PELS RIJCKEN

De inzet van (digitale) preregistratie en biometrische toegangspoortje door betaald voetbalorganisaties

Pels Rijcken | Postbus 11756 | 2502 AT Den Haag | +31 70 515 3000 | pelsrijcken.nl

Inhoud

1 INLEIDING

1.1 Op verzoek van het ministerie van Volksgezondheid, Welzijn en Sport ('VWS') heeft de Landsadvocaat op 2 juli jl. het rapport "De inzet van slimme technologie in voetbalstadions voor de aanpak van discriminatie en racisme' uitgebracht. In dit rapport is een verkenning verricht van de privacyrechtelijke kaders voor de inzet van slimme technologieën in voetbalstadions. In dit rapport is reeds eerder al toegelicht dat er, behoudens de wettelijke grondslag 'uitdrukkelijke toestemming', geen toereikende wettelijke grondslag is voor de inzet van biometrie als voorwaarde voor toegang tot het voetbalstadion.

1.2 In de praktijk merken Sportinnovator en de KNVB echter dat sommige Betaald voetbal organisaties ('BVO's') (overwegen om te) experimenteren met een vorm van biometrische toegangscontrole. Dit terwijl bij andere BVO's juist wordt gekozen voor (digitale) preregistratie waarbij geen biometrie wordt toegepast. Met dit rapport zal helderheid worden gegeven over de (on)mogelijkheden om preregistratie (met biometrische identificatie) resp. biometrische toegangspoortjes in te zetten.

2 REIKWIJDTE EN VRAAGSTELLING VAN DIT RAPPORT

2.1 In dit advies zullen de volgende vragen/onderwerpen aan bod komen:

- In hoeverre beschikt de BVO over een wettelijke grondslag in de zin van artikel 6, artikel 9 en artikel 10 Algemene Verordening Gegevensbescherming ('AVG') om bij de toegangscontrole gebruik te maken van digitale preregistratie en/of biometrie (gezichtsherkenning, vingerafdruk, handpalm)? Maakt het daarbij uit of het betreffende middel wordt ingezet ten behoeve van reguliere toegangscontrole of het controleren van een voetbalstadionverbod[1]?

- Kan de inzet van biometrie worden gebaseerd op 'uitdrukkelijke toestemming' van de bezoeker, en zo ja, welke maatregelen moeten door de BVO of het voetbalstadion worden getroffen om deze grondslag succesvol te kunnen inroepen? Kan de hierboven bedoelde toestemming eenmalig worden gegeven of moet dit voor elke wedstrijd opnieuw worden gegeven en wat zijn de consequenties als een bezoeker zijn of haar toestemming voor een wedstrijd weer intrekt?

- In welke andere situaties, naast die van de beveiliging van een kerncentrale, kan artikel 29 UAVG een wettelijke grondslag voor BVO's een wettelijke basis bieden voor de inzet van biometrie?

- In hoeverre voldoet de inzet van biometrische toegangspoortjes aan het noodzakelijkheidsbeginsel c.q. dataminimalisatie? Hoe dient daarbij te worden meegewogen dat uit andere pilots volgt dat preregistratie (zonder enige vorm van biometrie) uitkomst kan bieden?

- Voor zover een grondslag bestaat voor de inzet van biometrische toegangspoortjes, welke overige juridische, technische en organisatorische maatregelen dienen door de BVO getroffen te worden om rechtmatig biometrie toe te passen?

2.2 Wij zullen de antwoorden van deze vragen nader belichten aan de hand van drie vormen van toegangscontrole die reeds nu al door BVO's worden ingezet.

[1] Hierbij zal rekening worden gehouden met het soort stadionverbod, te weten een civielrechtelijke stadionverbod en een strafrechtelijk stadion verbod.

Casus 1: Digitale preregistratie (IBA)

De eerste identificatiemogelijkheid is die van *Identity Based Access ('IBA').* Dit is een vorm van ' digitale preregistratie' en werkt als volgt. Om als bezoeker toegang te verkrijgen tot het stadion met zijn ticket, moet hij zich in een app registeren. Bij eenmalige registratie haalt de desbetreffende app informatie/ gegevens uit een ID-kaart, paspoort of rijbewijs van de bezoeker die zich registreert. Het gaat dan om de volgende gegevens: naam, geboortedatum en pasfoto. Deze gegevens worden opgeslagen in een datakluis op de smartphone van de bezoeker. In de app wordt ten aanzien van deze gegevens gebruik gemaakt van encryptie. De beheerder van de app kan dus niet bij deze gegevens.

Als een bezoeker meerdere tickets koopt kan hij deze doorsturen naar andere personen die het ticket willen overnemen. De werkelijke bezoekers van het voetbalstadion moeten zich daarna (voordat zij het ticket kunnen accepteren en gebruiken) registreren in de app. Deze persoonsgegevens worden opgeslagen in een datakluis op de smartphone van deze bezoeker. Pas als de bezoeker een ticket accepteert, dit betreft aldus een andere handeling dan het kopen en downloaden van het ticket, worden zijn persoonsgegevens overgedragen aan de desbetreffende BVO. De bezoeker wordt daartoe op een zogeheten gastenlijst van de club geplaatst. Uiteindelijk heeft de club zo een (centraal) overzicht van alle personen die toegang hebben tot het stadion. Vervolgens vindt er dan bij de ingang van het stadion nog een handmatige controle plaats.

Op dit moment wordt de hierboven beschreven vorm van preregistratie nog enkel toegepast voor de toegangscontrole tot het voetbalstadion. Daarbij geldt dat een bezoeker ook altijd de mogelijkheid blijft houden om geen gebruik te maken van de app, maar om via de fysieke controle het voetbalstadion naar binnen te gaan. Hoewel dit in de praktijk nog niet plaatsvindt, zal ook worden bezien in hoeverre het juridisch haalbaar is om deze techniek toe te passen ter handhaving van stadionverboden door de BVO resp. het voetbalstadion.

Casus 2: Preregistratie met (biometrische) identificatie

Bij de tweede identificatiemogelijkheid kunnen bezoekers zich online registeren in een app door middel van het uitlezen van de NFC-chip van een identiteitsbewijs. Daarna identificeert de gebruiker zich met een 'selfie' en een "liveness check". Bij een positieve identificatie ontvangt de BVO enkel een bevestiging dat de verificatie van de identiteit is geslaagd (zonder dat daarbij de onderliggende gegevens met de BVO worden gedeeld). De bezoeker geeft voor het delen van dit resultaat toestemming in de app. Ten aanzien van deze methode worden biometrische gegevens verwerkt. In de app wordt ten aanzien van deze gegevens gebruik gemaakt van encryptie. De beheerder van de app kan dus niet bij deze gegevens.

De BVO *kan* voor de toegang tot het voetbalstadion een verplichte identificatie instellen. Om een kaart te kunnen activeren voor toegang moeten alle bezoekers zich registeren en identificeren (ook de losse kaarten). Bezoekers hoeven dit niet verplicht middels de app te doen, maar kunnen zichzelf handmatig laten identificeren bij de balie of de poortjes in het voetbalstadion. Zij hoeven dan geen 'selfie' en een 'liveness check' te doen. Van een verwerking van biometrische gegevens is bij de handmatige controle van de identiteit van de bezoeker geen sprake. Mensen met een stadionverbod kunnen op zo'n manier geen kaart kopen of activeren en kunnen derhalve geen geldig ticket verkrijgen. Zoals hierna zal worden toegelicht, is het aanbieden van een alternatieve digitale preregistratie als bedoeld in deze casus vooralsnog enkel mogelijk op basis van uitdrukkelijke toestemming van de bezoeker. Een wettelijk vereiste om van biometrische preregistratie gebruik te kunnen maken, is dat er ook een vrije keuze bestaat voor preregistratie zonder biometrie. De hierboven beschreven handmatige controle achten wij op zichzelf in overeenstemming met de regels van de AVG. Voor de verwerking van persoonsgegevens in het kader van de

handmatige controle, gelden dezelfde conclusies en aanbevelingen als bij casus 1. Wij zullen de alternatieve handmatige controle (als onderdeel van casus 2) in het verdere rapport dus niet afzonderlijk toetsen. Wij beperken ons in dit verdere rapport tot een analyse van de preregistratie met biometrische identificatie.

In dit rapport zal mede worden bezien in hoeverre het juridisch haalbaar is om preregistratie met biometrische identificatie verplicht te stellen ter handhaving van stadionverboden door de BVO resp. het voetbalstadion.

Casus 3: Biometrische toegangspoortjes

Na de identificatie is er een tweede stap in het proces dat toegang geeft tot het stadion, te weten de biometrische toegangspoortjes. Aan het gebruik van de biometrische toegangspoortjes gaat het in casus 2 beschreven proces van preregistratie vooraf. Ook hierbij moet een bezoekers zichzelf dus eerst registreren in een app. In de praktijk maakt een biometrisch toegangspoortje gebruik van (a) een biometrische controle van het gezicht en (b) een controle van het toegangsrecht van de bezoeker (vaak aan de hand van een QR-code).

(a) Toegang met gezichtsherkenning

De bezoeker heeft de keuze om toestemming te geven voor het gebruik gezichtsherkenning ten behoeve van de toegang tot het stadion. Zowel de foto van het geüploade identiteitsbewijs als de selfie worden omgezet naar een code (een zogenoemde face vector).

Een face vector van de foto resp. de selfie wordt gemaakt met een algoritme waar de beheerder van de app zelf niet bij kan. Beide codes (face vectors) worden met elkaar vergeleken binnen de (afgesloten) app van de gebruiker. Op deze manier wordt de juistheid van de face vector gevalideerd. De gevalideerde face vector wordt versleutel (ge-encrypt) en als encrypted code opgeslagen in een centraal overzicht (centrale collectie) van de app beheerder. De face vector wordt in deze fase niet gedeeld met de voetbal club. Vervolgens wordt er toestemming gevraagd aan de bezoeker om de face vector te gebruiken binnen het proces van de toegangscontrole tot het stadion. Dit gaat concreet als volgt.

Het biometrische poortje maakt een foto van de bezoeker bij het biometrische poortje en zet deze om naar een face vector. Deze face vector wordt vergeleken met face vector die reeds in de collectie van de app beheerder staat opgeslagen. Het resultaat van deze vergelijking wordt wel gedeeld met de BVO en betreft alleen het relatienummer. Op basis van het relatienummer wordt vervolgens aan de hand van de QR-module (zie hierna) het toegangsrecht van de bezoeker gecheckt.

(b) Toegang met een QR-code

De toegangscontrole (het geautoriseerd zijn om het stadion voor een specifiek evenement op een specifieke locatie/toegangspoort en tijdstip te kunnen betreden, inclusief de uitoefening van een stadionverbod) wordt uitgevoerd aan de hand van de scan van de QR code van de bezoeker. De biometrische module geeft enkel een unieke code terug aan dit toegangscontrolesysteem op basis van het aangeboden gezicht. De bepaling van het wel/niet toegang geven zal door de QR-module worden uitgevoerd.

Op dit moment wordt de hierboven beschreven vorm van biometrische toegangspoortjes nog enkel toegepast voor de toegangscontrole tot het stadion. In dit rapport zal evenwel ook worden bezien in hoeverre het juridisch haalbaar is om deze techniek toe te passen ter handhaving van stadionverboden door de BVO.

2.3 Wij zijn tot bovengenoemde casussen gekomen door interviews te houden met twee Nederlandse BVO's. Het eerste interview was met een BVO die op dit moment gebruik maakt van een app waarin mensen zich moeten registreren voordat zij een ticket kunnen accepteren en kunnen gebruiken om toegang te krijgen tot het stadion. Het andere interview was met een BVO die op dit moment naast normale toegangspoortjes ook experimenteert met biometrische toegangspoortjes. Bij deze interviews waren ook de ontwikkelaars van de app resp. de biometrische toegangspoortjes aanwezig.

3 TOEPASSELIJKHEID VAN DE AVG: WORDEN ER PERSOONSGEGEVENS VERWERKT?

3.1 Voordat wordt toegekomen aan een inhoudelijke beoordeling van de toelaatbaarheid van de inzet van (digitale) preregistratie resp. biometrische toegangspoortjes in BVO's, is allereerst van belang om vast te stellen of en zo ja, in hoeverre de AVG en/of eventuele aanvullende sectorale gegevensbeschermingswetgeving van toepassing is.

3.2 De AVG is van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[2]

3.3 Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbaar natuurlijk persoon. Als een identificeerbaar persoon wordt beschouwd iedere informatie die direct (bijvoorbeeld een naam, adres of telefoonnummer), dan wel indirect (bijvoorbeeld een Burgerservicenummer ('BSN')) herleidbaar is tot een natuurlijke persoon.[3] Van een persoonsgegeven is aldus snel sprake.

3.4 Voor de vraag of sprake is van identificeerbaarheid moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de partij of door derden om de persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken. Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen.[4] Niet relevant is of die middelen daadwerkelijk worden ingezet. Van 'anonieme' gegevens is pas sprake indien de identificatie van de betrokkene bij de wet verboden of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt.

3.5 Alleen gegevens die daadwerkelijk niet meer tot individuele personen terug te herleiden zijn (re-identificatie), zullen kwalificeren als *anonieme gegevens* waarop de AVG niet (langer) van toepassing is. In dat geval is er, met andere woorden, geen sprake meer van een persoonsgegeven. Herleidbaarheid dient aldus onomkeerbaar te zijn uitgesloten. Wij benadrukken dat deze toets dient te worden verricht voor zowel de verstrekker als de ontvanger van de data. Het is niet uitgesloten dat voor de verstrekker van een dataset sprake is van 'gepseudonimiseerde gegevens', terwijl voor de ontvanger sprake is van anonieme gegevens.

> Wij wijzen in dit verband op HvJ EU 26 april 2023, T-557/20, ECLI:EU:T:2023:219, waarin het Europese Hof van Justitie ('HvJ') oordeelt dat het enkele feit dat een verstrekker van een gepseudonimiseerde dataset beschikt over een pseudonimiseringsleutel onvoldoende is om te concluderen dat (ook) de ontvanger (Deloitte) van deze gepseudonimiseerde dataset

[2] Zie artikel 2, eerste lid, AVG.
[3] In definitie van het begrip persoonsgegeven in de AVG wordt gesproken over identificatie "met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".
[4] Zie overweging 26 van de considerans van de AVG. Zie ook Hof van Justitie van de Europese Unie 19 oktober 2016, ECLI:EU:C:2016:779, C-582/14, par. 24 e.v.

'persoonsgegevens' verwerkt. Een dergelijke dataset kan voor de ontvanger anoniem zijn. Om een en ander vast te stellen is volgens het HvJ een juridische en technische analyse vereist vanuit de positie van de ontvanger. Om te bepalen of de doorgezonden informatie voor specifiek de ontvanger persoonsgegevens betreffen, is het aldus noodzakelijk om je te verplaatsen in de positie van de ontvanger teneinde te bepalen of de aan de ontvanger toegezonden informatie voor hem betrekking heeft op 'identificeerbare personen'. Er dient te worden onderzocht of de ontvanger over wettelijke (en in de praktijk uitvoerbare) middelen beschikt om toegang te krijgen tot de aanvullende gegevens die nodig zijn voor de heridentificatie.

3.6 Er bestaat veel discussie over de vraag wanneer sprake is van anonieme gegevens. In de Europese rechtspraak en de opinies van de Europese Toezichthouders (de European Data Protection Board (EDPB)[5]) en de nationale toezichthouder (de Autoriteit Persoonsgegevens ('AP')) wordt aangenomen dat vrijwel nooit sprake is van anonieme gegevens. Vooralsnog hanteren de EDPB en de AP[6] tot uitgangspunt dat het vrij lastig is – lees: vrijwel onmogelijk - om tot volledige anonimiteit te komen.

3.7 Een verwerking is iedere bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Dit betreft een zeer ruim begrip. Als voorbeelden noemt artikel 4, tweede lid, AVG onder meer het verzamelen, opslaan, bijwerken en doorzenden van persoonsgegevens.[7] Ook het enkel bezoeken en/of analyseren van persoonsgegevens betreft een verwerking in de zin van de AVG.

3.8 Het verdient aanbeveling om ten aanzien van de vraag of er sprake is van anonieme persoonsgegevens een technische audit uit te laten voeren. Door middel van zo'n technische audit zou dan kunnen worden aangetoond dat de gegevens daadwerkelijk niet meer tot individuele personen terug te herleiden zijn (re-identificatie).

Casus 1: Digitale preregistratie (IBA)

Bij casus 1 wordt gebruik gemaakt van een decentrale opslag van de persoonsgegevens van de betrokkene in de app op zijn telefoon. Van een verwerking door de BVO is slechts sprake voor zover hij (of diens verwerker) beschikt over redelijkerwijs in te zetten middelen om toegang te krijgen tot de decentraal opgeslagen persoonsgegevens.

In de fase van de registratie en het betreden van het stadion, wordt op een centrale wijze persoonsgegevens verwerkt van toeschouwers. Het kan daarbij (onder meer) gaan om het verwerken van persoonsgegevens zoals naam, geboortedatum, email

5 Voorheen was de EDPB de Artikel 29-Werkgroep.

6 In meerdere adviezen en boetebesluiten wordt bij de bespreking van 'geanonimiseerde gegevens' verwezen naar het advies over anonimiseringstechnieken van de Artikel 29-Werkgroep en de daarin gehanteerde definitie van anonimiseren. Zie onder meer het boetebesluit van 11 maart 2021 van de Autoriteit Persoonsgegevens gericht aan de gemeente Enschede over wifitracking Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf. Autoriteit Persoonsgegevens, 'Microsoft Windows 10. De verwerking van persoonsgegevens via telemetrie', Rapport definitieve bevindingen 29 augustus 2017met correcties 6 oktober 2017. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_onderzoek_microsoft_windows_10_okt_2017.pdf. Autoriteit Persoonsgegevens, 'Normenkader digitale billboards', 25 juni 2018. Raadpleegbaar via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_branche_normkader_digitale_billboards.pdf.

7 Zie voor de volledige opsomming artikel 4, tweede lid, AVG: "verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."

adres en pasfoto. De BVO is verwerkingsverantwoordelijke voor de verwerkingen die ten behoeve van IBA plaatsvinden.

Casus 2: Preregistratie met biometrische identificatie

Voor casus 2 geldt hetzelfde als casus 1. Een verschil is dat bij casus 2 sprake is van een decentrale verwerking van gegevens. Een belangrijk verschil is bovendien dat bij de preregistratie met biometrische identificatie ook en vergelijking tussen de face vector van de foto en de face vector van de selfie wordt gemaakt binnen de app van de gebruiker. Van een verwerking door de BVO is slechts sprake voor zover hij beschikt over redelijkerwijs in te zetten middelen om toegang te krijgen tot de decentraal opgeslagen persoonsgegevens.

Casus 3: Biometrische toegangspoortjes

In geval van de in casus 3 beschreven vorm van biometrische toegang, wordt gebruik gemaakt van de decentrale opslag van persoonsgegevens van de betrokkene in de app op zijn telefoon. Ook de selfie en daaruit afgeleide (code van de) face vector worden in beginsel eerst enkel decentraal opgeslagen. De hiervoor beschreven gegevens zijn met encryptie versleuteld. Deze decentraal (geëncrypte) persoonsgegevens kunnen daardoor niet worden uitgelezen door de beheerder.

Voor de beheerder zal er ten aanzien van de decentraal opgeslagen versleutelde gegevens toch sprake zijn van de verwerking van persoonsgegevens, voor zover de beheerder beschikt over middelen om de encryptie ongedaan te maken.

Van de verwerking van gepseudonimiseerde persoonsgegevens door de beheerder is in ieder geval sprake op het moment dat de code van de face vector centraal wordt opgeslagen in de database van de beheerder. Het valt wat ons betreft niet uit te sluiten dat de beheerder, eventueel door middel van bestandskoppeling of aan de hand van metadata, (indirect) kan vaststellen op wie de code betrekking heeft. Ook in deze fase dient er dus vanuit te worden gegaan dat de beheerder gepseudonimiseerde persoonsgegevens verwerkt en (door)verstrekt ten behoeve van de controles die via de poortjes plaatsvinden. Ook hier geldt dat de versleuteling naar verwachting niet maakt dat sprake is van anonieme gegevens. Zowel voor de app beheerder als de BVO vormt de code van de Face vector naar verwachting een gepseudonimiseerd persoonsgegeven.

Doordat de beheerder optreedt als verwerker van de BVO, heeft de BVO beslissende zeggenschap over het doel en de middelen. De BVO/het voetbalstadion treedt daarbij op als verwerkingsverantwoordelijke en dient te beschikken over een wettelijke grondslag. Wij benadrukken dat eventuele contractuele afspraken dat de encryptie niet wordt teruggedraaid of dat de beheerder geen aanvullende informatie aan de BVO verstrekt, niet tot gevolg hebben dat de BVO geen persoonsgegevens verwerkt. Het is voor de BVO in ieder geval mogelijk om de identiteit van de persoon te koppelen aan de code van de Face vector die door het biometrische poortje wordt gecontroleerd.

Persoonlijk of huishoudelijk gebruik?

3.9 In casus 1 en 2 worden persoonsgegevens decentraal opgeslagen in de app van de bezoeker. In de praktijk rijst geregeld de vraag of de verwerking van de persoonsgegevens in de afgesloten app valt onder de materiële reikwijdte van de AVG. Meer concreet gaat het daarbij om de vraag of de verwerking in de afgesloten app kan worden aanmerkt als 'zuiver persoonlijk of huishoudelijk gebruik'. Artikel 2, tweede lid, aanhef en onder c, AVG bepaalt namelijk dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. De Europese wetgever legt deze uitzondering op de AVG strikt uit.

Zie Overweging 18 van de AVG:

"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. Tot persoonlijke of huishoudelijke activiteiten kunnen behoren het voeren van correspondentie of het houden van adresbestanden, het sociaal netwerken en online-activiteiten in de context van dergelijke activiteiten. Deze verordening geldt wel voor verwerkingsverantwoordelijken of verwerkers die de middelen verschaffen voor de verwerking van persoonsgegevens voor dergelijke persoonlijke of huishoudelijke activiteiten."

3.10 Deze strikte uitleg is in diverse uitspraken van het Hof van Justitie bevestigd. Bepalend is dus datde activiteit van de persoon uitsluitend gericht is op persoonlijke of huishoudelijke doeleinden.

Zie HvJ EU 11 december 11 december 2014, Ryneš, C-212/13, EU:C:2014:2428, par. 30 en 33:

"deze bepaling onttrekt niet de gegevensverwerking die in activiteiten met gewoonweg persoonlijke of huishoudelijke doeleinden wordt verricht, maar wel die welke in activiteiten met „uitsluitend" persoonlijke of huishoudelijke doeleinden wordt verricht, aan de werkingssfeer van deze richtlijn"

3.11 Of ook de (decentrale) opslag van (biometrische) gegevens in bovengenoemde casussen valt onder de uitzondering van zuiver persoonlijk gebruik, kan niet in algemene zin worden vastgesteld. Deze vraag is vooralsnog niet expliciet aan de orde geweest in de opinies of besluiten van de AP of de Europese of nationale rechtspraak. De Franse Europese toezichthouder ('CNIL') heeft daarentegen een nuttige richtlijn gepubliceerd aan de hand waarvan zij toelicht wanneer de verwerking van biometrische persoonsgegevens in apparaten (met name de verwerking van iemands vingerafdruk voor het ontgrendelen van een smartphone) valt onder de reikwijdte van de uitzondering van zuiver persoonlijk gebruik.[8] CNIL maakt daarbij onderscheid tussen twee soorten systemen.

De eerste categorie betreft de situatie waarbij de biometrische analyse c.q. code is opgeslagen in het apparaat, onder de uitsluitende controle van de persoon (in een volledige afgescheiden omgeving). Het gaat hier bijvoorbeeld om de volledige autonome verwerking van iemands vingerafdruk voor het openen van zijn mobiel of voor de toegang tot een app.

De tweede categorie betreft apps of apparaten die werken vanaf een externe server of daarmee in verbinding staan. Voor dergelijke apparatuur en apps neemt CNIL tot uitgangspunt dat de verwerking niet onder de uitzondering van persoonlijk gebruik valt. Dit is slechts anders indien wordt voldaan aan de volgende strikte randvoorwaarden:

1. de gebruiker gebruikt de app resp. het apparaat privé (bijv. om toegang te krijgen tot apps die hij uit eigen beweging heeft gedownload);
2. de gebruiker beslist zelfstandig om de in zijn apparaat ingebouwde biometrie te gebruiken. Dit sluit elke opgelegde biometrische authenticatie uit (met name door werkgevers);
3. de biometrische code wordt opgeslagen in het apparaat in een afgesloten omgeving en is niet toegankelijk voor de app beheerder en wordt ook niet extern verzonden. Zodra een van biometrie afgeleide code naar een externe

[8] https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees.

database wordt gestuurd of de app beheerder technisch bij de gegevens kan, valt de verwerking niet langer onder zuiver persoonlijk gebruik;
4. de biometrische code wordt versleuteld opgeslagen in de app of het apparaat met behulp van geavanceerde encryptie en sleutelbeheer;
5. tijdens de controle of validatie van de identiteit wordt alleen een token of gegeven verzonden aan de beheerder dat aangeeft dat de biometrische vergelijking is geslaagd (of juist niet).

CNIL benadrukt dat zodra de biometrische controle in de app of apparatuur van de gebruiker in wisselwerking staat met externe servers van een derde (bijvoorbeeld die van de appbeheerder), deze derde gehouden is om te voldoen aan de verplichtingen van de AVG. Ook voor zover deze derde de zeggenschap heeft over de implementatie van de biometrische authenticaties of de controle heeft over alle of een deel van de biometrische verwerkingsmiddelen (bijvoorbeeld de biometrische lezer of de database voor het opslaan van het sjabloon), is de beheerder als verwerkingsverantwoordelijke gebonden aan de AVG. Van een zuiver persoonlijk gebruik is in dat geval geen sprake.

De AP heeft de richtlijnen van CNIL (vooralsnog) niet overgenomen. Het is in zoverre dus onduidelijk of de AP dezelfde mening is toegedaan als CNIL. Er bestaat dus de mogelijkheid dat de AP tot een andere uitleg komt dan CNIL.

3.12 Hoewel wij dit niet geheel uitsluiten, is onze eerste indruk dat de verwerking van de (biometrische) persoonsgegevens in de app van de gebruiker (casus 1 en 2) niet snel onder de uitzondering van zuiver persoonlijk gebruik zal vallen. De verwerking houdt immers verband met een commerciële activiteit, namelijk het vaststellen van de identiteit en het toegangsrecht van de bezoeker ten behoeve van een specifieke voetbalwedstrijd. Het doel van de verwerking is niet uitsluitend een persoonlijk gebruik. In geval van casus 3 is *in ieder geval* geen sprake van zuiver persoonlijk gebruik, aangezien daarbij gegevens uit de app worden uitgewisseld met externe servers van de app-beheerder.

4 BIJZONDERE PERSOONSGEGEVENS

4.1 Bijzondere persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn. Het gaat bijvoorbeeld om gegevens over iemands gezondheid, ras, etniciteit, politieke opvatting of seksuele gerichtheid. Ook biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van een persoon betreffen bijzondere persoonsgegevens.[9] Gegevens over nationaliteit zijn niet zonder meer bijzondere persoonsgegevens over iemands ras of etniciteit. De termen 'ras' en 'etnische afkomst' worden niet gedefinieerd in de AVG. Door de AP wordt echter aangenomen dat voor een omschrijving van 'ras' moet worden aangeknoopt bij verschillende kenmerken die van fysieke (bijv. huidskleur), etnische, geografische, culturele, historische of godsdienstige aard kunnen zijn.

4.2 Het staat op grond van de AVG vast dat gegevens die indirect informatie onthullen over iemands ras of etnische afkomst valt aan te merken als een indirect bijzonder persoonsgegevens. Het verbod op de verwerking van bijzondere persoonsgegevens is in een dergelijk geval onverkort van toepassing. De AP stelt voorop dat nationaliteit op zichzelf niet kwalificeert als een gegeven over iemands ras of etnische afkomst, omdat er geen direct verband bestaat met iemands nationaliteit. Nationaliteit is namelijk slechts een staatsrechtelijke term. Nationaliteit op zichzelf bezien geeft daarmee hooguit een indicatie dat het om ras of etnische afkomst zou kunnen gaan.

[9] Zie artikel 9, eerste lid, AVG voor een limitatieve opsomming van de persoonsgegevens die als bijzondere persoonsgegevens kwalificeren.

4.3 In sommige gevallen kan nationaliteit echter wel een indirect gegeven vormen over iemands ras of etnische afkomst.

4.4 Voor het antwoord op de vraag of nationaliteit een (indirect) bijzonder persoonsgegeven betreft, is allereerst van belang welke overige persoonsgegevens in combinatie met de nationaliteit van de betreffende persoon worden verwerkt. "Indien nationaliteit wordt verwerkt in combinatie met bijvoorbeeld geboorteland, geboorteplaats, herkomst en/of pasfoto, wordt in rechtspraak aangenomen dat er wel sprake is van gegevens waaruit het ras of de etnische afkomst blijkt."[10] De AP verwijst in dit verband naar rechtspraak van onder meer de Afdeling.[11]

4.5 Ook de context van de verwerking kan volgens de AP ertoe leiden dat de nationaliteit van een persoon moet worden aangemerkt als een (indirect) bijzonder persoonsgegeven. De AP beschouwt nationaliteit als bijzonder persoonsgegeven wanneer de verwerking tot doel heeft om onderscheid te maken naar ras of etnische afkomst, of indien het voor de verwerkingsverantwoordelijke redelijkerwijs voorzienbaar is dat de verwerking tot het maken van onderscheid naar ras of etnische afkomst zal leiden.[12]

Welke gegevens zijn te kwalificeren als bijzondere persoonsgegevens?

Het verwerken van een foto van de betrokkene vormt niet zonder meer een verwerking van ras of etniciteit, en betreft aldus geen verwerking die valt onder het regime van bijzondere persoonsgegevens.

Zie 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".

De AP beschouwt beelden van personen niet als een bijzonder persoonsgegevens als:

"het doeleinde van de verwerking niet gericht is op het verwerken van bijzondere persoonsgegevens dan wel op het onderscheid maken op grond van een bijzonder persoonsgegeven; het voor de verantwoordelijke redelijkerwijs niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van een bijzonder persoonsgegeven; en de verwerking van die bijzondere persoonsgegevens onvermijdelijk is bij die verwerking. Indien de verwerking van camerabeelden echter identificatie tot doel heeft, worden deze beelden wel als een rasgegeven aangemerkt."[13]

---

10 Zie Onderzoeksrapport AP 'Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag' d.d. 17 juli 2020, p. 35.

11 Zie overweging 5 van de uitspraak van de rechtbank Rotterdam van 16 mei 2012 (ECLI:NL:RBROT:2012:BW5513), overweging 4.1 van de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 13 augustus 2014 (ECLI:NL:RVS:2014:3002) en overweging 13 tot en met 16 van de uitspraak van de rechtbank Rotterdam van 11 september 2018 (ECLI:NL:RBMNE:2018:4404). Deze overige verwerkte gegevens zijn bijvoorbeeld: geboorteland, geboorteplaats, herkomst en/of pasfoto.

12 De AP verwijst in dat verband naar Kamerstukken II 1997/98, 25892, nr. 3, p. 106: "Indien een school bij voorbeeld met het oog op de identificatie van de leerlingen van hen allen de geboorteplaats in de administratie opneemt, vloeit uit deze verwerking, indien het gaat om de geboorteplaats in het buitenland, niet rechtstreeks een gevoelig gegeven voort. De verwerking heeft niet plaats gevonden met het doel om de mogelijk andere etnische herkomst van de leerlingen te registreren. Dit laat de mogelijkheid open dat dergelijke gegevens, mogelijk door vergelijking met andere gegevens, alsnog worden gebruikt om gegevens omtrent ras te herleiden." Ook in het kader van het verwerken van nationaliteit concludeerde de AP al in 2016 dat: "Gezien de gevoelige ondertoon die het verwerken van het gegeven nationaliteit heeft bij het selecteren of screenen van kandidaten, kan het verwerken van het gegeven nationaliteit binnen de context van een screeningsprocedure daarom niet anders worden beschouwd dan het verwerken van een rasgegeven".
Zie:https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_rapport_db_hoffmann_openbare_versie_21062016_def.pdf.

13 Zie Beleidsregels cameratoezicht, College bescherming persoonsgegevens, artikel 2.11.

De Hoge Raad heeft bij uitspraak van 27 juni 2017 (impliciet) geoordeeld dat de verwerking van camerabeelden met als doel het herkennen van een persoon geen verwerking van bijzondere persoonsgegevens impliceert.[14] In deze uitspraak ging het over de vraag of het vorderen van beelden van een beveiligingscamera bij een pinautomaat een vordering betrof van een gevoelig gegeven. In zijn conclusie oordeelt de A-G van niet:

"Een ongenuanceerde uitleg van deze overwegingen zou ertoe leiden dat opnamen van beveiligingscamera's per definitie gevoelige gegevens bevatten, omdat uit die opnamen het ras van de afgebeelde persoon is op te maken. Dat lijkt mij overtrokken. Het komt mij voor dat het de bedoeling is geweest te voorkomen dat via een eenvoudige vordering persoonsgegevens beschikbaar zouden komen die door onderlinge vergelijking en combinatie, bijvoorbeeld van namen, adressen en identificatiefoto's, de conclusie zouden mogelijk maken dat deze met naam en toenaam bekend geworden persoon tot een bepaald ras behoort. Het bekijken van opnames van beveiligingscamera's met het oog op een mogelijke herkenning van een afgebeelde persoon is van geheel andere orde. Als een politieambtenaar de afgebeelde persoon herkent betekent dat niet dat deze politieambtenaar pas door het bekijken van de afbeeldingen de conclusie kan trekken dat de persoon die hem bekend is een voorheen aan de politieambtenaar onbekende eigenschap vertoont, te weten dat hij tot een bepaald ras behoort."[15]

Al met al achten wij het verdedigbaar dat de verwerking van foto's van personen in casus 1 (IBA), niet zal leiden tot de verwerking van bijzondere persoonsgegevens. Zelfs voor zover de foto's van bezoekers door de club zouden worden gebruikt voor identificatie, leidt dat niet zonder meer tot de verwerking van een rasgegeven. In casus 1 gaat het immers om het opslaan en eventueel bekijken van de foto's met het oog op de mogelijke herkenning van de afgebeelde persoon (bijvoorbeeld naar aanleiding van een incident of ter controle van het stadionverbod). Uit de Hoge Raad uitspraak lijkt te volgen dat een dergelijk spontane herkenning niet leidt tot de verwerking van een rasgegeven. Ook voor zover dit onverhoopt anders mocht zijn, dan nog leidt deze vaststelling niet tot de onrechtmatige verwerking van een bijzonder persoonsgegeven.

De BVO zal naar verwachting namelijk een beroep toekomen op de uitzondering van artikel 25 UAVG dat bepaalt dat het verbod op de verwerking van gegevens over ras of etnische afkomst niet van toepassing is, indien de verwerking geschiedt met het oog op de identificatie van de betrokkene, en slechts voor zover de verwerking voor dat doel onvermijdelijk is.

Het maken van een biometrische vergelijking van een foto van een identiteitsbewijs van een betrokkene met een selfie (het opzetten van een face vector) is wel een verwerking van biometrische gegevens, dus van bijzondere persoonsgegevens. Ook het gebruik van poortjes waarbij ter identificatie van een vingerafdruk of een handpalm wordt gescand, levert de verwerking van biometrische persoonsgegevens op.

Het maken van onderscheid tussen supporters van een specifieke voetbalclub betreft geen (indirect) onderscheid op ras of etniciteit. De verwerking van dergelijke gegevens kwalificeert dan ook niet als de verwerking van bijzonder persoonsgegevens.

Als er wel onderscheid wordt gemaakt naar nationaliteit (geen Belgische supporters) kan dat een (indirect) bijzonder persoonsgeven vormen over iemands ras of etniciteit indien dat volgt uit de context van de verwerking, of als dat gegeven wordt gebruikt om te selecteren op ras of etniciteit.

[14] Zie HR 27 juni 2017, ECLI:NL:HR:2017:1166.
[15] Zie Conclusie A-G Machielse van 27 juni 2017, ECLI:NL:PHR:2017:547.

Ook als er sprake is van de verwerking van bijzondere persoonsgegevens, leidt die vaststelling er niet toe dat het onderscheid juridisch mag plaatsvinden. Een dergelijk onderscheid kan namelijk alsnog leiden tot verboden onderscheid of discriminatie zoals bedoeld in artikel 14 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 1 van het Twaalfde Protocol bij het EVRM (Twaalfde Protocol). Voor een (indirect) onderscheid op nationaliteit dient een gerechtvaardigd doel te bestaan en dient proportioneel te zijn in het licht van het nagestreefde doel. De bewijslast rust op de partij die het onderscheid maakt. Volgens het Europees Hof van de Rechten van de Mens ('EHRM') is een dergelijk onderscheid op nationaliteit slechts toelaatbaar als daarvoor 'very weighty reasons' bestaan.[16] Het Hof van Justitie volgt een vergelijkbaar criterium. Als onderscheid wordt gemaakt op basis van nationaliteit, dan is dat onderscheid enkel gerechtvaardigd indien het is gebaseerd op objectieve overwegingen, die losstaan van de nationaliteit van de betrokken personen. Het verdient aldus aanbeveling om altijd op voorhand te controleren of eventuele maatregelen gericht tegen specifieke voetbalfans met een bepaalde nationaliteit niet leidt tot verboden onderscheid.

4.6 Op grond van artikel 9, eerste lid, AVG is het verboden om bijzondere persoonsgegevens te verwerken, tenzij de verwerking kan worden gebaseerd op een doorbrekingsgrond (ook wel: uitzonderingsgrond).

4.7 De algemene uitzonderingsgronden op het verbod om **bijzondere persoonsgegevens** te verwerken, staan beschreven in artikel 9 AVG en de artikelen 22 tot en met 33 van de UAVG. Ook een bijzondere wet kan een doorbrekingsgrond voor het verwerken van bijzondere persoonsgegevens bevatten. In dit rapport worden de volgende doorbrekingsgronden besproken:

- Uitdrukkelijke toestemming (artikel 9, tweede lid, aanhef en onder a, AVG jo. artikel 22, tweede lid, aanhef en onder a, UAVG).
- Biometrische gegevens ten behoeve van authenticatie en beveiligingsdoeleinden (artikel 9, tweede lid, aanhef en onder g, AVG jo. artikel 29 UAVG).

Uitdrukkelijke toestemming

4.8 De verwerking van biometrische gegevens zou allereerst gebaseerd kunnen worden op uitdrukkelijke toestemming. Van rechtsgeldige, uitdrukkelijke toestemming in de zin van artikel 9, tweede lid, aanhef en onder a, AVG is sprake indien de toestemming van de bezoeker (a) vrijelijk, (b) specifiek, (c) geïnformeerd en (d) op een ondubbelzinnige wijze is verkregen.

Ad a. Vrijelijk

4.9 De eerste voorwaarde, (i) vrijelijke toestemming, houdt in dat de bezoeker daadwerkelijk een vrije keuze moet hebben of hij toestemming geeft voor de verwerking van zijn persoonsgegevens. Een belangrijke eis daarbij is dat de bezoeker geen nadelige gevolgen ondervindt indien hij zijn toestemming weigert of intrekt.[17] De AVG gaat slechts beperkt in op de vraag wat moet worden verstaan onder 'nadelige gevolgen'. Volgens de EDPB kan er worden gesproken van 'nadeel' voor zover het niet verlenen van toestemming leidt tot hoge kosten of het (ten nadele van de betrokkene) bijstellen van de overeenkomst. Andere voorbeelden van 'nadeel' zijn bedrog, intimidatie, dwang of aanzienlijke negatieve gevolgen voor de betrokkene. Indien de betrokkene bij het intrekken van zijn toestemming slechts een mogelijk extra voordeel

[16] Zie onder meer EHRM 18 februari 2009, nr. 55707/00 (Andrejeva/Latvia), par. 87.
[17] Vgl. Overwegingen 42 AVG: "Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen." Zie tevens: Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 5-6.

verliest, is geen sprake van een nadeel.[18] Ook voor zover met biometrisch toegangspoortje sneller toegang zou kunnen worden verkregen tot het stadion, is dat onvoldoende om te kunnen spreken van een 'nadeel' voor personen die niet hun toestemming verlenen. Voorts is van belang dat de toestemming *apart* moet worden gevraagd. Het verzoek om toestemming mag niet zijn verstopt in bijvoorbeeld de algemene voorwaarden of een contract. Het verzoek om toestemming voor de verwerking van persoonsgegevens moet duidelijk te onderscheiden zijn.[19]

Ad b. Specifiek

4.10 De tweede voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming gespecificeerd moet zijn: er moet om specifieke, gerichte toestemming worden gevraagd. Het toestemmingsformulier moet zo zijn vormgegeven dat de bezoeker zijn toestemming per verwerkingsverantwoordelijke, per doel en per type persoonsgegevens kan differentiëren.[20] De doeleinden mogen niet zodanig vaag zijn dat zij na het verkrijgen van toestemming ruimer zouden kunnen worden geïnterpreteerd.

Ad c. Geïnformeerd

4.11 De derde voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat sprake moet zijn van geïnformeerde toestemming. De bezoeker dient voorafgaand aan het verlenen van zijn toestemming uitvoerig te zijn geïnformeerd over de beoogde verwerking (met slimme technologieën), zodat hij een geïnformeerde beslissing kan nemen of hij al dan niet zijn toestemming verleent. De AVG schrijft niet voor op welke wijze de hiervoor genoemde informatie moet worden gegeven. De wijze waarop om toestemming wordt gevraagd is in zoverre vormvrij. Dat neemt niet weg dat bepaalde kwaliteitseisen gelden ten aanzien van de inhoud van de informatie. Zo moet het verzoek om toestemming in een begrijpelijke en gemakkelijke toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd.[21]

Ad d. 'Ondubbelzinnig'

4.12 De laatste voorwaarde voor het verkrijgen van rechtsgeldige toestemming is dat de toestemming ondubbelzinnig – door middel van een actieve handeling – moet zijn geuit. Er dient kortom altijd sprake te zijn van een 'opt-in'. De wijze waarop dit moet gebeuren, is in principe vormvrij. Het actief kunnen aankruisen van een vakje is in de ogen van de Europese privacy toezichthouders voldoende. Een al aangevinkt vakje dat kan worden uitgezet (een 'opt-out') is niet voldoende.

4.13 De term 'uitdrukkelijk' verwijst naar de manier waarop toestemming door de bezoeker tot uitdrukking wordt gebracht. Het betekent dat de bezoeker een uitdrukkelijke verklaring van toestemming moet geven, vaak via een digitale of schriftelijke verklaring.[22]

> Een schriftelijke en ondertekende verklaring is niet altijd vereist. In de digitale of online context kan een bezoeker bijvoorbeeld toestemming geven door het invullen van een elektronisch formulier, het versturen van een e-mail, het uploaden van een gescand document met handtekening, of door middel van een elektronische handtekening. Mondelinge verklaringen kunnen in theorie ook voldoende zijn, maar het kan lastig zijn voor de BVO om te bewijzen dat aan alle voorwaarden voor geldige uitdrukkelijke toestemming is voldaan. Een organisatie kan ook toestemming verkrijgen via een telefoongesprek, waarbij de keuze duidelijk en begrijpelijk wordt uitgelegd en

[18] Artikel-29 Werkgroep, 'Guidelines on consent under Regulation 2016/679' van 10 april 2018, WP259 rev. 01, p. 14.
[19] Vgl. Artikel 7, vierde lid, AVG jo. overweging 43 AVG
[20] Daarbij kan gebruik worden gemaakt van afzonderlijke (digitale) formulieren per betrokkene.
[21] Artikel 7, tweede lid, AVG.
[22] Zie ook WP29 Advies 15/2011 over de definitie van 'toestemming' (WP 187), blz. 25.

de bezoeker om specifieke bevestiging wordt gevraagd (bijvoorbeeld door een knop in te drukken of mondeling bevestiging te geven).

Ook Tweestapsverificatie kan worden gebruikt om de geldigheid van de toestemming te waarborgen. Bijvoorbeeld, een bezoeker ontvangt een e-mail waarin wordt uitgelegd dat de BVO van plan is om bijzondere gegevens te verwerken. Als de betrokkene instemt, wordt hem of haar gevraagd om de e-mail te beantwoorden met de boodschap "Ik ga akkoord". Vervolgens ontvangt de bezoeker een verificatielink of een sms met een verificatiecode om de toestemming te bevestigen.

Ad d. Toestemmingsregister

4.14 De BVO's moet verder kunnen aantonen dat zij de bovenstaande toestemming heeft verkregen.[23] Een manier waarop de BVO's dit kunnen waarborgen, is door een register bij te houden van de ontvangen toestemmingsverklaringen. Dit register kan informatie bevatten over hoe toestemming is verkregen, wanneer dit is gebeurd en welke informatie aan de betrokkene is verstrekt. Om aan te kunnen tonen dat bezoekers goed zijn geïnformeerd verdient het per toestemming aanbeveling om een kopie of een vermelding van de versie van de privacyverklaring ten tijd van het vragen van toestemming te registreren.

Ad e. Intrekken toestemming

4.15 Bezoekers behouden altijd het recht om de door hen verleende toestemming in te trekken. Artikel 7 lid 3 AVG bepaalt in dat kader dat de BVO's ervoor moeten zorgen dat het intrekken van toestemming door een bezoeker net zo gemakkelijk moet zijn als het geven ervan. Hoewel de AVG niet vereist dat het geven en intrekken van toestemming altijd op dezelfde manier plaatsvindt, ligt dat bij elektronische toestemming wel in de rede. Als toestemming wordt verkregen via een specifieke gebruikersinterface (zoals een website, app, gebruikersaccount, IoT-apparaatinterface of e-mail), is het duidelijk dat de bezoeker zijn of haar toestemming via dezelfde elektronische interface moet kunnen intrekken. Ook hier geldt dat de betrokkene zijn of haar toestemming kunnen intrekken zonder enig nadeel. Dit betekent dat de BVO's ervoor moet zorgen dat het intrekken van toestemming kosteloos is en dat dit geen negatieve invloed mag hebben op het serviceniveau.[24]

4.16 Als algemene regel geldt verder dat als toestemming wordt ingetrokken, alle verwerkingen van de gegevens die overeenkomstig de AVG waren gebaseerd op toestemming en plaatsgevonden hebben voordat de toestemming werd ingetrokken, rechtmatig blijven, maar de BVO's wel moet stoppen met de desbetreffende verwerkingsactiviteiten. Als er geen andere rechtsgrond is voor de verwerking (bijv. verdere opslag) van de gegevens, moeten deze door de verwerkingsverantwoordelijke worden gewist.

4.17 In gevallen waarin de bezoeker zijn of haar toestemming intrekt en de BVO's op basis van een andere rechtsgrond door willen gaan met de verwerking van de persoonsgegevens, kan een BVO niet stilzwijgend overschakelen van toestemming (die ingetrokken is) op deze andere rechtsgrond. Elke wijziging van de rechtsgrond voor verwerking moet aan de bezoekers worden meegedeeld overeenkomstig de informatievereisten in de artikelen 13 en 14 en op grond van het algemene beginsel van transparantie.

---

[23] Zie Overweging 42 van de AVG: "Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking."

[24] Zie ook WP29 Advies 4/2010 over de Europese gedragscode van FEDMA voor het gebruik van persoonsgegevens in het kader van direct marketing (WP174) en het Advies over het gebruik van locatiegegevens voor het verstrekken van diensten met toegevoegde waarde (WP 115).

4.18 Met andere woorden, de BVO's kunnen niet van toestemming op een andere rechtsgrond overstappen. Het is bijvoorbeeld niet toegestaan om achteraf de rechtsgrond 'rechtmatig belang' te gebruiken ter rechtvaardiging van verwerking wanneer problemen zijn ondervonden met de geldigheid van toestemming. Uit het voorgaande volgt dat uitdrukkelijke toestemming weliswaar een grondslag kan vormen voor het voetbalstadion, maar tegelijkertijd ook een onbetrouwbare grondslag kan vormen, omdat bezoekers dit op ieder moment kunnen intrekken.

Artikel 29 UAVG

4.19 BVO's mogen op grond van artikel 9, eerste lid, aanhef en onder g, AVG jo. artikel 29 UAVG biometrische gegevens verwerken als dat noodzakelijk is voor authenticatie- of beveiligingsdoeleinden. De vervolgens te beantwoorden vraag is of de voorgenomen verwerking van de BVO noodzakelijk is voor deze authenticatie- en beveiligingsdoeleinden, dat wil zeggen: of deze verwerking voldoet aan vereisten van proportionaliteit en subsidiariteit. Voor de proportionaliteitstoets gaat het erom dat er een redelijke en evenwichtige verhouding is tussen enerzijds het belang bij een goede authenticatie en beveiliging en anderzijds de privacybelangen van de werknemers. Voor de subsidiariteitstoets gaat het erom of er geen gebruik kan worden gemaakt van andere, minder ingrijpende methoden voor de authenticatie en beveiliging.

4.20 In de parlementaire geschiedenis van de UAVG wordt ingegaan op de noodzakelijkheid van de inzet van biometrie als authenticatie of beveiligingsmiddel in te zetten.

> Zie *Kamerstukken II* 2017/18, 34851, nr. 3, p. 109:
>
> "Er dient […] een afweging te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen."

Duidelijk is dat de wetgever de werking van deze uitzondering heeft willen beperken tot uitzonderlijke situaties (kerncentrales) waarin de inzet van biometrie wordt gerechtvaardigd door de aanwezigheid van concrete en zwaarwegende veiligheidsrisico's. Voor meer alledaagse gevallen (garage van een reparatiebedrijf)[25] biedt de uitzondering geen ruimte. Deze bandbreedte (tussen kerncentrales en reparatiebedrijven) is tamelijk ruim. Van belang bij de invulling daarvan is dat de wetgever, waar het gaat om systemen met veel persoonsgegevens, biometrie suggereert als een mogelijke goede beveiligingsmethode:

> "Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen."[26]

4.21 Van belang is tot slot dat momenteel een wetsvoorstel aanhangig is die zal leiden tot een tekstuele wijziging van artikel 29 UAVG; de Verzamelwet gegevensbescherming.

---

[25] Op de website van de Autoriteit persoonsgegevens wordt als voorbeeld van een situatie waarin biometrie als beveiligingsmethode niet is toegestaan nog het recreatiegebied genoemd.

[26] *Kamerstukken* II 2017/18, 34 851, nr. 3, p. 109.

Voor zover deze wet wordt aangenomen, zal dat leiden tot de volgende tekstuele wijziging:

> "In artikel 29 wordt «beveiligingsdoeleinden» vervangen door «omwille van beveiligingsdoeleinden en slechts voor zover dit noodzakelijk is vanwege een zwaarwegend algemeen belang van rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen"[27]

De wetgever heeft met deze tekstuele toevoeging van een extra waarborg willen voorzien:

> "Met het in de wettekst opnemen van de eis dat bij het gebruik maken van deze wettelijke uitzondering, het noodzakelijk is ook nog in het concrete geval te toetsen aan het bedoelde zwaarwegend algemeen belang, wordt in een extra waarborg voorzien. In de rechtspraktijk zal een verwerkingsverantwoordelijke nu telkens zelf actief moeten toetsen of ook in het specifieke geval wel aan het vereiste «noodzakelijk voor een zwaarwegend algemeen belang» is voldaan, voordat een beroep op de uitzondering kan worden gedaan. Deze afweging zal vervolgens door de AP en uiteindelijk ook door de rechter kunnen worden beoordeeld.
> (…)
> Met de dubbele noodzakelijkheidstoets (noodzakelijk voor de authenticatie of beveiligingsdoeleinden én noodzakelijk omwille van een zwaarwegend algemeen belang) wordt invulling gegeven aan de eis van artikel 9, tweede lid, onderdeel g, AVG, die passende en specifieke maatregelen vergt ter bescherming van grondrechten en de fundamentele belangen van betrokkene. Naast het benoemen van het criterium van het zwaarwegend algemeen belang in de wettekst wordt tevens voorgesteld om ook de doelbeperking expliciet te maken, namelijk de rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatie- of werkprocessystemen."[28]

> Wederom worden er allerlei voorbeelden aangehaald waarbij een geslaagd beroep kan worden gedaan op deze uitzondering. De handhaving van stadionverboden wordt niet genoemd:

> "De beveiliging van een kerncentrale is natuurlijk een aansprekend voorbeeld van een zwaarwegend algemeen belang. Maar ook het beschermen van de volksgezondheid, het voorkomen van milieuschade of het beveiligen van vitale processen kunnen redenen zijn waarmee aan de eis van zwaarwegend algemeen belang wordt voldaan. Naast het reeds genoemde voorbeeld van een kerncentrale, kan bij controle op toegangsbevoegdheden op vitale, gevoelige of gevaarlijke locaties, gedacht worden aan bedrijven en/of diensten uit de vitale infrastructuur (zoals telecomcentrum, beheercentrum energie-infra), aanbieders van essentiële diensten en voor digitale dienstverleners (NIS-Richtlijn34), bedrijven of gebieden met veiligheidsrisico's zoals bedrijven met veel risico's op zware ongevallen door de aanwezigheid van grote hoeveelheden gevaarlijke stoffen die onder het Besluit risico's zware ongevallen35 vallen en lucht- en zeehavens."[29]

4.22 De Europese privacytoezichthouders, verenigd in de Artikel 29 Werkgroep ("de werkgroep") gaan uit van een beperkte werking van de uitzondering. In een advies over biometrische technologie stelt de werkgroep zich op het standpunt dat de inzet van biometrie niet snel zal zijn toegestaan voor 'gewone beveiliging van goederen en

[27] *Kamerstukken II* 2022/23, 36 264, nr. 2, p. 4.
[28] *Kamerstukken II* 2022/23, 36 264, nr. 3, p. 23.
[29] *Kamerstukken II* 2022/23, 36 264, nr. 3, p. 23.

personen', alsmede dat de inzet van biometrie vereist dat er aantoonbaar sprake is van 'hoogrisicosituaties'. Een voorbeeld daarvan betreft, aldus blijkt uit dit advies, 'een laboratorium waarin onderzoek wordt gedaan naar gevaarlijke virussen':[30]

> "In het algemeen mag het gebruik van biometrie voor de gewone beveiliging van goederen en personen niet worden beschouwd als een gerechtvaardigd belang dat prevaleert boven de belangen die samenhangen met de grondrechten en fundamentele vrijheden van betrokkenen. Integendeel, de verwerking van biometrische gegevens is slechts gerechtvaardigd als een noodzakelijk middel ter beveiliging van eigendommen en/of personen, als aan de hand van objectieve en gedocumenteerde omstandigheden kan worden aangetoond dat een aanzienlijk risico concreet aanwezig is. (…) Om aan het evenredigheidsbeginsel te voldoen, moet een voor de verwerking verantwoordelijke die met deze hoogrisicosituaties wordt geconfronteerd, nagaan of met alternatieve maatregelen het doel even goed maar met minder privacyschending kan worden bereikt, en zo ja, voor die alternatieve maatregelen kiezen."[31]

4.23 Of er in de context van het betaald voetbal kan worden gesproken van een situatie waarin gebruik kan worden gemaakt van biometrische authenticatie, is in belangrijke mate afhankelijk van het belang dat wordt toegekend aan de effectieve handhaving van stadionverboden, en/of het aanpakken van andere problemen bij voetbalwedstrijden, zoals discriminerende spreekkoren. In zoverre is dat dan aan de politiek. Met die kanttekening betekent dat voor de voorgenomen biometrische toegangspoortjes door BVO's dat er gebruik kan worden gemaakt van de uitzondering van artikel 29 UAVG, voor zover het voetbalstadion aan de hand van objectieve en gedocumenteerde omstandigheden kan aantonen dat zich aanmerkelijke en concrete beveiligingsrisico's voordoen, die met andersoortige alternatieve toegangssystemen (lees handmatige controle of IBA) niet goed kunnen worden weggenomen. Dit vereist dat het voetbalstadion bijvoorbeeld documenteert op welke wijze het gebruik van minder privacygevoelige toegangspoortjes tekortschiet, en wat daarvan de nadelige gevolgen zijn of kunnen zijn. Een logische plek waarin deze onderbouwing kan worden opgenomen is de 'Data Protection Impact Assessment' of 'DPIA' in de zin van artikel 35, eerste lid, AVG die in ieder geval moet worden verricht.[32]

4.24 Er is dus een nadere analyse en motivering nodig per BVO waarom in diens concrete geval een aantoonbare noodzaak bestaat om biometrie in te zetten in plaats van 'normale' toegangscontroles of IBA. Daarbij gelden de volgende aanbevelingen:

- Stel een gedetailleerd overzicht op van het aantal incidenten die recentelijk hebben plaatsgevonden binnen het stadion en die aanleiding hebben gevormd voor het opleggen van de stadionverboden. Ga daarbij in op de ernst van de incidenten.

- Motiveer welke gevaren dergelijke incidenten opleveren voor andere bezoekers en werknemers van het stadion. Haal daarbij zoveel mogelijk praktijkvoorbeelden aan die zich hebben voorgedaan binnen het stadion.

- Toon met concrete feiten en omstandigheden aan dat handmatige controles en de inzet van IBA onvoldoende borgen dat personen met een stadionverbod worden geweerd. Geef daarbij een overzicht van de situaties waarin is vastgesteld dat personen met stadionverboden de handmatige controles of IBA hebben weten te omzeilen. Beschrijf ook wat de vermoedelijke redenen zijn waarom handmatige controles en IBA geen

---

30 WP29, Advies 3/2012 over ontwikkelingen op het gebied van biometrische technologieën, (WP193), 27 april 2012, p. 14.

31 WP29, Advies 3/2012 over ontwikkelingen op het gebied van biometrische technologieën, (WP193), 27 april 2012, p. 14-15.

32 De inzet van biometrie is namelijk een zogenoemde 'hoog-risico' verwerking ten aanzien waarvan op grond van artikel 35, eerste lid, AVG een DPIA moet worden verricht.

soelaas bieden en waarom biometrie deze risico's naar verwachting wegneemt. Een aspect dat in de interviews naar voren komt is bijvoorbeeld dat stewards, gezien de drukte en het aantal personen, niet goed in staat zijn om personen met stadionverboden te identificeren. Voor zover stewards daar wel in slagen, blijkt het geregeld voor te komen dat stewards fysiek en verbaal onder druk worden gezet om een persoon met een stadionverbod toegang te verlenen. Indien aan de hand van cijfers kan worden aangetoond dat dergelijke situaties zich voordoen in de praktijk, vormt dit een nadere onderbouwing voor de noodzaak voor de inzet van biometrische toegangspoortjes.

- Licht toe waarom niet kan worden volstaan met een hybride mix van 'normale toegangspoortjes' (eventueel gekoppeld aan IBA) en biometrische toegangspoortjes voor zover uitdrukkelijke toestemming is gekregen. Daarbij zou bijvoorbeeld gewezen kunnen worden op het eerder beschreven 'waterbedeffect'.

  Een aanbeveling is tot slot om in de motivering te verwijzen naar relevante beslissingen van andere toezichthouders waarin reeds een zwaarwegend algemeen belang is aangenomen om biometrische toegangspoortjes in te zetten ter handhaving van stadionverboden. Wij wijzen bijvoorbeeld op het oordeel van de Deense privacy toezichthouder. Op 13 juni 2019 kondigde de Deense BVO Brøndby IF aan dat ze vanaf juli 2019 automatische gezichtsherkenningstechnologie wenste te implementeren in het Brøndby Stadion. De BVO wilde deze technologen gebruiken om personen te identificeren die een stadionverbod hebben gekregen voor voetbalwedstrijden van Brøndby IF, vanwege overtredingen van de gedragsregels van de club. Het AFR-systeem maakt gebruik van camera's die het openbare gebied voor de ingangen van het stadion scannen, waardoor personen op de verbodslijst kunnen worden gedetecteerd voordat ze de ingang bereiken. Op basis van de Deense nationale wetgeving is het mogelijk voor de Deense toezichthouder om voorafgaande toestemming te geven voor de verwerking van bijziendere persoonsgegevens, mits dat noodzakelijk is voor een zwaarwegend algemeen belang. De Deense toezichthouder heeft haar toestemming voor de inzet van biometrie ingezet. Biometrie mocht naar oordeel van de Deense toezichthouder ook worden ingezet in geval van uitwedstrijden van Brøndby IF. De Deense gegevensbeschermingsautoriteit heeft hiermee besloten dat deze verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang en dat de verwerking evenredig is met het nagestreefde doel.[33] Hoewel in de Nederlandse wetgeving geen mogelijkheid voor de AP bestaat om de verwerking van bijzondere persoonsgegevens toe te staan, biedt het Deense voorbeeld wel een aanknopingspunt voor het oordeel dat het voorkomen van incidenten binnen het stadion een zwaarwegend algemeen belang in de zin van de AVG zou kunnen zijn.

4.25 Onze eerste indruk is dat er een juridisch risico blijft bestaan dat de AP de noodzaak van de inzet van biometrische toegangspoortjes niet zal aannemen. Praktijk leert dat de AP de uitzondering van artikel 29 UAVG zeer strikt uitlegt. Ook andere toezichthouder hanteren deze strikte uitleg. Zo heeft de Franse privacytoezichthouder Commission nationale de l'informatique et des libertés ('CNIL') recent een sportclub gewaarschuwd over het gebruik van gezichtsherkenningstechnologie in een stadion.[34] Die technologie zou worden ingezet ten behoeve van de handhaving van stadionverboden, onderzoek naar voorwerpen en de strijd tegen terrorisme. Volgens CNIL is de inzet van gezichtsherkenningstechnologie in beginsel verboden en zijn in het betreffende geval andere middelen voorhanden om genoemde doelen te bereiken.

---

33 https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/

34 Zie https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-unavertissement-un-club.

4.26 Tegelijkertijd heeft de AP zich nog niet expliciet uitgelaten over de mogelijkheid om met een beroep op artikel 29 UAVG biometrische toegangspoortjes in te zetten ter handhaving van stadionverboden. Evenmin is deze specifieke vraag aan bod gekomen in de rechtspraak. Dit biedt aldus juridische ruimte voor BVO's om, na het opstellen van de hiervoor beschreven motivering en het voltooien van de DPIA, de inzet van biometrische toegangspoortjes toe te passen. Zonder juridisch risico is dat als gezegd niet.

Casus 1: Digitale preregistratie (IBA)

Toegangscontrole voetbalstadion & handhaving stadionverbod

In geval van de inzet van IBA worden er geen bijzondere persoonsgegevens verwerkt. Dit betreft een juridisch voordeel ten opzichte van oplossingen waarbij biometrie wordt ingezet, aangezien het voetbalstadion enkel een grondslag nodig heeft in de zin van artikel 6, eerste lid, AVG (zie hoofdstuk hierna).

Casus 2: Preregistratie met biometrische identificatie

Toegangscontrole voetbalstadion

In het geval van toepassing van casus 2 worden biometrische persoonsgegevens verwerkt. Er wordt namelijk een selfie gemaakt van de bezoeker op grond waarvan de face vector wordt gemaakt. Wij achten het verdedigbaar dat BVO's aan bezoekers uitdrukkelijke toestemming vragen voor deze manier van identificeren. Deze toestemming wordt ook uitdrukkelijk gevraagd voordat het resultaat van de face vector wordt gedeeld met de BVO's (dus de telefoon verlaat).

Er dient dan wel te worden voldaan aan de strikte randvoorwaarden van rechtsgeldige toestemming. Van rechtsgeldige, uitdrukkelijke toestemming in de zin van artikel 9, tweede lid, aanhef en onder a, AVG is sprake indien de toestemming van de bezoeker (a) vrijelijk, (b) specifiek, (c) geïnformeerd en (d) op een ondubbelzinnige wijze is verkregen. Ook dient een toestemmingsregister bij te worden gehouden en dient de toestemming gemakkelijk te kunnen worden ingetrokken.

Om daadwerkelijk te kunnen spreken van 'vrijelijke toestemming' is een randvoorwaarde dat bezoekers de keuze behouden om zichzelf ook te laten identificeren zonder het maken van een selfie. Dat is in deze casus het geval omdat bezoekers ook zichzelf kunnen laten identificeren aan de balie van het voetbalstadion waardoor er geen bijzondere persoonsgegevens worden verwerkt.

Handhaving stadionverbod

Het vragen van uitdrukkelijke toestemming voor de inzet van biometrie lijkt ons enkel haalbaar voor reguliere toegangscontrole. Zie hieronder ten aanzien van casus 3 de juridische risico's.

Casus 3: Biometrische toegangspoortjes

Toegangscontrole voetbalstadion

Wij achten het verdedigbaar dat BVO's aan bezoekers uitdrukkelijke toestemming vragen voor de inzet van biometrische toegangspoortjes voor reguliere toegangscontrole. Er dient dan wel opnieuw te worden voldaan aan de strikte randvoorwaarden van rechtsgeldige toestemming. Van rechtsgeldige, uitdrukkelijke toestemming in de zin van artikel 9, tweede lid, aanhef en onder a, AVG is sprake indien de toestemming van de bezoeker (a) vrijelijk, (b) specifiek, (c) geïnformeerd en (d) op een ondubbelzinnige wijze is verkregen. Ook dient een toestemmingsregister bij

te worden gehouden en dient de toestemming gemakkelijk te kunnen worden ingetrokken.

Om daadwerkelijk te kunnen spreken van 'vrijelijke toestemming' is een randvoorwaarde dat bezoekers de keuze behouden om toegang te verkrijgen via een poortje waar geen bijzondere persoonsgegevens worden verwerkt (bijv. handmatige controle of Identity Based Access). Voor zover er aldus gekozen wordt voor biometrische toegang gebaseerd op uitdrukkelijke toestemming, kan er enkel sprake zijn van een hybride mix van zowel biometrische poortjes en toegangspoortjes met handmatige controle of Identity Based Access.

Ook hier maakt het feit dat in geval van een biometrisch toegangspoortje sneller toegang kan worden verkregen tot het stadion dan andere toegangspoortjes, niet dat van een vrije keuze geen sprake meer is.

Handhaving stadionverbod

Het vragen van uitdrukkelijke toestemming voor de inzet van biometrie lijkt ons enkel haalbaar voor reguliere toegangscontrole. Wij zien juridische risico's bij het vragen van toestemming voor het gebruik van biometrie ter handhaving van stadionverboden. Een juridisch risico is dat in geval van de handhaving van stadionverboden een zekere machtsverhouding (en daarmee een wanverhouding) bestaat tussen het voetbalstadion en de bezoeker. In deze situatie zal vrijelijke toestemming niet snel kunnen worden aangenomen. De bezoeker met het stadionverbod zal zich althans gedwongen kunnen voelen om toestemming te geven. Een ander praktisch risico is dat het niet te verwachten valt dat bezoekers met een stadionverbod toestemming zullen geven voor het gebruik van hun biometrische gegevens. De inzet van biometrische toegangspoortjes gebaseerd op uitdrukkelijke toestemming ter handhaving van stadionverboden, zal dus niet het gewenste effect sorteren. De verwachting is eerder dat een zeker waterbed-effect ontstaat waarbij bezoekers met een stadionverbod kiezen voor de alternatieve toegangspoortjes zonder biometrie.

Het stadionbreed inzetten van biometrische toegangspoortjes is wat ons betreft enkel mogelijk voor zover het stadion een beroep toekomt op artikel 29 UAVG (authenticatie en beveiligingsdoeleinden). De slagingskans van een beroep op deze wettelijke uitzondering hangt af van de verantwoording van de precieze noodzaak van de inzet van biometrie door de BVO in plaats van IBA. Onze eerste indruk is dat er een juridisch risico bestaat dat de AP de noodzaak van de inzet van biometrische toegangspoortjes niet zal aannemen. De AP hanteert een zeer strikte uitleg van artikel 29 UAVG. Wij hebben diverse processtrategieën beschreven om op voorhand meer juridische zekerheid te verkrijgen.

Een andere optie is uiteraard dat er een expliciete wettelijke grondslag wordt gecreëerd die regelt dat BVO's biometrische gegevens mogen verwerken ter handhaving van een voetbalstadion verbod. In dat geval kan de verwerking worden gebaseerd op artikel 9, eerste lid, aanhef en onder g, AVG.

5 In hoeverre bestaat er een wettelijke grondslag in de zin van artikel 6 AVG?

5.1 De vraag rijst of en zo ja, in hoeverre BVO's beschikken over een wettelijke grondslag in de zin van artikel 6 AVG om bij de toegangscontrole gebruik te maken van IBA resp. biometrie (gezichtsherkenning, vingerafdruk, handpalm). Daarbij zullen we tevens ingaan op de vraag of het uitmaakt of de technologie wordt ingezet voor reguliere toegangscontrole of het controleren van een voetbalstadionverbod[35].

[35] Hierbij zal rekening worden gehouden met het soort stadionverbod, te weten een civielrechtelijke stadionverbod en een strafrechtelijk stadion verbod.

5.2 Voor zover het gaat over de verwerking van persoonsgegevens bepaalt artikel 6, eerste lid, van de AVG dat een verwerking van 'gewone' persoonsgegevens is toegestaan voor zover daarvoor een zogenoemde 'wettelijke grondslag' bestaat.[36] Ten aanzien van preregistratie kunnen BVO's zich beroepen op de volgende drie wettelijke grondslagen:

> a) de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
>
> b) de verwerking is **noodzakelijk voor de uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
>
> f) de verwerking is noodzakelijk voor de behartiging van **de gerechtvaardigde belangen van de verwerkingsverantwoordelijke** of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

5.3 Wij lichten deze grondslagen kort toe, waarna wij vervolgens per techniek en toepassing aanbevelingen zullen doen voor de keuze voor één van deze wettelijke grondslagen.

Toestemming (artikel 6, eerste lid, aanhef en onder a, AVG).

5.4 In de praktijk zien wij dat BVO's zich geregeld baseren op de wettelijke grondslag 'toestemming'. Voor de randvoorwaarden voor het verkrijgen van rechtsgeldige toestemming verwijzen wij naar randnrs. 4.1 e.v. van dit rapport. De BVO moet verder kunnen aantonen dat zij de bovenstaande toestemming heeft verkregen. Tot geldt dat de toestemming op ieder moment door de bezoeker moet kunnen worden ingetrokken.

Noodzakelijk voor de uitvoering van de overeenkomst (artikel 6, eerste lid, aanhef en onder b, AVG)

5.5 Een andere reële grondslag is die van artikel 6, eerste lid, aanhef en onder b, AVG. Dit artikel bepaalt dat persoonsgegevens enkel verwerkt mogen worden indien de verwerking noodzakelijk is voor de uitvoering van een overeenkomst of het treffen van precontractuele maatregelen. Een beroep op deze wettelijke grondslag is alleen mogelijk indien de bezoeker van wie de persoonsgegevens worden verwerkt partij is bij de overeenkomst of als de betrokkene heeft verzocht om het treffen van precontractuele maatregelen.[37]

5.6 De European Data Protection Board ('EDBP') stelt zich op het standpunt dat een beroep op de wettelijk grondslag 'uitvoering overeenkomst' alleen mogelijk is als daadwerkelijk sprake is van een overeenkomst, deze overeenkomst geldig is op basis van toepasselijk nationaal recht en de verwerking van persoonsgegevens naar objectieve maatstaven noodzakelijk is voor de uitvoering van de overeenkomst.[38]

5.7 De overeenkomst in dit concrete geval is de aankoop van het toegangsbewijs door de toeschouwers en de registratie daarvan in de app. Daarmee committeert de toeschouwer zich (automatisch) aan de huisregels van de BVO en de algemene

---

[36] Voor alle algemene wettelijke grondslagen van artikel 6 AVG wordt verwezen naar het rapport: *De inzet van slimme technologie in* voetbalstadions

[37] Zie Kamerstukken II 1997-1998, 25 892, nr. 3, p. 80 en 81.

[38] Zie EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 8 October 2019, punt 26; zie ook Rechtbank Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407, nr.s 12.13-12.16.

voorwaarden die door de KNVB zijn geformuleerd[39] en het verbod om zich onrechtmatig in het stadion te gedragen (artikel 8.5 van de Algemene Voorwaarden).

Gerechtvaardigd belang (artikel 6, eerste lid, aanhef en onder f, AVG)

5.8 De derde grondslag is die van het gerechtvaardigd belang zoals bedoeld in artikel 6, eerste lid onder f AVG. Op grond van deze bepaling is de verwerking van persoonsgegevens toegestaan indien dit noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De BVO's kunnen zich op deze wettelijke grondslag beroepen voor zover wordt voldaan aan de volgende criteria:

- Allereerst moet sprake zijn van een echt, concreet, rechtstreeks 'gerechtvaardigd belang' van de BVO of een derde. De AP ziet onder meer het borgen van een veilig leven in een dreigende situatie, het tegengaan van inbreuken op persoonlijkheidsrechten, het tegengaan van onrechtmatig gedrag en het nakomen van zorgplichten ten aanzien van klanten als gerechtvaardigde belangen.
- De verwerking moet strikt noodzakelijk zijn om het gerechtvaardigde belang te behartigen.
- Tot slot dient een afweging plaats te vinden tussen de belangen van de BVO's (en/of diens partners) enerzijds en de belangen van de bezoekers anderzijds. De gerechtvaardigde belangen dienen zwaarder te wegen dan de belangen van de bezoekers. De volgende factoren zijn bij deze afweging relevant:[40]
  - de gevolgen voor de betrokkene;
  - de (aanvullende) waarborgen die de verwerkingsverantwoordelijke of derde heeft getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of beperken;
  - de ernst van de inmenging op het grondrecht van de betrokkene;
  - of de betrokkene de verwerking min of meer kan verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor diegene toestemming heeft gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

Het antwoord op de vraag welke wettelijke grondslag het beste kan worden ingeroepen, is afhankelijk van de gekozen technologie en de concrete toepassing daarvan.

Casus 1: Digitale preregistratie (IBA)

Toegangscontrole voetbalstadion

Voor zover casus 1 (preregistratie zonder biometrische identificatie) wordt ingezet ten behoeve van de reguliere controle, verdient het aanbeveling om de verwerking te baseren op artikel 6, eerste lid, aanhef en onder b, AVG (overeenkomst). Wij achten de controle van het ticket en de toegewezen plaats een noodzakelijk onderdeel van de uitvoering van de overeenkomst door de BVO. Deze grondslag biedt een bestendigere basis dan toestemming, aangezien toestemming vrijelijk kan worden ingetrokken. Het vragen van toestemming is bovendien juridisch risicovol, nu het de vraag is of de toestemming wel vrijelijk kan worden geweigerd. Uit de interviews is gebleken dat Preregistratie in beginsel ten opzichte van een ieder wordt opgelegd. Om tot het stadion toegang te krijgen is toestemming vereist. Er kan derhalve worden gezegd dat het weigeren van de toestemming een nadelig gevolg heeft voor de toeschouwer – hij komt het stadion niet in.

[39] https://www.knvb.nl/downloads/bestand/2785/knvb-standaardvoorwaarden-per-1-september-2014
[40] WP29, Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, vastgesteld op 9 april 2014, par. III.3.4.

Handhaving stadionverbod

Naar wij begrijpen, zou een eventueel stadionverbod kunnen worden gehandhaafd door de autorisatie van het gebruik van de preregistratie in te trekken, waardoor de betreffende persoon geen kaarten meer kan kopen resp. geen toegang meer kan krijgen. Voor zover de preregistratie wordt ingezet voor het handhaven van het stadionverbod, lijkt artikel 6, eerste lid, aanhef en onder f, AVG (gerechtvaardigd belang) de meeste reële wettelijke grondslag te zijn. Wij achten het in algemene zin goed verdedigbaar dat het intrekken van de autorisatie kan worden gebaseerd op het gerechtvaardigde belang van de BVO om onrechtmatig gedrag – waaronder geweld, discriminatie of gevaarzetting – tegen te gaan. Daarbij wegen wij mee dat de AP in haar normuitleg heeft onderkend dat vergelijkbare belangen – het borgen van een veilig leven in een dreigende situatie, het tegengaan van inbreuken op persoonlijkheidsrechten, het tegengaan van onrechtmatig gedrag en het nakomen van zorgplichten – als gerechtvaardigde belangen als bedoeld in artikel 6, eerste lid, aanhef en onder f, AVG kunnen kwalificeren. Voor zover de BVO zich beroept op deze grondslag, is het van belang dat de bestaande gerechtvaardigde belangen worden gemotiveerd in een verantwoordingsdocument.

Het vragen van toestemming achten wij een onbetrouwbare grondslag voor de handhaving van het stadionverbod. Dit heeft immers het onwenselijke gevolg dat de toeschouwer zijn toestemming intrekt, waardoor de verwerkingsgrondslag vervalt.

Artikel 6, eerste lid, aanhef en onder b, AVG (overeenkomst) zou in potentie een grondslag kunnen bieden, maar wij achten dat wel een juridisch risico. Het is discutabel of het effectueren van een stadionverbod daadwerkelijk een uitvloeisel is van de overeenkomst die met de toeschouwer is gesloten.

Casus 2: Preregistratie met biometrische identificatie

Toegangscontrole voetbalstadion

Voor zover preregistratie met biometrische identificatie wordt ingezet, verdient het aanbeveling om de verwerking te baseren op artikel 6, eerste lid, aanhef en onder b, AVG (overeenkomst). Zodra de bezoeker echter een selfie maakt en vervolgens een biometrische analyse plaatsvindt (bijvoorbeeld bij het maken van een face vector), is sprake van de verwerking van een bijzonder persoonsgegeven. Er dient aanvullend toestemming te worden gevraagd zoals bedoeld in artikel 9, eerste lid, aanhef en onder a, AVG en artikel 6, eerste lid, aanhef en onder a, AVG. Zoals hierboven reeds aangestipt, is het vragen van toestemming juridisch risicovol. Het is namelijk de vraag of de toestemming wel vrijelijk kan worden geweigerd. Wij achten dit verdedigbaar indien de bezoekers altijd de mogelijkheid blijven houden om zichzelf aan de balie van het voetbalstadion te identificeren.

Handhaving stadionverbod

Ten aanzien van de handhaving van stadionverboden geldt hetzelfde regime als besproken onder casus 1 ‘handhaving stadionverbod’.

Casus 3: Toegang door middel van Biometrische toegangspoortjes

Toegangscontrole voetbalstadion & handhaving stadionverbod

In tegenstelling tot preregistratie ligt het in de rede dat de verwerking van persoonsgegevens die plaatsvindt bij de inzet van biometrische toegangspoortjes wordt gebaseerd op toestemming (artikel 6, eerste lid, aanhef en onder a, AVG). Vooralsnog is de verwerking van de biometrische gegevens immers gebaseerd op

uitdrukkelijke toestemming. Van belang is dat daarbij wordt voldaan aan de randvoorwaarden van toestemming in de zin van artikel 6, eerste lid, aanhef en onder a, AVG.

Voor zover de verwerking van biometrie niet op uitdrukkelijke toestemming, maar op artikel 29 UAVG wordt gebaseerd (zie hoofdstuk 5 hiervoor), ligt het in de rede om de verwerking te baseren op artikel 6, eerste lid, aanhef en onder f, AVG. Zie voor een nadere motivering casus 1 (IBA, handhaving stadionverbod) hiervoor. Van belang is dat goed gedocumenteerd wordt wat het gerechtvaardigde belang is om te kiezen voor biometrie in plaats van IBA of handmatige toegangscontrole.

Burgerservicenummer (BSN)

5.9 Het komt geregeld voor dat bij digitale preregistratie gegevens worden uitgelezen van het paspoort, ID- of rijbewijs van de gebruiker of bezoeker. Dikwijls vindt dat plaats door het maken van een foto van het paspoort, ID-bewijs of rijbewijs, dan wel door het uitlezen van de 'Near Field Communication-chip' ('NFC chip') van het betreffende document. BVO's dienen altijd goed te controleren of bij het maken van een foto of het uitlezen van de NFC-chip (onbedoeld) leidt tot de verwerking van het BSN. Het BSN mag enkel door de BVO resp. de appbeheerder worden verwerkt voor zover daarvoor een specifieke wettelijke grondslag bestaat in de zin van artikel 87 AVG jo. artikel 46 UAVG.

5.10 Artikel 46 van de UAVG regelt dat het BSN alleen gebruikt mag worden ter uitvoering van die wet, dan wel voor doelen bij de wet bepaald. Dit is een kapstokbepaling, op basis waarvan in andere wetten invulling kan worden gegeven aan het verwerken van het BSN.[41]

> Zie artikel 46 UAVG
>
> 1.Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald.
>
> 2. Bij algemene maatregel van bestuur kunnen andere dan in het eerste lid bedoelde gevallen worden aangewezen waarin een daarbij aan te wijzen nummer als bedoeld in het eerste lid, kan worden gebruikt. Daarbij kunnen nadere regels worden gegeven over het gebruik van een zodanig nummer.

5.11 Uit de toelichting bij artikel 46 UAVG volgt dat het BSN alleen voor andere doeleinden kan worden verwerkt indien 1) het doel verenigbaar is met de doeleinden waarvoor het BSN is verkregen en 2) voor zover de verwerking van BSN voor andere doeleinden dan de uitvoering van de betreffende wet bij de wet is bepaald.[42]

5.12 Voor BVO's is tot op heden geen formele wettelijke basis gecreëerd voor het verwerken van het BSN. Dit maakt dat BVO's géén gebruik mogen maken van het BSN. Meer concreet houdt dit in dat BVO's die willen experimenteren met preregistratie, biometrische identificatie of biometrische toegangspoortjes maatregelen moeten treffen die voorkomen dat het BSN wordt verwerkt. Een maatregel die wij in de praktijk vaak zien, is dat het BSN weliswaar kortstondig wordt uitgelezen, maar direct wordt geanonimiseerd. Een andere maatregel die in de praktijk voorkomt is dat

---

41 Met deze bepaling heeft de Nederlandse wetgever uitvoering gegeven aan artikel 87 AVG, dat bepaalt: "De lidstaten kunnen de specifieke voorwaarden voor de verwerking van een nationaal identificatienummer of enige andere identificator van algemene aard nader vaststellen. In dat geval wordt het nationale identificatienummer of enige andere identificator van algemene aard alleen gebruikt met passende waarborgen voor de rechten en vrijheden van de betrokkene uit hoofde van deze verordening."

42 Zie Kamerstukken II, vergaderjaar 2017–2018, 34 851, nr. 3, p. 52.

het BSN (kortstondig) wordt verwerkt binnen de app van de gebruiker en vervolgens wordt verwijderd, zonder dat het BSN in het verdere proces toegankelijk is of wordt gedeeld met de app-beheerder of de BVO. Hoewel dergelijke maatregelen de risico's van de verwerking van het BSN mitigeren, voorkomen dergelijke maatregelen vaak niet dat het BSN kortstondig wordt verwerkt. De BVO loopt aldus het risico dat de beperkte verwerking van het BSN kwalificeert als een overtreding van artikel 46 UAVG. In dat licht doet de BVO er verstandig aan om te bezien of er maatregelen getroffen kunnen worden die maken dat het BSN in zijn geheel niet in de app wordt verwerkt, bijvoorbeeld door het BSN in de foto van het ID-bewijs te laten lakken door de bezoeker vóórdat deze in de app wordt geüpload. Een andere maatregel is dat technisch wordt geborgd dat het informatieveld met daarin het BSN niet wordt uitgelezen.

5.13 Wij benadrukken dat de hiervoor beschreven problematiek zich met name voordoet ten aanzien van identiteitsbewijzen die zijn uitgegeven vóór 30 augustus 2021. In geval van identiteitsbewijzen die zijn uitgegeven vóór 30 augustus 2021 staat het BSN namelijk opgenomen op de voorkant van het identiteitsbewijs. Bij identiteitsbewijzen uitgegeven vóór 30 augustus 2021 is het BSN bovendien opgenomen in de NFC-chip van het identiteitsbewijs. Zonder het treffen van nadere maatregelen, leidt het maken van een foto of het uitlezen van de NFC-chip aldus automatisch tot het verwerken van het BSN. Voor identiteitsbewijzen die zijn uitgegeven na 30 augustus 2021 ligt dat anders.[43] Ter voorkoming van het ongeautoriseerde gebruik van het BSN, is bij deze identiteitsbewijzen het BSN verplaatst naar de achterkant. Het BSN is bovendien verwijderd uit de NFC-chip. Het BSN kan voortaan enkel digitaal worden uitgelezen door gebruik te maken van de nieuw toegevoegde QR-code aan de achterkant van het identiteitsbewijs.[44] Het voorgaande maakt aldus dat de BVO resp. de app beheerder in geval van paspoorten uitgegeven na 30 augustus 2021 e.v. geen, althans minder maatregelen hoeven te treffen ter voorkoming van de verwerking van het BSN. Het maken van een foto van de voorkant van het paspoort of het uitlezen van de NFC-chip levert immers geen verwerking (meer) op van het BSN.

6 STRAFRECHTELIJKE PERSOONSGEGEVENS

6.1 In artikel 10 AVG zijn regels gesteld voor "persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen" ('strafrechtelijke persoonsgegevens'. Bij de handhaving van stadionverboden valt niet uit te sluiten dat strafrechtelijke persoonsgegevens worden verwerkt. Strafrechtelijke persoonsgegevens zijn gegevens die "zowel op veroordelingen als op min of meer gegronde verdenkingen" betrekking hebben. Er moet sprake zin van zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring – in de zin van artikel 350 Sv. – kunnen dragen.[45] Het gaat dus om gegevens die een zwaardere verdenking opleveren dan een redelijk vermoeden van schuld.[46]

6.2 Voor wat betreft het handhaven van stadionverboden en de verwerking van strafrechtelijke persoonsgegevens geldt dat een verschil bestaat tussen een civielrechtelijk stadionverbod en een strafrechtelijk stadionverbod. Binnen het betaald voetbal kan een civielrechtelijk stadionverbod door de KNVB worden opgelegd aan bezoekers die volgens een melding van een BVO of het Openbaar Ministerie in en/of buiten het Stadion in het kader van een Evenement:

---

43 Zie Stcrt. 2021, 46527.

44 Zie antwoord op Kamervragen aan de Staatssecretaris BZK 'Paspoortscanner op mobieltje vormt risico op identiteitsfraude' van 5 november 2019, *Kamerstukken II* 2019/20, nr. 629. Zie tevens Stcrt. 2021, 46527.

45 Gerechtshof Arnhem-Leeuwarden 28 april 2020, ECLI:NL:GHARL:2020:3374, rov. 5.26 e.v.; Rb. Rotterdam 6 januari 2020, ECLI:NL:RBROT:2020:211, rov. 4.6 en 4.8.; Rb. Midden-Nederland 21 december 2021, ECLI:NL:RBMNE:2021:1641, rov. 3.8: Hoge Raad 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4; HvJEU 24 september 2019, C- 136/17, ECLI:EU:C:2019:773 (GC e.a. CNIL)

46 Gerechtshof 28 april 2020, ECLI:NL:GHARL:2020:3374, rov. 5.26 e.v; Hoge Raad 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o 4.4

(a) in strijd met de Standaardvoorwaarden hebben gehandeld; en/of
(b) een strafbaar feit hebben begaan; en/of
(c) zich schuldig hebben gemaakt aan voetbalgerelateerd wangedrag; en/of
(d) zich zodanig hebben gedragen dat daardoor het aanzien en/of het belang van het voetbal wordt geschaad.

6.3 Zowel een BVO als het OM kunnen bij de KNVB melding doen van een toeschouwer die zich vermoedelijk schuldig heeft gemaakt aan het overtreden van de standaardvoorwaarden van de KNVB of die anderszins voetbal gerelateerd wangedrag heeft vertoond. Indien de melding voldoende aanknopingspunten bevat, gaat de KNVB in beginsel over tot oplegging van een landelijk stadionverbod.[47] Het voorgaande laat overigens de bevoegdheid van BVO's onverlet om ook een lokaal stadionverbod op te leggen.

6.4 Een door KNVB of een BVO opgelegd stadionverbod heeft een civielrechtelijk karakter.[48] Voor zover het gaat om een civielrechtelijk stadionverbod die is opgelegd naar aanleiding van een strafbaar feit, zal vaak sprake zijn van de verwerking van een (indirect) strafrechtelijk persoonsgegeven. De KNVB resp. de BVO verkrijgen voor het opleggen van stadionverboden gegevens van politie en justitie over aanhoudingen wegens voetbal gerelateerde strafbare feiten via het zogenoemde Ketenvoorziening Voetbal. Gemeenten, politie, BVO's en het OM gebruiken de Ketenvoorziening Voetbal mede om per wedstrijd veiligheidsrisico's in te schatten.

6.5 Voor zover het gaat om civielrechtelijk, landelijk of lokaal stadionverbod die is opgelegd wegens overtredingen, *zonder* dat er sprake is van een strafbaar feit, zal géén sprake zijn van de verwerking van strafrechtelijke persoonsgegevens.

6.6 Naast een civielrechtelijke stadionverbod, kan aan een bezoeker ook een strafrechtelijk stadionverbod worden opgelegd. Het OM kan op grond van artikel 509hh WvSv een strafrechtelijke gedragsaanwijzing opleggen aan een toeschouwer. Een strafrechtelijke gedragsaanwijzing is een voorlopige maatregel die aan een persoon wordt opgelegd om ervoor zorgen dat zijn ernstig hinderlijke of storende gedrag wordt beëindigd. De officier van justitie kan daarnaast vanuit zijn strafvorderlijke bevoegdheid op basis van de Wet maatregelen bestrijding voetbalvandalisme en ernstige overlast (hierna: 'MBVEO') een gedragsaanwijzing geven aan een verdachte in de vorm van een gebiedsverbod, een meldingsplicht, een contactverbod of een begeleidingsverplichting. Het gaat in deze gevallen om een strafrechtelijk stadionverbod.[49] Bij een dergelijk strafrechtelijk stadionverbod is er voor het voetbalstadion zonder meer sprake van de verwerking van strafrechtelijke persoonsgegevens.

6.7 Voor strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG geldt dat deze alleen mogen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan op grond van het Unierecht of nationaal recht, en passende waarborgen worden geboden voor de rechten en vrijheden van de betrokkene. De algemene uitzonderingsgronden zijn in het nationale recht in artikelen 32 en 33 UAVG neergelegd. Daarnaast kan sectorspecifieke wetgeving uitzonderingen bevatten.

6.8 Op grond van artikel 32, eerste lid, aanhef en onder a, UAVG kan de uitdrukkelijke toestemming een grondslag bieden voor het verwerken van strafrechtelijke persoonsgegevens. Zoals eerder toegelicht, achten wij deze uitzondering echter niet goed haalbaar.

6.9 Als een stadionverbod wordt opgelegd op grond van persoonsgegevens die zijn verkregen door de politie of het OM krachtens de Wet politiegegevens of de Wet

---

47 Ministerie van Veiligheid en Justitie (thans Ministerie van Justitie en Veiligheid), 'Kader voor beleid, voetbal en veiligheid', p. 51.
48 In welk kader en onder welke omstandigheden een dusdanig stadionverbod wordt opgelegd wordt uitgebreid beschreven in *De inzet van slimme technologie in voetbalstadions*
49 Ministerie van Veiligheid en Justitie (thans Ministerie van Justitie en Veiligheid), 'Kader voor beleid, voetbal en veiligheid'.

justitiële en strafvorderlijke gegevens en deze gegevens zijn verstrekt aan de KNVB, of BVO's, is het voor deze laatste partijen mogelijk om een beroep te doen op artikel 33, eerste lid, sub a, UAVG:

> "de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, dan wel door verwerkingsverantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens";

6.10 Indien er strafrechtelijke persoonsgegevens worden gedeeld in het hierboven beschreven samenwerkingsverband, kan mogelijk een beroep worden gedaan op artikel 33 eerste lid, sub b, UAVG:

> "de verwerking geschiedt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken, indien:
> 1°.de verwerking noodzakelijk is voor de uitvoering van de taak van deze verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken; en
> 2°.bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad";

6.11 In specifieke gevallen zou artikel 33, tweede lid, UAVG een potentiële wettelijke grondslag kunnen vormen voor de verwerking strafrechtelijke persoonsgegevens door de BVO ten eigen behoeve:

(a) ter beoordeling van een verzoek van betrokkene om een beslissing over hem te nemen of aan hem een prestatie te leveren; of
(b) ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn.

6.12 Het beroep op bovengenoemde gronden is mogelijk voor zover daadwerkelijk kan worden gesteld dat het stadion enkel *ten eigen behoeve* strafrechtelijke persoonsgegevens verwerkt. Er mag dus geen persoonsgegevens worden uitgewisseld aan derden. Met name artikel 32, tweede lid, aanhef en onder b, UAVG lijkt een bestendige grondslag te kunnen vormen, voor zover de delicten die ten grondslag liggen aan het stadionverbod tot schade van het stadion of diens medewerkers heeft geleid.

De andere mogelijke doorbrekingsgrond voor het verwerken van persoonsgegevens van strafrechtelijke aard ten aanzien van het handhaven van zowel civielrechtelijke als strafrechtelijke stadionverboden is het vragen van een vergunning van de AP (artikel 33 lid 4 sub c en lid 5 UAVG).

6.13 Voordat een BVO een aanvraag voor een vergunning kan doen bij de AP moet deze eerst een Data Protection Impact Assessment ('DPIA') uitvoeren. Daarnaast moet de BVO een protocol opstellen en in dit protocol omschrijven hoe de strafrechtelijke gegevens worden verwerkt en hoe deze voorgenomen gegevensverwerking voldoet aan de eisen uit de AVG.

Casus 1 Digitale pre-regisratie , Casus 2: Preregistratie met biometrie en Casus 3: Biometrische toegangspoortjes

Handhaving stadionverbod

De verwerking van strafrechtelijke persoonsgegevens doet zich enkel voor in geval van de handhaving van stadionverboden. Voor digitale preregistratie, preregistratie met biometrische identificatie resp. biometrische toegangspoortjes geldt dat niet valt uit te

sluiten dat strafrechtelijke persoonsgegevens worden verwerkt (in ieder geval waar het gaat om civiele stadionverboden die zijn opgelegd n.a.v. strafbare feiten resp. strafbare stadionverboden).

De verwerking van dergelijke strafrechtelijke persoonsgegevens kan wat ons betreft niet goed gebaseerd worden op uitdrukkelijke toestemming, nu er van vrijelijke toestemming niet echt sprake lijkt te zijn. Als de handhaving van het stadionverbod plaatsvindt op grond van strafrechtelijke persoonsgegevens die (bijvoorbeeld via de Ketenvoorziening Voetbal) zijn verkregen van de politie of het OM krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens, kan de verwerking plaatsvinden op grond van artikel 33, eerste lid, sub a, UAVG.

Wij achten het bovendien verdedigbaar dat de verwerking wordt gebaseerd op artikel 32, tweede lid, aanhef en onder b, UAVG, mits de verwerking enkel ten eigen behoeve plaatsvindt en gemotiveerd kan worden dat de specifieke persoon met een stadionverbod naar verwachting een strafbaar feit zal plegen gericht tegen het voetbalstadion of zijn medewerkers**.** Een alternatief is tot slot het aanvragen van een vergunning. Zie voor tips voor de motivering van de noodzaak als onderdeel van een dergelijke vergunningsaanvraag randnr. 4.26 van dit rapport.

7 Noodzakelijkheidsbeginsel c.q. dataminimalisatie

7.1 Het door middel van de inzet van digitale preregistratie (*IBA),* biometrische identificatie en/of biometrische toegangspoortjes verwerken van persoonsgegevens moet voldoen aan het noodzakelijkheidsbeginsel van artikel 5 lid 1 sub c AVG, ook wel aangeduid als 'het beginsel van dataminimalisatie'.

7.2 Het noodzakelijkheidsbeginsel heeft gevolgen voor de toegang tot, de omvang van en de aard van de persoonsgegevens die door middel van de door de preregistratie of biometrische toegangspoortjes mogen worden verwerkt door de BVO's. De persoonsgegevens dienen toereikend en ter zake dienend te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Kort en goed houdt dit in dat de BVO en diens partners enkel 'need tot know'-informatie mag verwerken, in plaats van 'nice to know'-informatie. Uit het noodzakelijkheidsbeginsel volgt voorts dat de privacyinbreuk die met de inzet van de preregistratie of biometrische toegangspoortjes gepaard gaat in evenredige verhouding moet staan tot het doel waarvoor deze technologie wordt ingezet, te weten het verlenen van toegang tot het stadion en het handhaven van stadionverboden.

7.3 Daarnaast mogen de BVO's slechts overgaan tot het verwerken van persoonsgegevens door middel van de preregistratie of biometrische toegangspoortjes indien het hiervoor beschreven doel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit'). Gezien de gevoelige aard van biometrische gegevens, voldoet een oplossing waarbij géén biometrische gegevens worden verwerkt sneller aan het beginsel van dataminimalisatie dan een biometrische oplossing. Daarmee is niet gezegd dat preregistratie met biometrische identificatie, dan wel een biometrische toegangspoort zonder meer is uitgesloten. Dergelijke biometrische oplossingen zijn reeds nu al mogelijk, mits de verwerking van biometrische gegevens plaatsvindt op grond van uitdrukkelijke toestemming van de bezoeker. Daarnaast moet de BVO in een Data Protection Impact Assessment ('DPIA') kunnen aantonen dat er een zwaarwegend algemeen belang en strikte noodzaak bestaat om biometrie toe te passen. Om tot een goede motivering van de concrete noodzaak van preregistratie met biometrische identificatie resp. biometrische toegangspoortjes te komen, zal de BVO steeds moeten kunnen toelichten dat minder ingrijpende middelen geen soelaas biedt. In zoverre noopt het beginsel van dataminimalisatie tot een bepaalde volgorde in de keuze voor een oplossing (eerst het minst ingrijpende en pas dan het meer ingrijpende middel). Wij komen in dat licht tot de volgende proportionaliteitsladder:

1

Digitale preregistratie

De noodzaak voor de inzet van digitale preregistratie (zonder de verwerking van biometrische gegevens) zal naar verwachting snel kunnen worden aangenomen. Doordat geen bijzondere persoonsgegevens worden verwerkt rust op de BVO geen verzwaarde motiveringsplicht.

2

Biometrische identificatie (toestemming)

Ook voor zover toestemming wordt verkregen van de bezoeker, dient gemotiveerd te worden wat de noodzaak is om bijzondere persoonsgegevens te verwerken. Waarom kan niet volstaan worden met digitale preregistratie (zonder biometrie)? Deze noodzaak zou er bijvoorbeeld in gelegen kunnen zijn dat bij digitale preregistratie vaak sprake is van identiteitsfraude, in het licht waarvan een noodzaak bestaat om de identiteit van de bezoeker biometrisch te valideren in de identificatiefase. Om tot een gedegen motivering te kunnen komen, zal de BVO data moeten verzamelen en incidenten moeten aandragen waaruit blijkt dat digitale preregistratie (zie vorige stap) onvoldoende soelaas biedt (zie randnr. 4.24 voor meer tips).

3

Biometrische identificatie (verplicht)

Het stadionbreed invoeren van preregistratie met biometrische identificatie leidt tot een omvangrijkere verwerking dan vrijwillige biometrische identificatie. Nu zal van iedere bezoeker biometrische gegevens worden verwerkt. Dit kan alleen voor zover de verwerking kan worden gebaseerd op artikel 29 UAVG. De BVO dient aan te tonen dat het gebruik van biometrische identificatie nodig is voor een zwaarwegend algemeen belang (in dit concrete geval het handhaven van stadionverboden, ter bevordering van de veiligheid in het stadion). De BVO zal ook de noodzaak van het gebruik van specifiek biometrie moeten kunnen motiveren. Indien de BVO borgt dat het biometrische gegeven technisch niet toegankelijk is voor de BVO of de beheerder, kan dat ertoe leiden dat sneller wordt voldaan aan het beginsel van dataminimalisatie. Om tot een gedegen motivering te kunnen komen, zal de BVO data moeten verzamelen en incidenten moeten aandragen waaruit blijkt dat vrijwillige biometrische identificatie (zie vorige stap) onvoldoende soelaas biedt (zie randnr. 4.24 voor meer tips).

4

Biometrische toegangspoortjes (toestemming)

Biometrische toegangspoortjes leiden naar hun aard tot een ingrijpendere verwerking dan preregistratie met enkel biometrische identificatie. Om de biometrische poortjes te kunnen gebruiken, zal er immers een authenticatie moeten plaatsvinden van de van de Face vector afgeleid code (hetgeen op zichzelf een gepseudonimiseerd biometrisch gegeven is). Om de stap naar biometrische toegangspoortjes te zetten, zal gemotiveerd moeten worden waarom niet volstaan kan worden met digitale preregistratie met of zonder biometrie. Doordat deze variant van biometrische toegangscontrole is gebaseerd op uitdrukkelijke toestemming, gelden er relatief lichtere motiveringsvereisten dan bij verplichte (stadionbrede) biometrische toegangscontrole. Dat neemt niet weg dat de BVO data zal moeten verzamelen en incidenten zal moeten aandragen waaruit blijkt dat (verplichte) biometrische identificatie onvoldoende soelaas biedt (zie randnr. 4.24 voor meer tips).

5

Biometrische toegangspoortjes (verplicht)

Het meest ingrijpende middel is het stadionbreed invoeren van biometrische toegangspoortjes. Dit kan alleen voor zover de verwerking kan worden gebaseerd op artikel 29 UAVG. De BVO dient aan te tonen dat het gebruik van biometrische toegangspoortjes nodig is voor een zwaarwegend algemeen belang (in dit concrete geval het handhaven van stadionverboden, ter bevordering van de veiligheid in het stadion). Om tot een gedegen motivering te kunnen komen, zal de BVO data moeten verzamelen en incidenten moeten aandragen waaruit blijkt dat de hiervoor beschreven oplossingen onvoldoende effect sorteren (zie randnr. 4.24 voor meer tips).

7.4 Het noodzakelijkheidsbeginsel zal ook technisch moeten worden geborgd, zodat kan worden voldaan aan de beginselen van privacy by design & default.[50]

Casus 1: Preregistratie zonder biometrische identificatie (IBA) , Casus 2: Preregistratie met biometrische identificatie en casus 3: Biometrische toegangspoortjes

Ongeacht de keuze voor preregistratie of biometrische toegangspoortjes, Op grond van privacy by design & default zullen de BVO's en andere betrokken partijen, waar mogelijk technisch moeten borgen dat het noodzakelijkheidsbeginsel door ontwerp standaardinstellingen gewaarborgd blijft. De BVO's dienen in iedere fase kritisch te bezien welke privacy waarborgende maatregelen genomen kunnen worden.

8 Overige aandachtspunten en maatregelen

Geautomatiseerde besluitvorming

8.1 Voor zover de inzet van IBA of biometrie geautomatiseerd leidt tot de weigering van de toegang tot het stadion, zal er naar verwachting sprake zijn van geautomatiseerde besluitvorming. Wij lichten dit toe.

8.2 Artikel 22 AVG geeft de betrokkene, behoudens uitzonderingen, het recht om niet te worden onderworpen aan een uitsluitend op een geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.[51] De betrokkene hoeft dit recht niet in te roepen. Het recht van de betrokkene komt daarom feitelijk neer op een verbod voor de verwerkingsverantwoordelijke. Op dat verbod bestaan wel uitzonderingen.

> De AVG definieert profilering als elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling om zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.[52]

8.3 Om te kunnen vaststellen of sprake is van *geautomatiseerde besluitvorming* als bedoeld in artikel 22 AVG dient te worden getoetst of sprake is van (i) een uitsluitend op geautomatiseerde verwerking gebaseerd besluit (ii) met rechtsgevolgen of dat de betrokkene anderszins in aanmerkelijke mate treft. Hieronder volgt een nadere uitwerking van deze begrippen.

<u>(i) Is sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit?</u>

8.4 Als er sprake is van menselijke tussenkomst voordat het besluit wordt genomen, is er geen sprake van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Een geautomatiseerd proces dat slechts een aanbeveling doet, die vervolgens door een medewerker in combinatie met andere informatie wordt afgewogen bij het nemen van een uiteindelijk besluit, vormt geen geautomatiseerd besluit.

> Zie Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, rov. 4.19;
>
> Zo oordeelde de Rechtbank Amsterdam dat sprake was van betekenisvolle menselijke tussenkomst door Uber bij het gebruik van software waarmee

[50] Zie meer over Privacy by design & default in het rapport in *De inzet van slimme technologie in voetbalstadions*
[51] Artikel 22, lid 1, AVG.
[52] Artikel 4, aanhef en onder 4, AVG.

potentiële frauduleuze activiteiten kunnen worden gesignaleerd:

"Bij een […] signaal volgt afhankelijk van de ernst of duur van de activiteiten een waarschuwing aan de chauffeur of een onderzoek door een werknemer van het Risk-team. […] Op grond van de protocollen moeten de werknemers de potentiële fraudesignalen en de feiten en omstandigheden analyseren om / het bestaan van fraude te bevestigen of uit te sluiten. Zij gebruiken daarbij ook feiten en omstandigheden die zij op basis van hun kennis en ervaring relevant achten. Als een werknemer op basis van het onderzoek vaststelt dat sprake is van een consequent patroon van fraude, kan worden besloten om het account van de chauffeur te deactiveren. Hiervoor is een unaniem besluit van twee werknemers van het Risk-team nodig."[53]

Recentelijk is Gerechtshof Arnhem evenwel teruggekomen op dit oordeel van de Rechtbank Amsterdam (zie Gerechtshof Amsterdam 4 april 2023, ECLI:NL:GHAMS:2023:793, r.o. 3.18 en 3.19). Het Hof oordeelde dat voorafgaand aan het besluit tot het deactiveren van accounts van Uber-chauffeurs naar aanleiding van fraudesignalen, er geen sprake was van betekenisvolle menselijke tussenkomst omdat de Uber-chauffeurs niet waren gehoord, de besluiten algemeen geformuleerd waren en de door onderzoekmedewerkers geschreven notities niet alle gegevens betrokken.[54]

Zie in gelijke zin: HvJ Conclusie AG Pikamäe 16 maart 2023, C-634/21 ECLI:EU:C:2023:220, r.o. 42 t/m 47.[55] In zijn conclusie stelt AG Pikamäe dat als een besluit in dusdanig sterke mate wordt bepaald door een score dat die score als het ware doordringt in het besluitvormingsproces, er sprake is van een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Hij geeft aan dat door de score het besluit in principe vooraf is bepaald en dat het feit dat menselijke tussenkomst nog mogelijk is hier in dat geval niet aan af doet omdat die menselijke tussenkomst dan niet betekenisvol zal zijn. De HvJ heeft dit oordeel van de AG grotendeels gevolgd. [56] Het HvJ oordeelt dat reeds sprake is van een geautomatiseerd besluit indien er weliswaar sprake is van menselijke tussenkomst, maar de geautomatiseerde verwerking een 'determining role' speelt in het uiteindelijke besluit. Van belang is dan vooral dat het HvJ kennelijk ook van oordeel is dat er ook sprake is van zo een geautomatiseerd besluit, als er enige menselijke tussenkomst is. Voldoende daarvoor is dat het besluit hoofdzakelijk afhangt van de geautomatiseerde analyse, niet dat het uitsluitend daarvan afhangt. Het Hof lijkt daarmee de reikwijdte van het begrip ruimer op te vatten dan daarvoor wel werd aangenomen.

8.5 De menselijk tussenkomst moet betekenis hebben. Het klakkeloos overnemen van de uitkomst van de geautomatiseerde verwerking geldt niet als betekenisvolle menselijke tussenkomst. De menselijke tussenkomst moet leiden tot zinvol toezicht op de besluitvorming en degene die de menselijke tussenkomst uitvoert, moet alle relevante gegevens bij de herbeoordeling betrekken en bevoegd en bekwaam zijn om een andersluidend besluit te nemen.[57]

<u>(ii) Leidt het geautomatiseerde besluit tot rechtsgevolgen of is sprake van een besluit dat een betrokkene anderszins in aanmerkelijke mate treft?</u>

8.6 Indien vastgesteld wordt dat inderdaad sprake is van een uitsluitend op geautomatiseerd verwerking gebaseerd besluit, dient vervolgens te worden gekeken

[53] Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, rov. 4.19
[54] Tegen deze uitspraak staat op het moment van schrijven nog een cassatietermijn open.
[55] Dit betreft het arrest van de AG waaraan nog geen rechtsgevolgen kunnen worden verbonden. De conclusie van het HvJ zelf dient aldus te worden afgewacht.
[56] HvJ EU 7 december 2023, *SCHUFA*, C-634/21, ECLI:EU:C:2023.957.
[57] Zie WP29, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 24.

naar de specifieke gevolgen van dat besluit. Het verbod van artikel 22 AVG is erop gericht om personen te beschermen tegen aanzienlijke effecten van geautomatiseerde besluitvorming. Het verbod geldt slechts indien sprake is van 'besluitvorming met rechtsgevolgen' voor de betrokkene of 'besluitvorming die de betrokkene anderszins in aanmerkelijke mate treft'.[58]

> Met het begrip besluit doelt de AVG niet alleen op juridische besluiten, het kan ook om feitelijke beslissingen gaan.

8.7 Met besluiten waaraan rechtsgevolgen zijn verbonden, wordt volgens de Artikel 29-Werkgroep (nu de EDPB) bedoeld een besluit dat van invloed is op iemands wettelijke rechten (zoals het stemrecht of het recht om rechtsmiddelen in te stellen). De Artikel 29-Werkgroep noemt als voorbeeld rechtsgevolgen die iemands juridische status beïnvloeden, waaronder bijvoorbeeld: (i) het recht op of weigering van een uitkering, zoals kinderbijslag of huurtoeslag of (ii) de weigering tot toelating tot een land of de toekenning van een nationaliteit.[59] Betrekkelijk vager is de categorie besluiten die de betrokkene 'in aanmerkelijke mate treft'. Het gaat hier om besluiten die weliswaar geen rechtsgevolg teweegbrengen, maar de betrokkene toch in vergelijkbare mate kan treffen. WP29 neemt daarbij als uitgangspunt dat "de effecten van de verwerking groot of belangrijk genoeg moeten zijn om aandacht te verdienen".[60]

> Het is moeilijk om in zijn algemeenheid te bepalen welk gevolg ernstig genoeg is om te kunnen spreken van een gevolg dat een betrokkene in aanmerkelijke mate treft. Een en ander zal moeten worden uitgekristalliseerd in de Europese en nationale rechtspraak. WP29 neemt als uitgangspunt dat sprake kan zijn van een besluit dat een betrokkene in aanmerkelijke mate treft indien het besluit het potentieel heeft om "[i] de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen; [ii] een langdurig of blijvend effect op de betrokkene te hebben; of [iii] in het uiterste geval, tot uitsluiting of discriminatie van personen te leiden".[61]

8.8 In de parlementaire geschiedenis van de (U)AVG en in de eerdergenoemde opinie van de Artikel 29-Werkgroep worden de volgende voorbeelden aangehaald:

- de automatische weigering van een (online) ingediende kredietaanvraag[62];
- verwerking van sollicitaties zonder menselijke tussenkomst[63];
- besluiten die iemands financiële situatie treffen, waaronder bijvoorbeeld het in aanmerking komen voor een lening[64];
- besluiten die iemands toegang tot gezondheidszorg treffen[65];
- besluiten waarmee iemand de toegang tot de arbeidsmarkt wordt geweigerd of waarmee hij ernstig wordt benadeeld;
- besluiten die iemands toegang tot onderwijs treffen, bijvoorbeeld de toelating tot een universiteit[66].

---

58 Achterliggende gedachte van het verbod is dat "niemand mag worden onderworpen aan de gevolgen van een besluit enkel en alleen op basis van kenmerken van een bepaalde groep waartoe hij of zij behoort. De ratio van deze bepaling is dat het in dit licht bijzonder kwetsbaar is om besluitvorming te baseren op enkele persoonskenmerken". Zie overweging 71 van de considerans van de AVG en *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 39.

59 Zie WP29, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 25.

60 WP29, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 25.

61 WP29, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 10-11.

62 Overweging 71 van de considerans van de AVG.

63 Overweging 71 van de considerans van de AVG.

64 Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 26.

65 Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 26.

66 Vgl. WP29, 'Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679', WP 251rev01, p. 10-11

8.9 Relevant in dat kader is de vraag of de (eventuele) geautomatiseerde selectie van gegevens reeds tot gevolg heeft dat de betrokkene rechtsgevolgen ondervindt of sprake is van gevolgen die de betrokkene in aanmerkelijke mate treffen. Verdedigbaar kan zijn dat pas in de uiteindelijke besluitvormingsfase, bij het opstellen van het daadwerkelijke besluit, de betrokkene rechtsgevolgen respectievelijk aanmerkelijke gevolgen ondervindt van de (geautomatiseerde) selectie van zijn persoonsgegevens. Immers pas dan wordt de beslissing, waarvan de betrokkene gevolgen ondervindt, genomen.[67]

Uitzonderingen

8.10 Het nemen van een geautomatiseerd besluit is op grond van artikel 22, lid 2, AVG alleen toegestaan als het besluit:

- noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
- is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene (zoals artikel 40 UAVG dat onder meer een uitzondering bevat voor geautomatiseerde besluitvorming *anders dan op basis van profilering*, die noodzakelijk is voor de vervulling van een taak van algemeen belang[68]); of berust op de uitdrukkelijke toestemming van de betrokkene.

Analyse casussen

8.11 Toegepast op IBA en biometrische toegangspoortjes ter handhaving van stadionverboden, is onze inschatting dat sprake zal zijn van geautomatiseerde besluitvorming voor zover er geen enkele menselijke tussenkomst plaatsvindt bij de digitale beoordeling of iemand een toegangsrecht heeft tot het stadion. Vanuit juridisch perspectief is dit problematisch, aangezien de BVO geen aanspraak lijkt te kunnen maken op één van de wettelijke uitzonderingen op het verbod van geautomatiseerde besluitvorming als beschreven in randnr. 8.10 van dit rapport. In feite zal geautomatiseerde besluitvorming enkel mogelijk zijn indien hiervoor een expliciete wettelijke grondslag voor wordt gecreëerd. In afwachting daarvan, zijn de BVO's aldus gedwongen om wezenlijke menselijke tussenkomst toe te passen. Dit kan plaatsvinden bij de controle aan de poort. Hierbij kan worden gedacht aan de situatie dat het poortje rood kleurt en vervolgens door middel van een videoverbinding direct een tweede menselijke hercontrole plaatsvindt door een steward van het stadion. In die situatie zou gesteld kunnen worden dat het rode scherm enkel een aanbeveling is voor de steward om kritisch te bezien of de betreffende persoon daadwerkelijk een stadionverbod opgelegd heeft gekregen. Om discussies aan de poort in zijn geheel te voorkomen, zou de menselijke tussenkomst naar onze optiek beter eerder in het proces plaats moeten vinden, bijvoorbeeld door handmatig het account of de identificatie van de betreffende bezoeker in te trekken, zodat hij geen toegangsrecht meer kan verkrijgen of überhaupt geen gebruik kan maken van het (biometrische) poortje. Een dergelijke handmatige intrekking van de autorisatie of het toegangsrecht betreft een handmatig besluit, met als gevolg dat een daarop volgend rood scherm bij een poging toegang naar zijn aard niet meer kwalificeert als een geautomatiseerd besluit.

---

67 Zie Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, rov. 4.17 e.v.

68 Artikel 40, lid 1, UAVG bepaalt: "Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang."

Verdere verwerking in geval van incidenten

8.12 In de praktijk rijst geregeld de vraag of BVO's in geval van een incident in het stadion de persoonsgegevens die oorspronkelijk zijn verzameld en worden verwerkt in het kader van de (digitale) preregistratie respectievelijk de biometrische toegangspoortjes, mogen worden geraadpleegd en gebruikt ten behoeve van het vinden of sanctioneren van de bezoeker die (vermoedelijk) betrokken is bij het incident.

8.13 Voor het antwoord op deze vraag dient een onderscheid te worden gemaakt tussen enerzijds toegangscontrole die is gebaseerd op het gerechtvaardigde belang van de BVO of artikel 29 UAVG, dan wel (uitdrukkelijke) toestemming:

- In geval van (digitale) preregistratie zonder biometrische identificatie met als doel reguliere toegangscontrole (gebaseerd op artikel 6, eerste lid, aanhef en onder b, AVG, 'uitvoering van de overeenkomst'), zal sprake zijn van de verdere verwerking van persoonsgegevens. De persoonsgegevens worden immers voor een ander doel verwerkt dan waarvoor zij oorspronkelijk zijn verzameld. Het ligt in dit concrete geval in de rede dat in de overeenkomst tot uitdrukking wordt gebracht dat de gegevens mede worden verwerkt ten behoeve van het oplossen van incidenten in het stadion.

- In geval van (digitale) preregistratie zonder biometrische identificatie met als doel reguliere toegangscontrole of de handhaving van een stadionverbod (gebaseerd op artikel 6, eerste lid, aanhef en onder f, AVG, 'gerechtvaardigd belang') zal eveneens sprake zijn van de verdere verwerking van persoonsgegevens. Een verdere verwerking mag ingevolge artikel 6, vierde lid, AVG slechts plaatsvinden voor zover de verwerking berust op (i) toestemming, (ii) een Europese of nationale wettelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een in artikel 23, eerste lid, AVG bedoelde doelstelling, óf (iii) het doeleinde van de verdere verwerking verenigbaar is met het oorspronkelijke doel van de verwerking van de gegevens in het licht van de verenigbaarheidscriteria van artikel 6, vierde lid, AVG. Of en zo ja, in hoeverre sprake is van een verenigbare verdere verwerking wordt getoetst aan de hand van de volgende criteria:

  - Het verband tussen de doeleinden waarvoor de gegevens zijn verzameld en de doeleinden van de verdere verwerking;
  - Het kader waarin de persoonsgegevens zijn verzameld en dan met name de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke (ook wel: de wijze van verkrijging en de verwachting van de betrokkene);
  - De aard van de gegevens;
  - De mogelijke gevolgen van de voorgenomen verdere verwerking voor betrokkenen; en
  - Het bestaan van passende waarborgen, zoals pseudonimisering.

  Wij achten het verdedigbaar dat de verdere verwerking wordt gezien als een 'verenigbare verdere verwerking', aangezien het borgen van de veiligheid binnen het stadion in het verlengde ligt van de doelstellingen die met de reguliere toegangscontrole of de handhaving van het stadionverbod worden nagestreefd.

- Voor zover het gaat om preregistratie (met biometrische identificatie) of biometrische toegangspoortjes gebaseerd op toestemming, zal separate uitdrukkelijke toestemming moeten worden gevraagd voor de verdere verwerking van de gegevens ten behoeve van het afhandelen van incidenten.

- Voor zover het gaat om preregistratie (met biometrische identificatie) of biometrische toegangspoortjes gebaseerd op artikel 29 UAVG ligt het in de

rede om het doeleinde ‘opsporen en afhandelen incidenten’ expliciet te benoemen als doelstelling van de verwerking. In de DPIA kan vervolgens ook gemotiveerd worden waarom de verwerking noodzakelijk is voor het afhandelen van incidenten. Van een verdere verwerking is in dat geval geen sprake (meer). Doordat de doelstelling van meet af aan is opgenomen in de DPIA en de privacy verklaring, vormt het gebruik van de persoonsgegevens ten behoeve van de afhandeling van incidenten een primaire verwerking. In zoverre hoeft niet meer getoetst te worden aan artikel 6, vierde lid, AVG.

8.14 Let op: het vergelijken van een foto van een identiteitsbewijs dat oorspronkelijk is verzameld in het kader van preregistratie of biometrische toegangscontrole met een camerabeeld van het incident, betreft een verdere verwerking, die kan leiden tot de verwerking van bijzondere persoonsgegevens. Voor zover de camerabeelden van een incident handmatig worden vergeleken met de foto van het identiteitsbewijs gaat het enkel om de verwerking van ‘gewone’ persoonsgegevens. Dit is anders wanneer de camerabeelden geautomatiseerd worden vergeleken met foto’s van identiteitsbewijzen. In dit geval is er sprake van een biometrische vergelijking. Daarvoor is een expliciete wettelijke grondslag vereist in de zin van artikel 9, tweede lid, AVG (zie hoofdstuk 5 van dit rapport).

Juistheid

8.15 Tref de nodige maatregelen die borgen dat IBA of de inzet van biometrie leidt tot de verwerking van juiste en nauwkeurige persoonsgegevens:

- Geef een indicatie van de mate van (on)zekerheid van de kwaliteit en juistheid van de vastgestelde identiteit.
- Licht bovendien toe wat de mate van (on)zekerheid bepaalt.
- De biometrische camera’s kunnen worden beschadigd (door slijtage of technisch falen), onklaar gemaakt of gestolen. Relevant is dus of er mogelijkheden zijn om op afstand vast te stellen of de camera nog optimaal werkt.
- Voer bovendien steekproefsgewijs een controle uit om te beoordelen of de door IBA gegenereerde identiteit en de face vector en biometrische controle nog voldoende nauwkeurig zijn.
- Hanteer passende procedures waarmee factoren die aanleiding geven tot onjuistheden van persoonsgegevens worden gecorrigeerd of verwijderd.

Beveiliging

8.16 Stel een beveiligingsplan vast dat concreet is toegespitst op de inzet van IBA resp. biometrische toegangspoortjes.

8.17 Toets periodiek de hierboven beschreven beveiligingsmaatregelen. Houd daarbij rekening met de stand van de techniek. Actualiseer voor zover nodig de beveiligingsmaatregelen.

8.18 Waarborg door middel van een autorisatiematrix en een controleproces dat degene die toegang verkrijgen tot de omgeving daadwerkelijk daartoe bevoegd is.

8.19 Stel een werkwijze vast om medewerkers toegang te geven tot gegevens en stel vast wie de bevoegdheid heeft om de toegang tot de data-omgeving te verwezenlijken. Zorg daarbij voor een werkwijze voor het verlies van technische of fysieke sleutels tot de beveiligde omgevingen.

8.20 Maak heldere afspraken over het verrichten van audits en het geven van uitvoering aan de resultaten van beveiligingsaudits.

8.21 Stel technische en organisatorische maatregelen vast (waaronder een noodplan) om eventuele schade te beperken in het geval een beveiligingsgebrek wordt geconstateerd of dat de drone neerstort.

8.22 Waarborg dat eventuele (sub)verwerkers eveneens passende beveiligingsmaatregelen treffen.

8.23 Het verdient opmerking dat er op dit moment ten aanzien van de verschillende casussen enkel sprake is van decentrale en ecrypted data. Dit zorgt al voor een hoger beveiligingsniveau dan wanneer hier geen sprake van zou zijn.

Transparantie

8.24 Zorg dat personen die het voetbalstadion betreden overeenkomstig artikelen 13 en 14 AVG geïnformeerd worden over de verwerking die bij de inzet van IBA of biometrie plaatsvindt. In het voetbalstadion zullen maatregelen getroffen moeten worden om de transparantie te verhogen. Er kan niet worden volstaan met het plaatsen van één bord op een centrale plek binnen het voetbalstadion, maar er moet in ieder geval per toegangspoortje aan de bezoeker kenbaar worden gemaakt dat zij een biometrisch toegangspoortje naderen.

8.25 Op grond van artikel 23 AVG kunnen de hierboven genoemde rechten van betrokkene (waaronder begrepen de informatieplicht) worden ingeperkt. Deze uitzonderingen zijn uitgewerkt in artikel 41, eerste lid, UAVG:

> 1. De verwerkingsverantwoordelijke kan de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34138 van de verordening, buiten toepassing laten voor zover zulks noodzakelijk en evenredig is ter waarborging van:
> a. de nationale veiligheid;
> b. landsverdediging;
> c. de openbare veiligheid;
> d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
> e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
> f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
> g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
> h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e, g;
> i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
> j. de inning van civielrechtelijke vorderingen.

8.26 De BVO's zullen zelf moeten afwegen of zich een of meer uitzonderingsgronden voordoen. Daarbij moeten zij op grond van artikel 41, tweede lid, UAVG in ieder geval, voor zover van toepassing, rekening houden met:

a. de doeleinden van de verwerking of van de categorieën van verwerking;
b. de categorieën van persoonsgegevens;
c. het toepassingsgebied van de ingevoerde beperkingen;
d. de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;

9 AFSLUITEND

9.1 Tot zover dit rapport. Voor een overzicht van onze bevindingen verwijs ik u naar de samenvatting aan het begin van dit rapport.

****