning, leeftijdsverificatie of andere aanverwante zaken, waarin een gezicht ook een rol speelt of kan spelen. Dat neemt niet weg dat de AP ook risico's ziet bij deze toepassingen.[8] Ook bij deze gegevensverwerking moet u aan de regels voldoen van o.a. de AVG.

Externe consultatie

Een eerdere versie van dit document is ter consultatie voorgelegd aan een aantal externe partijen. Uit de consultatie is waardevolle input gekomen. De opmerkingen zijn verwerkt in deze versie van het document. Enkele partijen hebben aangegeven dat de verwerking van biometrische gegevens met als doel het bevestigen van de identiteit niet valt onder het verwerkingsverbod voor bijzondere persoonsgegevens. De AP neemt hier een ander standpunt over in en licht dit uitgebreider toe onder vraag 3.

[4] Zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning.
[5] Zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-pas-op-met-camera%E2%80%99s-met-gezichtsherkenning.
[6] Zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-supermarkten-op-regels-gezichtsherkenning.
[7] De Wpg en de Wjsg bevatten de implementatie van de Richtlijn (EU) 2016/680 over gegevensbescherming, opsporing en vervolging van strafbare feiten.
[8] Zie https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-pleiten-voor-verbod-op-gezichtsherkenning.

De techniek achter gezichtsherkenning[9]

Er zijn verschillende manieren om een computer gezichten te laten herkennen. In de 'Guidelines on the use of facial recognition technology in the area of law enforcement'[10] van de European Data Protection Board (EDPB) wordt gezichtsherkenning omschreven als een proces met 2 fasen: (a) de verzameling van gezichtsafbeeldingen en de transformatie in een template of sjabloon, gevolgd door (b) de herkenning van het gezicht door het template of sjabloon te vergelijken met corresponderende templates of sjablonen. Technisch gezien omvat geautomatiseerde gezichtsherkenning globaal de volgende stappen:

Fase a →	Voorbeeld van een specifieke technische verwerking →	Fase b
1) inputbeeld 2) gezichtsdetectie 3) normalisatie	4) getalsmatige representatie van een gezicht	5) resultaat

Juridisch gezien kan stap 4 het moment zijn dat er sprake kan zijn van een 'specifieke technische verwerking', waardoor een natuurlijk persoon eenduidig en uniek herkend kan worden (artikel 4, aanhef, onder 14, van de AVG). Hierna volgt een beschrijving van de 5 verschillende stappen.

Stap 1 - Inputbeeld

Het inputbeeld dat wordt gebruikt voor gezichtsherkenning is afkomstig van een camera. Het kan hier gaan om een stilstaande foto of een bewegende video. Doordat een computer alleen de losse pixels van een afbeelding ziet, hebben de omstandigheden waaronder het beeld is genomen een grote invloed op de bruikbaarheid ervan. Denk aan lichtinval, (gedeeltelijk) bedekte gezichten, hoek en afstand tot het subject.

Stap 2 - Gezichtsdetectie

Gezichtsdetectie is de eerste stap van geautomatiseerde gezichtsherkenning, waarbij wordt vastgesteld of een afbeelding wel of geen gezicht bevat. Dit valt onder de categorie objectclassificatie. Als er een gezicht op de afbeelding staat, dan wordt dat deel van de foto verder verwerkt. Dit is in essentie voor een computer niet anders dan het herkennen van zebrapaden of verkeersborden op foto's.

Stap 3 - Normalisatie

In deze stap volgt een bewerking: normalisatie.[11] Het doel is om de impact van de omstandigheden waaronder de afbeelding is gemaakt (zoals omschreven bij stap 1) te verminderen door het gezicht in een standaardrepresentatie weer te geven. Er zijn variaties in, zoals: belichting, pose, expressie en occlusie.

Een voorbeeld van een normalisatieproces: eerst wordt het gezicht gedetecteerd (detectie). Daarna worden de karakteristieke punten gezocht (landmarking), zoals de ogen, neus en mond. Met deze karakteristieke punten wordt het gezicht als het ware rechtop gezet en op een standaardgrootte afgebeeld (registratie). Als laatste wordt een segment uit de afbeelding uitgesneden (segmentatie) voor de verdere herkenning. Daardoor heeft het systeem geen last van variaties, bijvoorbeeld in haardracht.

Stap 4 - Getalsmatige representatie van een gezicht

De volgende stap in het proces is het coderen van de gezichten tot een unieke getalsmatige representatie. Er bestaan diverse methoden om gezichten te coderen. Convolutional Neural Network (CNN) is de meest actuele en accurate methode om gezichten te representeren. Convolutie maakt feitelijk een hiërarchie van

[9] Zie: https://www.mdpi.com/2079-9292/9/8/1188.
[10] Zie: EDPS-Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, p. 9.
[11] Zie: 14175 Oratieboekje Veldhuis (utwente.nl), p. 21-23.

abstracties van wat een CNN leert uit de afbeelding en doet dit in veel verschillende lagen. Er is bijvoorbeeld een laag die de randen van een gezicht representeert. In een andere laag worden de randen van het gezicht gecombineerd om te leren of er bijvoorbeeld stukjes van een oog of neus te ontdekken zijn. Een van de laatste lagen combineert alle eigenschappen van een gezicht met elkaar om een getalsmatige representatie te maken van het gezicht. De volgorde van de CNN-lagen is nagenoeg niet te volgen en daarom wordt deze vaak als een 'black box' omschreven.

Stap 5 - Resultaat

Het resultaat van de voorgaande stappen is dat er een getalsmatige representatie is gemaakt van een gezicht. Deze getalsmatige representatie helpt om gezichten met elkaar te vergelijken. Hoewel de representatie zelf door de omstandigheden van de opname per geval zal verschillen, is de representatie voor ieder individu grotendeels gelijk. Dit maakt het mogelijk de representaties – en dus de gezichten – op te slaan en met elkaar te vergelijken.

Disclaimer

In deze paragraaf staan de meest voorkomende technische stappen om gezichten te herkennen, aan de hand van een aantal veelgebruikte technische methoden. Er zijn veel meer methoden, dit is dus geen volledig overzicht.

1. Wanneer is het verwerken van persoonsgegevens via de inzet van gezichtsherkenning een zuiver persoonlijke of huishoudelijke activiteit en is de AVG niet van toepassing?

De AVG is niet van toepassing bij de inzet van gezichtsherkenning door natuurlijke personen voor activiteiten met een zuiver persoonlijk of huishoudelijk doel.[12]

Veel apparaten bevatten tegenwoordig biometrische authenticatiemechanismes. Dat houdt in dat het mogelijk is om de apparaten te ontgrendelen met vingerafdrukken of gezichtsherkenning. Dit soort gebruik van gezichtsherkenning kan een verwerking van persoonsgegevens zijn die uitsluitend betrekking heeft op een persoonlijke of huishoudelijke activiteit, mits het gebruik lokaal (alleen op het apparaat) en autonoom (de gebruiker beslist zelf) kan plaatsvinden zonder externe toegang (derden hebben geen toegang tot de gegevens op het apparaat). De AP benadrukt dat u alleen een beroep kunt doen op deze uitzondering wanneer u voldoet aan alle volgende voorwaarden:

1. Het door de gebruiker van de mobiele elektronica gebruikmaken van het apparaat of de dienst om toegang te verkrijgen tot (gedownloade applicaties op) het apparaat is aan te merken als privégebruik;
2. De gebruiker krijgt het gebruik van diens biometrische gegevens niet opgelegd door een werkgever of een andere derde (partij). De gebruiker heeft er dus zelf voor gekozen om gebruik te maken van de optie om door middel van de verwerking van biometrische gegevens toegang te verkrijgen. De gebruiker kan ook voor een alternatief kiezen, zoals inloggen met een wachtwoord;
3. De biometrische gegevens die van een gebruiker zijn opgeslagen, zijn niet toegankelijk voor derden. De gegevens kunnen niet naar bijvoorbeeld een externe database worden gestuurd en derden kunnen niet bij deze gegevens. Bovendien is de beveiliging van de opslag van de gegevens van een hoog niveau;
4. De biometrische gegevens worden op het apparaat opgeslagen met behulp van versleuteling volgens de stand van de techniek;
5. Bij een toegangscontrole geeft de techniek alleen door of de herkenning is gelukt of niet.

De AP sluit met deze 5 voorwaarden aan bij de eerder door de Franse toezichthouder (CNIL)[13] en Belgische toezichthouder (GBA)[14] gepubliceerde punten.

Signalering: gebruik van deurbel met gezichtsherkenning

Op dit moment zijn deurbellen met gezichtsherkenning in ontwikkeling. Deze deurbellen kunnen gericht zijn op de openbare weg. Met behulp van gezichtsherkenning kan de deurbel registreren wie er voor de deur staat, de bewoner daarvan op de hoogte brengen en bekenden automatisch binnenlaten. Ook kunnen er via de app beelden van de deurbel worden verspreid. De AP signaleert de opkomst van deze deurbellen en houdt deze ontwikkeling nauwlettend in de gaten. Let bij gebruik hiervan op de naleving van de regels uit de AVG.[15]

[12] Overweging 18 van de AVG geeft over deze uitzondering aan: 'Deze verordening is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon in het kader van een louter persoonlijke of huishoudelijke activiteit die als zodanig geen enkel verband houdt met een beroeps- of handelsactiviteit. [...] Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten.'

[13] 'Biométrie dans les smartphones des particuliers : application du cadre de protection des données', www.cnil.fr, 24 juli 2018.

[14] 'Aanbeveling betreffende de verwerking van biometrische gegevens', www.gegevensbeschermingsautoriteit.be, 1 december 2021.

[15] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-publiceert-beleidsregels-cameratoezicht.

2. Welke vereisten zijn er om te spreken van een biometrisch gegeven in de zin van de AVG bij de toepassing van een vorm van gezichtsherkenning?

In de AVG[16] zijn biometrische gegevens gedefinieerd als 'persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens'.

Het begrip 'biometrische gegevens' heeft in de wetenschappelijke context vaak een andere betekenis dan in de AVG. Om te spreken van een biometrisch gegeven zoals dat is gedefinieerd in de AVG, gelden er 3 cumulatieve criteria:[17]

1. **De aard van de gegevens:** het moet gaan om gegevens over de fysieke, fysiologische of gedragsgerelateerde kenmerken van natuurlijke personen.

Bij de inzet van een vorm van gezichtsherkenning gaat het om fysieke en fysiologische kenmerken die direct aan een natuurlijk persoon kunnen worden toegewezen. Deze kenmerken zijn meestal ook permanent verbonden aan een natuurlijk persoon. Het gaat hier bijvoorbeeld om gezichtsinformatie, zoals de afstand tussen iemands ogen.

2. **De middelen en de wijze van verwerken:** het moet gaan om persoonsgegevens 'die het resultaat zijn van een specifieke technische verwerking'.

Het resultaat van een specifieke technische verwerking betekent dat gegevens met bepaalde technische middelen worden geanalyseerd en vervolgens vergeleken met referentieparameters. Een voorbeeld van een verwerking die in ieder geval geen specifieke technische verwerking is, is het plaatsen van een foto van iemand in een krant. Het zijn niet de gegevens op zich maar het gebruik ervan, 'de specifieke technische verwerking', dat een gegeven biometrisch maakt.

Hoe een specifieke technische verwerking zich bij gezichtsherkenning voordoet, hangt uiteindelijk af van de gebruikte techniek. Het wordt bijvoorbeeld wél een specifieke technische verwerking wanneer uit het vastgelegde beeld van het gezicht de kenmerken van het gezicht naar een template worden omgezet. Die template is uniek en specifiek voor één persoon. Uiteindelijk kan de herkenning van een gezicht plaatsvinden door de template te vergelijken met eerder opgeslagen templates. In dit voorbeeld is zowel bij de fase van het opslaan van een template als de uiteindelijke vergelijking sprake van een specifieke technische verwerking. Zie hiervoor ook de paragraaf 'de techniek achter gezichtsherkenning'.

3. **Het doel van de verwerking:** eenduidige identificatie van die natuurlijke persoon is mogelijk of wordt bevestigd.

Tot slot moet u kijken naar het doel van de verwerking. De persoonsgegevens moeten eenduidige identificatie van die natuurlijke persoon mogelijk maken of bevestigen. In de AVG staat niet wat 'eenduidige identificatie' of 'bevestigen' precies inhoudt. Hieronder leest u meer over deze begrippen.

Houd er rekening mee dat de juridische betekenis van deze begrippen in de AVG en UAVG niet altijd overeenkomt met de technische of wetenschappelijke betekenis.

[16] Artikel 4, aanhef en onder 14, van de AVG.
[17] Zie ook de EDPB Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur.

Eenduidige identificatie

Bij eenduidige identificatie door gezichtsherkenning gaat het om de vraag: wie is deze persoon? Eenduidig betekent hier dat biometrische gegevens voor identificatie maar aan één natuurlijk persoon kunnen worden toegeschreven. Het biometrisch gegeven is dus uniek voor die persoon.

Een voorbeeld van eenduidige identificatie is het vergelijken van het gezicht van een persoon met gezichten van een groep personen die in een database zijn opgeslagen. Het gebruik van gezichtsherkenning met identificatie als doel, werkt technisch vaak als volgt. Eerst wordt een beeld van een gezicht verzameld en omgezet in een template. Vervolgens wordt een gezicht geïdentificeerd door die template met andere templates te vergelijken (ook wel: 'one-to-many'). Het doel is om vast te stellen of de template van een natuurlijk persoon met een andere template overeenkomt om zo de persoon te identificeren. Naast dit voorbeeld zijn er ook andere technische manieren om mensen met gezichtsherkenning te identificeren.

Voorbeeld: eenduidige identificatie

Let op: dit is slechts een voorbeeld ter verduidelijking van de hierboven genoemde definitie. Dit voorbeeld zegt niets over of dit een toelaatbare toepassing is volgens de AVG. Hiervoor moet een betrokkene onder andere geldige, uitdrukkelijke toestemming geven. Zie ook het antwoord op vraag 5.

Een winkelcentrum in Nederland heeft videoapparatuur met gezichtsherkenningstechnologie geïnstalleerd in de hal van het centrum. De verwerkingsverantwoordelijke heeft een database aangelegd met templates met gezichtskenmerken van alle bekende Nederlanders. Zodra een BN'er in het winkelcentrum is, wordt de verwerkingsverantwoordelijke door de videoapparatuur met gezichtsherkenningstechnologie gewaarschuwd wie de BN'er is.

Bevestiging van de identiteit

De definitie van biometrische gegevens[18] in de AVG gaat ook over 'bevestigen' van de identiteit. Bij het bevestigen van de identiteit gaat het om de vergelijking tussen 2 gezichten, dus om een controle op gelijkheid: is gezicht A gelijk aan gezicht B? (een 'one-to-one' vergelijking). Een biometrische vergelijking van het gezicht wordt dan gebruikt om te verifiëren en te bevestigen dat een individu dezelfde persoon is als de persoon van wie de biometrische gegevens eerder zijn vastgelegd. Het doel is om te controleren of de persoon is wie deze zegt te zijn. Het biometrisch gegeven van één natuurlijk persoon wordt alleen vergeleken met één ander biometrisch gegeven. Dit proces wordt ook wel authenticatie genoemd in de AVG.

Voorbeeld: identiteit bevestigen

Let op: dit is slechts een voorbeeld ter verduidelijking van de hierboven genoemde definitie. Dit voorbeeld zegt niets over of dit een toelaatbare toepassing is volgens de AVG. Hiervoor moet een betrokkene onder andere geldige, uitdrukkelijke toestemming geven. Zie ook het antwoord op vraag 5.

Wanneer je vanaf een vliegveld op vakantie gaat naar een land waarvoor je door de paspoortcontrole moet gaan en je geeft uitdrukkelijke toestemming voor de automatische paspoortcontrole, dan moet je je paspoort laten scannen. Om door de scan te komen, vergelijkt een algoritme de gezichtskenmerken uit een 'live' gezichtsfoto met de foto in je paspoort om je identiteit te verifiëren. Als het een 'match' is, kun je door de poort richting het vliegtuig.

[18] Artikel 4, aanhef en onder 14, van de AVG.

Voorbeeld: geen biometrisch gegeven in de zin van de AVG

Let op: dit is slechts een voorbeeld ter verduidelijking van de hierboven genoemde definitie. Dit voorbeeld zegt niets over of dit een toelaatbare toepassing is volgens de AVG.

Een gemeente gebruikt bij de aanvraag van identiteitsbewijzen aan de balie een gezichtsscanner om te controleren of de persoon die voor de medewerker staat ook degene is die op het paspoort staat. Op het scherm van de medewerker wordt het gezicht van de persoon uitvergroot, zodat de medewerker zelf de gezichtskenmerken kan vergelijken met de foto op het oude identiteitsbewijs. Er is hier *geen* specifieke technische verwerking: het gaat namelijk om een 'gewone' verwerking. Deze vorm van gezichtsherkenning valt dus niet onder de definitie van biometrie in de zin van de AVG, maar de overige voorwaarden uit de AVG kunnen natuurlijk wel van toepassing zijn.

Voorbeeld: wel gezichtsherkenning, maar geen eenduidige identificatie of bevestiging van identiteit en dus geen biometrisch gegeven in de zin van de AVG

Let op: dit is slechts een voorbeeld ter verduidelijking van de hierboven genoemde definitie. Dit voorbeeld zegt niets over of dit een toelaatbare toepassing is volgens de AVG.

Een winkelcentrum heeft videoapparatuur met gezichtsherkenning opgehangen en wil deze gebruiken om te zien welke doelgroepen naar het winkelcentrum komen. De apparatuur leidt alleen van een gezicht af of iemand man of vrouw is om het gezicht vervolgens in een categorie te plaatsen. Het winkelcentrum heeft geen database aangelegd met templates van andere personen. Het doel van de verwerking is hier om een categorie personen te onderscheiden van een andere categorie personen. Het is bovendien met de gebruikte apparatuur en de daaruit voortvloeiende gegevens *niet* mogelijk om een natuurlijk persoon eenduidig te identificeren of de gegevens te gebruiken voor authenticatie. Er is dus geen sprake van biometrische gegevens in de zin van de AVG.

Let op: dit zijn slechts voorbeelden. U moet ook aan de overige vereisten uit de AVG voldoen die gelden bij het verwerken van (biometrische) persoonsgegevens. Als alle 3 hierboven besproken criteria van toepassing zijn, dan is er sprake van een biometrisch gegeven in de zin van de AVG. Indien één of meerdere van de criteria niet van toepassing zijn, dan kan er nog steeds sprake zijn van een 'gewone' verwerking van persoonsgegevens. Ook in dat geval moet een verwerkingsverantwoordelijke voldoen aan de beginselen van gegevensverwerking en onder andere een grondslag hebben voor de verwerking.

3. Valt het verwerken van biometrische gegevens onder het verwerkingsverbod voor bijzondere persoonsgegevens als het doel is om iemands identiteit te bevestigen?

Biometrische gegevens behoren tot de categorie bijzondere persoonsgegevens zoals bedoeld in artikel 9 van de AVG als het gaat om de 'verwerking van (…) biometrische gegevens met het oog op de unieke identificatie van een persoon'. Dit is anders dan in de definitie van een biometrisch gegeven in artikel 4, onder 14, van de AVG. Dit artikel noemt eenduidige identificatie en bevestiging daarvan. Maar artikel 9, eerste lid, van de AVG spreekt dus over unieke[19] identificatie. De vraag is of onder het begrip unieke identificatie, naast eenduidige identificatie, in artikel 9 van de AVG ook bevestiging van de identiteit valt. Uit een letterlijke lezing van de tekst van artikel 9, eerste lid, AVG zou immers kunnen worden afgeleid dat het verwerkingsverbod uitsluitend gaat over de verwerking van biometrische gegevens met alleen als doel unieke identificatie van een natuurlijk persoon.

In artikel 9, eerste lid, van de AVG wordt het begrip biometrische gegevens gebruikt zoals dat is gedefinieerd in artikel 4, aanhef en onder 14, van de AVG. Daaruit valt af te leiden dat dus ook het verwerken van biometrische gegevens om de identiteit van een persoon te bevestigen onder het verbod valt van artikel 9, eerste lid, van de AVG. Dit volgt ook uit overweging 51 van de AVG: "De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken. In deze overweging wordt de definitie van artikel 4, aanhef en onder 14, van de AVG gekoppeld aan artikel 9, eerste lid, van de AVG en daarmee dus ook het bevestigen van de identiteit van een persoon.

In EDPB-verband is ook aangegeven dat het verwerken van biometrische gegevens voor dit doel behoort tot de categorie van bijzondere persoonsgegevens zoals bedoeld in artikel 9 van de AVG.[20]

Daarom houdt de AP deze lijn aan: het verwerken van biometrische gegevens met als doel iemands identiteit te bevestigen, valt óók onder artikel 9, eerste lid, van de AVG.

[19] Gelet op onder meer de Franse en Engelse tekst van de AVG wordt met eenduidige identificatie in artikel 4, aanhef en onder 14, AVG hetzelfde bedoeld als unieke identificatie in artikel 9, eerste lid, AVG.
[20] Zie EDPB-richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur en EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.

4. Wanneer kunt u een beroep doen op de uitzonderingen op het verwerkingsverbod bij de inzet van gezichtsherkenning, en in het bijzonder op uitdrukkelijke toestemming en de in een wettelijke bepaling verankerd zwaarwegend algemeen belang?

Het verwerken van biometrische gegevens voor unieke identificatie van een persoon valt onder het verwerkingsverbod van artikel 9, eerste lid, van de AVG. Dit verwerkingsverbod wordt alleen doorbroken als een uitzonderingsgrond van toepassing is uit artikel 9, tweede lid, van de AVG. Naast een uitzonderingsgrond moet u voor de verwerking ook altijd voldoen aan de beginselen van gegevensbescherming uit artikel 5 AVG en moet u als verwerkingsverantwoordelijke een grondslag uit artikel 6 AVG hebben.

Hierna bespreken we 2 mogelijke uitzonderingen voor gezichtsherkenning: uitdrukkelijke toestemming van de betrokkenen en een zwaarwegend algemeen belang.

Uitdrukkelijke toestemming

Een van de uitzonderingen op het verwerkingsverbod is 'uitdrukkelijke toestemming'. Deze uitzondering staat in artikel 9, tweede lid, sub a, van de AVG. Voor uitdrukkelijke toestemming gelden zwaardere eisen dan voor de 'gewone' toestemming uit artikel 6 en 7 van de AVG.[21] Uitdrukkelijke toestemming moet vrijelijk, ondubbelzinnig, geïnformeerd, specifiek en uitdrukkelijk zijn gegeven door middel van een verklaring of een ondubbelzinnige actieve handeling.[22] U moet rekening houden met de volgende voorwaarden:

- **Vrije toestemming: Bied een alternatief aan.**
  De toestemming moet in vrijheid worden gegeven. Heeft een betrokkene geen werkelijke keuze, voelt diegene zich gedwongen om toestemming te geven of heeft niet instemmen negatieve gevolgen voor deze persoon? Dan is de toestemming niet geldig. U moet betrokkenen actief een andere gelijkwaardige mogelijkheid aanbieden voor de gezichtsherkenning. U kunt bijvoorbeeld denken aan het gebruik van een pasje. Betrokkenen mogen geen druk voelen om akkoord te geven voor de optie gezichtsherkenning. Wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke en dit het onwaarschijnlijk maakt dat de toestemming in die specifieke situatie vrijelijk is verleend, dan kunt u zich niet beroepen op vrije toestemming. Dit is bijvoorbeeld al snel het geval in een arbeidsrelatie.
- **Informeer betrokkenen.**
  U moet de betrokkenen minimaal informeren[23] over:
  - de identiteit van de verwerkingsverantwoordelijke;
  - welke soorten gegevens worden verzameld en gebruikt;
  - het doel van het gebruik van de gezichtsherkenning en de grondslag voor de verwerking van de persoonsgegevens;
  - het recht van de betrokkenen om de toestemming weer in te trekken en daarna het recht op verwijdering van deze gegevens;
  - wie de ontvanger is van de gegevens;
  - hoe lang u de gegevens bewaart;

[21] Zie ook EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679.
[22] Zie uitgebreider: https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd#grondslag-toestemming en de EDPB, Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679.
[23] Zie ook artikel 12 , 13 en 14 van de AVG.

  - de mogelijkheden om gebruik te maken van een alternatief. U moet betrokkenen hier actief op wijzen;
  - het gebruik van de gegevens voor geautomatiseerde besluitvorming, indien van toepassing; en
  - de risico's van doorgiften van gegevens naar landen buiten de EER bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen.

  Deze informatie moet begrijpelijk zijn. Zo kan de betrokkene zelf goed kiezen om wel of niet akkoord te gaan met de optie gezichtsherkenning.
- **Betrokkenen moeten duidelijk en actief akkoord gaan met het gebruik van gezichtsherkenning**. De verwerkingsverantwoordelijke moet betrokkenen duidelijk laten weten welke persoonsgegevens verzameld worden en waarom deze persoonsgegevens verwerkt worden. De toestemming moet specifiek gericht zijn op het verwerkingsdoel van de verwerkingsverantwoordelijke. In overweging 32 van de AVG staat dat, als de verwerking meerdere doeleinden heeft, de betrokkene voor elk doeleinde afzonderlijk uitdrukkelijk toestemming moet verlenen. Het doel waarvoor de betrokkene toestemming geeft mag niet gaandeweg veranderen. Als dit wel verandert, dan zal de betrokkene opnieuw uitdrukkelijke toestemming moeten geven voordat de verwerkingsverantwoordelijke met deze verwerking mag starten. De uitdrukkelijke toestemming moet bovendien door middel van een ondubbelzinnige wilsuiting worden gegeven. Dit betekent: een ondubbelzinnige actieve handeling of een (digitale) schriftelijke of mondelinge verklaring van de betrokkene. Het aanvaarden van de algemene voorwaarden van een dienst geldt niet als toestemming.
- **Bewaar bewijs van de gekregen uitdrukkelijke toestemming.**
  U moet kunnen laten zien dat u toestemming heeft gekregen van elke gebruiker van de gezichtsherkenning. Bewaar de gegeven toestemming bijvoorbeeld op een lijst.
- **Zorg ervoor dat betrokkenen hun toestemming kunnen intrekken**.
  Betrokkenen hebben het recht om hun toestemming in te trekken. Dat moet even makkelijk zijn als toestemming geven. Deze gegevens moet de verwerkingsverantwoordelijke daarna verwijderen.

In een wettelijke bepaling verankerd zwaarwegend algemeen belang

Is er sprake van wetgeving die voldoet aan de voorwaarden van artikel 9, tweede lid, onderdeel g, AVG? Dan is het verbod om biometrische gegevens te verwerken niet van toepassing. Deze voorwaarden zijn:

- de verwerking is noodzakelijk 'om redenen van zwaarwegend algemeen belang';
- dit zwaarwegende algemene belang is vastgelegd in de wettelijke bepaling;
- de evenredigheid met het nagestreefde doel wordt gewaarborgd;
- de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd; en
- passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

Artikel 29 van de UAVG[24]

Artikel 29 van de UAVG geeft invulling aan artikel 9, tweede lid, onderdeel g, van de AVG door het creëren van een ontheffing op het verbod om biometrische gegevens te verwerken als die verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De uitzondering in artikel 29 van de UAVG vereist dat u een afweging maakt of unieke identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Daarnaast moet de verwerking van biometrische gegevens proportioneel zijn.

U moet per geval bekijken of er sprake is van een noodzakelijke verwerking van biometrische gegevens om redenen van zwaarwegend algemeen belang via vormen van gezichtsherkenning voor authenticatie of

[24] Artikel 29 van de UAVG luidt: "Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden."

beveiligingsdoeleinden. Deze toetsing van de noodzakelijkheid en proportionaliteit is essentieel. Als de impact van de verwerking van biometrische gegevens groot is en er alternatieven voorhanden zijn, dan is het verwerken van biometrische gegevens niet noodzakelijk.

In een actueel voorstel voor het wijzigen van artikel 29 van de UAVG staat dat alleen een beroep kan worden gedaan op de ontheffing bij een zwaarwegend algemeen belang. De verwerking moet dan dus noodzakelijk zijn voor authenticatie of beveiligingsdoeleinden én noodzakelijk zijn vanwege een zwaarwegend algemeen belang. Ook maakt de wijziging de doelbeperking expliciet door de toevoeging: 'tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen'.

Voorbeeld: uitzondering artikel 29 UAVG mogelijk wel van toepassing

ISPS-bedrijven (havenbedrijven die internationaal scheepvaartverkeer afhandelen) kunnen grote hoeveelheden stoffen verwerken die grote gevolgen hebben voor de gezondheid en veiligheid van werknemers en de omgeving. Daarnaast kunnen ISPS-bedrijven goederen of stoffen verwerken die een doelwit zijn voor (drugs)criminelen en/of terroristen. Voor beveiligingsdoeleinden kan de inzet van gezichtsherkenning noodzakelijk zijn om – in het geval van de ISPS-bedrijven – het risico op zware ongevallen te voorkomen of om de veiligheid van personeel en goederen te waarborgen. De ISPS-bedrijven moeten een concrete afweging maken op basis van de dubbele noodzakelijkheidstoets.[25]

Voorbeeld: gezichtsherkenning in de supermarkt

Een supermarkt wil gezichtsherkenning inzetten om diefstal tegen te gaan en om eigendommen en medewerkers te beschermen, en wil daarvoor uitdrukkelijke toestemming vragen aan betrokkenen. Klanten moeten uitdrukkelijke toestemming in vrijheid kunnen geven door middel van een duidelijke actieve handeling waaruit de toestemming blijkt. In de praktijk is het voor een supermarkt waarschijnlijk onmogelijk om van elke klant uitdrukkelijke toestemming te vragen. Deze uitzonderingsgrond is dan ook waarschijnlijk niet bruikbaar voor een supermarkt. Ook artikel 29 UAVG (en de voorgestelde nieuwe tekst) biedt voor een supermarkt geen uitzondering, omdat de lat voor een succesvol beroep hierop hoog ligt. Wanneer het doel van een supermarkt voor de inzet van gezichtsherkenning is om eigendommen en medewerkers te beschermen, kan dit belang weliswaar zwaarwegend zijn, maar lijkt geen sprake van zwaarwegende *algemene* belangen. Het inzetten van gezichtsherkenning is bovendien een forse inbreuk op de privacy van alle bezoekers en dit weegt zwaarder dan de zwaarwegende private belangen van de supermarkt.

[25] https://www.autoriteitpersoonsgegevens.nl/uploads/2023-09/Privacy%20Gedragscode%20Toegangsbeleid%20ISPS-bedrijven.pdf