Gegevensbeschermingsautoriteit

Aanbeveling betreffende de verwerking van biometrische gegevens

EXECUTIVE SUMMARY

Biometrische gegevens zijn persoonsgegevens die afgeleid worden uit de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon en die toelaten om die persoon te identificeren of authentiseren. Burgers worden vandaag steeds vaker geconfronteerd worden met de verwerking van biometrische gegevens op hun smartphones of tablets maar ook door de overheid en door private ondernemingen. Overeenkomstig artikel 9.1 AVG zijn biometrische gegevens, en dit in tegenstelling tot de situatie vóór de inwerkingtreding van de AVG, een bijzondere categorie van persoonsgegevens. Dit zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn omdat de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden van personen. Op grond van artikel 9.1 AVG is de verwerking van biometrische gegevens daarom verboden, tenzij de verwerkingsverantwoordelijke zich rechtmatig kan beroepen op een van de in artikel 9.2 AVG limitatief opgesomde uitzonderingsgronden.

Het is met name de gewijzigde juridische kwalificatie van het begrip biometrische gegevens en de onafzienbare toename van biometrische verwerkingsprocessen in het dagelijkse leven die de Autoriteit ertoe hebben bewogen om zich uit te spreken over dit onderwerp.

De aanbeveling heeft als voornaamste doel het begeleiden van verwerkingsverantwoordelijken en verwerkers om hen in staat te stellen de regels van de AVG inzake de verwerking van biometrische gegevens juist te interpreteren en toe te passen. In die context dient evenwel opgemerkt te worden dat de aanbeveling niet van toepassing is op de verwerking van biometrische gegevens door bevoegde autoriteiten in de zin van de Politie-Justitie richtlijn of enige andere verwerking van gegevens die niet gevat wordt door de AVG. Daarnaast wil deze aanbeveling de wetgever uitnodigen om te voorzien in een wettelijke basis voor de verwerking van biometrische gegevens.

In eerste instantie licht de Autoriteit in Hoofdstuk II uitvoerig het juridische kader van de geviseerde verwerking toe. Er wordt met name aandacht besteed aan de begrippen persoonsgegevens, verwerking van persoonsgegevens, verwerkingsverantwoordelijke en verwerker waarna in tweede instantie toelichting wordt gegeven bij de concrete omvang van de notie 'verwerking van biometrische gegevens'. Een goed begrip van de gebruikte terminologie is immers cruciaal vooraleer er overgegaan kan worden tot de toepassing van de gegevensbeschermingsprincipes op het verwerken van biometrische gegevens.

Hoofdstuk III handelt vervolgens over de relevante gegevensbeschermingsprincipes in het kader van de verwerking van biometrische gegevens. Daarbij wordt in het bijzonder aandacht besteed aan het kiezen van een juiste rechtsgrond (uitzonderingsgrond), het correct omschrijven van de doeleinden van de verwerking, de vereiste van proportionaliteit, de beveiliging van de verwerking, het beginsel van

opslagbeperking, de transparantieverplichting en de (eventuele) verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren.

Deze analyse, in het bijzonder voor wat betreft het beroep op een rechtsgrond, dan wel een uitzonderingsgrond die de verwerking van biometrische gegevens rechtvaardigt, leert dat er een lacune bestaat in het Belgische recht zodanig dat elke verwerking van biometrische gegevens in het raam van de authenticatie van personen, voor zover er geen beroep kan worden gedaan op de expliciete toestemming en met uitzondering van de verwerking van biometrische gegevens in het kader van de eID (elektronische identiteitskaart) (en het paspoort), op heden zonder rechtsgrond is. Dit betekent concreet dat de Belgische wetgever de modaliteiten van de verwerking van biometrische gegevens zal moeten neerleggen in de wet in zoverre de wetgever het gebruik van biometrische gegevens in een bepaalde context wil (blijven) toestaan. De Autoriteit aanvaardt evenwel dat deze vereiste in belangrijke mate afwijkt van het regime vóór de inwerkingtreding van de AVG. Daarom, rekening houdend met de beginselen van behoorlijk bestuur, wordt er met ingang van de publicatie van deze aanbeveling voorzien in een overgangsperiode van één jaar gedurende dewelke de verwerking van biometrische gegevens overeenkomstig de oude norm gedoogd zal worden en er door de Autoriteit niet proactief zal worden opgetreden. Deze periode van één jaar moet de verwerkingsverantwoordelijken en de wetgever in staat te stellen om te voorzien in een wettelijke basis teneinde de geviseerde verwerkingen in overeenstemming te brengen met de bepalingen van de AVG zoals toegelicht in de aanbeveling.

I. Inleiding

1. Voorwoord

De Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens* (hierna "AVG") trad op 25 mei 2018 in werking. Zij trekt de Richtlijn van het Europees Parlement en de Raad van 24 oktober 1995 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens* in en bevestigt en consolideert de rechtspraak zoals die door het Hof van Justitie van de Europese Unie en door de Werkgroep Artikel 29[1] (hierna "Groep 29") werden toegepast door middel van officiële standpunten en richtlijnen. Door over te stappen van een richtlijn naar een verordening heeft de Europese wetgever de bescherming van persoonsgegevens, die in artikel 8 van het Handvest van de grondrechten van de Europese Unie als grondrecht is vastgelegd, rechtstreeks en op uniforme wijze in de lidstaten toepasbaar willen maken.[2]

Een van de belangrijkste doelstellingen van de AVG is het versterken van de rechten van de betrokkenen. De AVG kent met name de toezichthoudende autoriteiten belangrijke bevoegdheden toe, zodat ze ook sancties kunnen opleggen in geval van niet-naleving van de erin vastgelegde regels. Uit de Eurobarometer van mei 2019 over de AVG blijkt dat de kennis van de betrokkenen over de toepasselijke gegevensbeschermingsregels en over hun rechten duidelijk toeneemt.[3] Zo oefenen ze meer dan vroeger hun rechten uit. Dit is onder meer het geval voor het intrekken van hun toestemming of het zich verzetten tegen de verwerking van hun gegevens voor commerciële doeleinden.[4]

Het is in het licht van deze versterkte rechten dat tal van consumenten- en burgerrechtenorganisaties het erover eens zijn dat de AVG sterk bijdraagt aan een rechtvaardige digitale samenleving, gebaseerd op het wederzijdse vertrouwen tussen betrokken personen en actoren die een rol spelen bij de verwerking van hun gegevens.

Om deze doelstelling te realiseren, legt de AVG de nadruk op de responsabilisering van de verschillende actoren die persoonsgegevens verwerken, ongeacht of het nu particulieren, beroepsbeoefenaars,

[1] De Groep 29 is vervangen door het Europees Comité voor gegevensbescherming (dikwijls aangeduid met de Engelse afkorting "EDPB"), dat de verschillende standpunten ingenomen door de Groep 29 overneemt. Er zal daarom in deze aanbeveling verwezen worden naar de standpunten van de EDPB.
[2] Met, op enkele uitzonderingen na, enige speelruimte voor de nationale wetgevers, waar we in deze aanbeveling niet dieper op ingaan.
[3] https://europa.eu/eurobarometer/screen/home en zie ook: https://ec.europa.eu/commission/presscorner/detail/nl/IP_19_2956.
[4] Zie het rapport van de "*Multistakeholder Group on the General Data Protection Regulation*" die naast de Europese Commissie werd opgericht en waarbij het maatschappelijk middenveld en vertegenwoordigers van de beroepssectoren, academici en mensen uit de praktijk betrokken zijn, dat beschikbaar is via de volgende link: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3537&Lang=NL&lang=nl.

rechtspersonen of overheden betreft, en dit in elke fase van de verwerking, zowel op nationaal, Europees als internationaal niveau.

De rol van de toezichthoudende autoriteiten is bijgevolg niet louter beperkt tot een repressief optreden. Gelet de aanzienlijke sancties waaraan overtreders blootstaan en het feit dat persoonsgegevens onontbeerlijk zijn geworden bij de uitoefening van de meeste sociaaleconomische activiteiten, wordt er in het bijzonder ingezet op preventie en sensibilisering.

2. Context en toepassingsgebied van de aanbeveling

Overeenkomstig artikel 9.1 AVG zijn biometrische gegevens, en dit in tegenstelling tot de situatie vóór de inwerkingtreding van de AVG, een bijzondere categorie van persoonsgegevens. Dit zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn omdat de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden van personen. Biometrische lichaamskenmerken kunnen uniek of quasi uniek zijn en zijn daarom bijna altijd te herleiden naar één individu. Daarnaast bevatten ze vaak meer informatie dan strikt noodzakelijk is voor de verwezelijking van de beoogde doeleinden, kunnen ze gevoelige gegevens bevatten over de gezondheidstoestand en zijn ze permanent of evolueren ze traag, wat impliceert dat een datalek ernstige lange termijn gevolgen met zich meebrengt. Op grond van artikel 9.1 AVG is de verwerking van biometrische gegevens daarom verboden, tenzij de verwerkingsverantwoordelijke zich rechtmatig kan beroepen op een van de in artikel 9.2 AVG limitatief opgesomde uitzonderingsgronden. Deze gewijzigde kwalificatie brengt evenwel met zich mee dat de richtlijnen van de Commissie voor de bescherming van de persoonlijke levenssfeer, de rechtsvoorganger van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit"), inzake het verwerken van biometrische gegevens in het raam van authenticatie van personen overeenkomstig het advies nr. 17/2008 niet langer relevant zijn.

Daarenboven, dankzij het steeds betrouwbaarder en goedkoper worden van biometrische authenticatiemethodes, heeft de Autoriteit vastgesteld dat individuen, zowel in hun relatie met de overheid als met private ondernemingen, steeds vaker geconfronteerd worden met de verwerking van hun biometrische gegevens.

Het is met name de gewijzigde juridische kwalificatie van het begrip biometrische gegevens en de onafzienbare toename van biometrische verwerkingsprocessen in het dagdagelijkse leven die de Autoriteit ertoe hebben bewogen om zich opnieuw uit te spreken over dit onderwerp.

De aanbeveling heeft als voornaamste doel het begeleiden van verwerkingsverantwoordelijken en verwerkers om hen in staat te stellen de regels van de AVG inzake de verwerking van biometrische gegevens juist te interpreteren en toe te passen. Een AVG-conforme werkwijze is immers een onmisbare

en nuttige bondgenoot in hun relatie met de betrokkenen. Het is door op een transparante manier met de betrokken te communiceren over hoe bepaalde persoonsgegevens verwerkt worden en door aan te tonen dat er gepaste maatregelen werden getroffen om ervoor te zorgen dat de verwerking in overeenstemming is met de regelgeving, dat er een vertrouwensrelatie tot stand kan komen die nodig is om de beoogde doelstellingen te verwezenlijken en te behouden. Deze aanbeveling treedt aldus niet in de plaats van de algemene verplichtingen die voortvloeien uit de AVG en de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*, maar wenst deze slechts aan te vullen of te specifiëren. Ondernemingen en instanties die een in deze aanbeveling geviseerde verwerking uitvoeren, zullen steeds alle wettelijke en regelgevende akten inzake de verwerking van persoonsgegevens in acht moeten nemen. In dit kader wil de Autoriteit evenwel benadrukken dat de draagwijdte van deze aanbeveling zich beperkt tot de verwerking van biometrische gegevens binnen het toepassingsgebied van de AVG. De in deze aanbeveling opgenomen richtlijnen zijn dus niet van toepassing op de verwerking van biometrische gegevens door bevoegde autoriteiten[5] in de zin van de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad*[6] (Politie-Justitie Richtlijn) of enige andere verwerking van gegevens die niet gevat wordt door de AVG.

Tot slot zal het noodzakelijk zijn om deze aanbeveling ten gepaste tijde aan te passen/ te vervolledigen, rekening houdend met nieuwe ontwikkelingen inzake de verwerking van biometrische gegevens.

3. Juridisch kader

De regelgeving inzake de verwerking van biometrische gegevens vinden we terug in de AVG. De analyse van de regels van de AVG is in voorkomend geval gebaseerd op de standpunten van het Europees Comité voor gegevensbescherming (hierna "EDPB") en van zijn voorganger, de Groep 29. Sommige van de richtlijnen van deze laatste werden reeds door de EDPB herzien en geactualiseerd, terwijl andere als zodanig werden aangenomen. De EDPB dient zich tevens uit te spreken over vragen of thema's die nog

[5] Artikel 3, 7) Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad* bepaalt dat voor de toepassing van de richtlijn wordt verstaan onder "bevoegde autoriteit":
"*a) iedere overheidsinstantie die bevoegd is voor 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; of*
b) ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op 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;"
[6] De richtlijn zoals bedoeld in voetnoot 5.

niet het voorwerp van eerdere standpuntbepalingen uitmaakten. Dit geldt met name voor de richtlijnen die worden verwacht m.b.t. de verwerking van biometrische gegevens. De door de Autoriteit ingenomen standpunten in deze aanbeveling doen evenwel geen afbreuk aan de toekomstige positie van de EDPB in dit kader. De Autoriteit maakt immers deel uit van, en is gebonden door de standpunten van de EDPB. Een wijziging van deze aanbeveling teneinde haar in overeenstemming te brengen met de Europese visie is bijgevolg niet uitgesloten. Om die reden raadt de Autoriteit aan regelmatig haar website te raadplegen, waar steeds de laatste versie van deze aanbeveling voorhanden zal zijn.

II. Verwerking van biometrische gegevens waar gaat het over?

1. Juridisch kader

1.1 Persoonsgegevens[7]

Artikel 4.1) AVG definieert 'persoonsgegevens' als volgt: "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als 'identificeerbaar' wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, 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*."

De termen 'geïdentificeerd' en 'identificeerbaar' zijn cruciaal om te begrijpen wat een persoonsgegeven is. Terwijl gegevens die toelaten een persoon direct te identificeren vaak evident zijn (bijvoorbeeld een combinatie van achternaam, voornaam en adres of geboortedatum of een uniek identificatienummer, zoals een klantnummer), is het soms moeilijker om te weten wat moet worden verstaan onder 'gegevens waardoor een persoon indirect geïdentificeerd kan worden' (bijvoorbeeld gepseudonimiseerde gegevens).

Overeenkomstig artikel 4.5) AVG zijn gepseudonimiseerde gegevens persoonsgegevens die op een zodanige manier verwerkt worden dat ze niet langer aan een specifieke betrokkene gekoppeld kunnen worden zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden

[7] Voor meer informatie over dit onderwerp, raadpleeg opinion 4/2007 (WP 136) over het begrip persoonsgegeven, goedgekeurd op 20 juni 2007 door de Groep 29 en beschikbaar op deze link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_nl.pdf.

gekoppeld. Met andere woorden, elk stukje informatie dat gekoppeld is aan een persoon, hoe gering het ook lijkt als u het op zichzelf beschouwt (bijvoorbeeld een leeftijd, een woonplaats, de kleur van de ogen of het geslacht, of zelfs een registratienummer), is een persoonsgegeven van zodra het in combinatie met een of meer andere gegevens een natuurlijke persoon kan identificeren. Zolang er aldus dergelijke aanvullende gegevens voorhanden zijn, en ongeacht de kwaliteit van de genomen technische of organisatorische maatregelen, vallen gepseudonimiseerde gegevens onder het toepassingsgebied van de AVG.

'Geanonimiseerde' gegevens daarentegen worden niet als persoonsgegevens aangemerkt, omdat de identificatie van een natuurlijke persoon aan de hand van dergelijke gegevens niet langer mogelijk is, zelfs niet met behulp van aanvullende informatie. Hoewel de AVG om deze reden dergelijke gegevens van zijn toepassingsgebied uitsluit, leert de praktijk dat het onderscheid tussen gepseudonimiseerde en geanonimiseerde gegevens steeds moeilijker te maken valt. In deze context kan worden opgemerkt dat de EDPB op heden werkt aan de richtsnoeren inzake anonymisering van gegevens.

Onthoud tot slot dat – in beginsel – enkel gegevens van levende, natuurlijke personen persoonsgegevens zijn.

1.2 Verwerking van persoonsgegevens

Artikel 4.2) AVG definieert 'verwerking' als volgt: *"een bewerking of geheel van bewerkingshandelingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het beperken, wissen of vernietigen van gegevens*".

Net als over zijn verwerkingsdoeleinden, moet elke verwerkingsverantwoordelijke ook transparant zijn over de verwerkingen die hij op de gegevens van een betrokkene uitvoert. De mate van detail hangt onder meer af van het type van betrokkenen (kinderen, professionals, experts, enz.), de manier waarop hun persoonsgegevens verwerkt worden en de mate waarin dergelijke verwerkingen een inmenging in hun recht op privacy met zich meebrengen. Het vaststellen van de verwerkingen die voor elk afzonderlijk oogmerk uitgevoerd worden is tevens een cruciaal element bij de beoordeling van de proportionaliteit (lees: de toelaatbaarheid) van de desbetreffende verwerking. In die zin is het onwaarschijnlijk dat de installatie van een vingerafdruksensor met het oogmerk toegang te verschaffen tot een koffiekamer de proportionaliteitstoets zal doorstaan.

Teneinde een overzicht te houden over de verwerkingsactiviteiten is het op grond van artikel 30 AVG tevens verplicht om een register van de verwerkingsactiviteiten bij te houden wanneer een bedrijf of organisatie meer dan 250 personen in dienst heeft of wanneer het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of **de verwerking bijzondere categorieën van gegevens betreft**. Indien er aldus sprake is van een verwerking van biometrische gegevens, zal het steeds verplicht zijn om een dergelijk register bij te houden.

Dit register bevat naast een lijst van de uitgevoerde verwerkingsactiviteiten ook andere informatie zoals de persoonsgegevens of de categorieën van persoonsgegevens die worden verwerkt. Dit register moet schriftelijk, of elektronisch, worden opgesteld en moet helder en begrijpelijk zijn.

Het register helpt dus ook bij de nauwkeurige inventarisering van de verwerkte gegevens en is daarom een onmisbaar hulpmiddel om inzicht te krijgen in het ecosysteem van de gegevensverwerkingen waarvoor een bepaalde verwerkingsverantwoordelijke verantwoordelijk is. Een correct bijgehouden register bespaart tijd bij het nakomen van uw AVG-verplichtingen en maakt dat alle mensen die in uw organisatie werken en betrokken zijn bij de verwerking van gegevens die nuttig zijn voor uw organisatie, indien nodig, geraadpleegd kunnen worden en/of geïnformeerd zijn over de verwerkingen binnen de organisatie, wat op alle niveaus ook bijdraagt tot een groter bewustzijn inzake gegevensbescherming. Het zal u ook helpen om een gegevensbeschermingseffectbeoordeling (zie *infra* rubriek III.7) op te stellen, en om samen te werken met de Autoriteit in het geval dat die vragen heeft betreffende een van uw verwerkingsactiviteiten.

1.3 Verwerkingsverantwoordelijke[8]

U bent 'verwerkingsverantwoordelijke' wanneer u, alleen of samen met anderen, de doeleinden en de middelen voor de verwerking van persoonsgegevens bepaalt.

Het is belangrijk om te onthouden dat een organisatie niet "van nature" een verwerkingsverantwoordelijke of verwerker is. Alles hangt af van de manier waarop de organisatie zich daadwerkelijk gedraagt. U dient zich voor elke handeling die u met biometrische gegevens verricht, af te vragen wie het doel van de verwerking heeft bepaald en de manier waarop de gegevens in kwestie worden verwerkt.

[8] Voor een volledig overzicht betreffende de figuur van verwerkingsverantwoordelijke, zie:: EDPB Guidelines 07/2020 *on the concepts of controller and processor in the GDPR* (vooralsnog enkel beschikbaar in het Engels). Te raadplegen via: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_nl.

Om uw rol en die van de andere partijen (zoals technische dienstverleners of derden die u gegevens verstrekken) te verduidelijken, stel uzelf volgende vragen:

- Wie beslist in eerste instantie om over te gaan tot de verzameling van (biometrische) gegevens?
- Wie omschrijft de betrokkenen of categorieën van betrokkenen?
- Wie bepaalt welke categorieën van gegevens verzameld dienen te worden?
- Wie bepaalt het/de doeleinde(n) waarvoor de gegevens gebruikt worden?
- Wie bepaalt de rechtsgrond voor de verwerking?
- Wie bepaalt of de gegevens moeten worden doorgegeven, en zo ja, aan wie?
- Wie bepaalt de inhoud van de informatie die aan de betrokkenen wordt verstrekt m.b.t de verwerking of verwerkingsactiviteiten die op hun gegevens worden toegepast?
- Wie bepaalt hoe lang de gegevens bewaard worden? en
- Wie bepaalt hoe gereageerd wordt wanneer betrokkenen hun rechten uitoefenen?

Al deze beslissingen kunnen enkel genomen worden door de verwerkingsverantwoordelijke in de context van zijn algemene controle over de gegevensverwerking. Neemt u een van deze beslissingen, dan bent u meer dan waarschijnlijk verwerkingsverantwoordelijke.

Artikel 26 van de AVG voorziet ook in de situatie waarin twee of meer verwerkingsverantwoordelijken co-existeren, de zogenaamde 'gezamenlijke verwerkingsverantwoordelijken'. Dit is het geval wanneer meerdere entiteiten gezamenlijk het doel en de middelen van de verwerking bepalen. Artikel 26 van de AVG bepaalt dat in dat geval de gezamenlijke verwerkingsverantwoordelijken hun respectieve verplichtingen op een transparante manier moeten vastleggen door middel van een overeenkomst, die hun respectieve rollen ten aanzien van de betrokkenen correct weergeeft.

1.4 Verwerker[9]

Wanneer een overheids- of private instantie of een natuurlijke persoon namens u, op basis van uw instructies, persoonsgegevens verwerkt met als enige doel u in staat te stellen uw doeleinden te realiseren, is er sprake van een verwerkersrelatie.

Het inschakelen van een verwerker heeft tot gevolg dat de vereisten van artikel 28 van de AVG nageleefd moeten worden.

Onthoud in de eerste plaats dat u ongeacht de situatie en ongeacht de verwerker, van zodra u als verwerkingsverantwoordelijke optreedt, gebonden bent aan de verplichtingen die de AVG u oplegt en dat u in voorkomend geval verantwoording dient af te leggen voor inbreuken op deze verplichtingen.

[9] Voor een volledig overzicht inzake de relatie verwerkingsverantwoordelijke-verwerker, zie: EDPB Guidelines 07/2020 *on the concepts of controller and processor in the GDPR*, zie voetnoot 8.

Het is om deze redenen dat artikel 28.1 van de AVG bepaalt dat u enkel een beroep mag doen op verwerkers die voldoende garanties bieden aangaande het toepassen van passende technische en organisatorische maatregelen. Dit vloeit ook voort uit artikel 24 van de AVG dat u verplicht om passende technische en organisatorische maatregelen te nemen teneinde zowel te waarborgen als aan te tonen dat uw gegevensverwerking in overeenstemming met de AVG wordt uitgevoerd. Een beroep doen op een gecertificeerde verwerker of een verwerker die zich bij een goedgekeurde gedragscode heeft aangesloten, vormt een element dat het bestaan van voldoende garanties zoals vereist door de artikelen 28.1 en 28.4 van de AVG kan aantonen.

Terwijl in een ideale situatie de verwerkingsverantwoordelijke volledige instructies geeft betreffende de verwerking die aan de verwerker is toevertrouwd, is dit in de realiteit vaak minder vanzelfsprekend en kan het zijn dat bepaalde elementen niet door de verwerkingsverantwoordelijke, maar door zijn verwerker bepaald worden op grond van diens deskundigheid op het vlak van de technologieën die toegepast worden bij de verwerking en/of de meest geschikte beveiligingsmaatregelen van de gegevens. Het feit dat een verwerker over meer deskundigheid beschikt dan u over de te gebruiken technische middelen bij de gegevensverwerking, leidt op zich niet tot een herkwalificatie van zijn positie van verwerker naar die van verwerkingsverantwoordelijke. Bepaalde verwerkers bieden kant-en-klare oplossingen aan zonder dat dit afbreuk doet aan uw verplichting om als verwerkingsverantwoordelijke de vereiste beslissingen te nemen met betrekking tot de verwerkte gegevens, de nagestreefde doeleinden en/of de middelen om die te bereiken.

Daarnaast dient nog opgemerkt te worden dat eenzelfde instantie zowel de rol van verwerker als van verwerkingsverantwoordelijke kan vervullen, maar niet voor dezelfde verwerking van persoonsgegevens. Een verwerker die zo handelt, moet ervoor zorgen dat zijn systemen en procedures een onderscheid maken tussen de persoonsgegevens die hij verwerkt in zijn hoedanigheid van verwerkingsverantwoordelijke en de persoonsgegevens die hij verwerkt in zijn hoedanigheid van verwerker. Indien bepaalde gegevens identiek zijn, moeten deze systemen een onderscheid kunnen maken tussen deze twee situaties, zodat op elke situatie verschillende processen en maatregelen toegepast kunnen worden.

Indien een organisatie evenwel gelijktijdig optreedt als verwerkingsverantwoordelijke en verwerker voor verschillende verwerkingsactiviteiten op basis van dezelfde persoonsgegevens, moeten de betrokkenen naar behoren worden geïnformeerd door de organisatie, zowel in haar hoedanigheid als verwerkingsverantwoordelijke als in haar hoedanigheid als verwerker. Dit is vanzelfsprekend voor zover de verwerkingsactiviteiten rechtmatig zijn. Dit geldt met name voor ontwikkelaars van gezichtsherkenningssoftware die enerzijds als verwerker optreden ten aanzien van een entiteit die gebruik maakt van deze software voor welbepaalde doeleinden (de verwerkingsverantwoordelijke) maar anderzijds de verzamelde gegevens ook voor persoonlijke doeleinden gaan verwerken. De te

verstrekken informatie moet in dit geval de verschillende verwerkingen vermelden evenals de verzamelde gegevens, de ontvangers van de gegevens en hun eigen doeleinden.

Voorbeeld

In een Chinees restaurant van de keten KFC wordt gezichtsherkenningssoftware (ontwikkeld door Baidu, de Chinese tegenhanger van Google) aangewend om de preferenties van de klant te voorspellen. In deze verhouding is KFC de verwerkingsverantwoordelijke (zij bepaalt immers het doel van de verwerking) en Baidu de verwerker aangezien haar software instaat voor de effectieve verwerking. Wanneer Baidu evenwel de persoonsgegevens in kwestie zou aanwenden om biometrische klantenprofielen op te stellen en deze te verstrekken aan derde ondernemingen dan handelt zij in die hoedanigheid als verwerkingsverantwoordelijke.[10]

Tot slot wil de Autoriteit erop wijzen dat uw werknemers niet uw verwerkers zijn. Zolang deze werknemers onder uw gezag handelen in een band van ondergeschiktheid, maken zij integraal deel uit van uw organisatie.

2. Definitie biometrische gegevens

2.1 Situering

Artikel 4.14) AVG definieert 'biometrische gegevens' als "*persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan* ***eenduidige identificatie van die natuurlijke persoon*** *mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens*". Ook wanneer de gegevens niet verwerkt worden met het oog op eenduidige identificatie van personen, maar wanneer zulks wel mogelijk zou zijn rekening houdend met de aard van de gegevens zal er aldus sprake zijn van een verwerking van biometrische gegevens in de zin van de AVG.

Teneinde elke verwarring hieromtrent te vermijden en de rechtszekerheid te bevorderen is het belangrijk om op te merken dat de notie biometrische gegevens in de wetenschappelijk context een andere betekenis heeft dan in de (Europese) gegevensbeschermingscontext. De wetenschappelijke definitie is terug te vinden in The International Standard ISO/IEC 2382–37[11] en luidt als volgt: "*biometric sample or aggregation of biometric samples at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property.*" De ISO/IEC-standaard beschouwt daarom

[10] Zie voor meer informatie: https://www.theguardian.com/technology/2017/jan/11/china-beijing-first-smart-restaurant-kfc-facial-recognition.

[11] International Standard ISO/IEC 2382–37 is de wetenschappelijke referentietekst inzake biometrie en harmoniseert de internationale woordenschat op het gebied van biometrie http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55194.

het volgende als biometrische gegevens: (1) de registratie van data (*'biometric sample'*), (2) de extractie van data uit de samples *('biometric feature'*), (3) de attributie van biometrische samples aan welbepaalde individuen (*'biometric reference'*) en (4) de vergelijking tussen de verschillende samples (*'biometric probe'*). Het valt meteen op dat de notie in de wetenschappelijke context niet noodzakelijkerwijze betrekking heeft op het verband tussen een individu en zijn of haar biometrische gegevens. Dit terwijl de identificatie, of liever de **identificeerbaarheid** van een individu fundamenteel is voor het begrip 'biometrische gegevens' in de gegevensbeschermingscontext. De verwerking van biometrische gegevens in de wetenschappelijke zin zonder de mogelijkheid om individuen te gaan identificeren valt bijgevolg buiten het toepassingsgebied van de AVG. Biometrische gegevens kunnen immers slechts geclassificeerd worden als persoonsgegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken (ook wanneer dit in eerste instantie niet de bedoeling is).[12] Dergelijke conclusie is conform artikel 4.1) AVG waaruit volgt dat het begrip persoonsgegevens enkel betrekking heeft op informatie **over een geïdentificeerde of identificeerbare natuurlijke persoon**.

Desalniettemin moet er worden vastgesteld dat de notie biometrische gegevens onder vrij algemene termen werd gedefinieerd, wat impliceert dat de AVG erkent dat biometrische technologie nog volop in ontwikkeling is en zal blijven evolueren.

Tot slot zijn biometrische gegevens op grond van artikel 9.1 AVG een bijzondere categorie van persoonsgegevens. De verwerking van dergelijke bijzondere categorieën is in beginsel verboden, tenzij er aan één van de in artikel 9.2 AVG genoemde uitzonderingsgronden op het verwerkingsverbod is voldaan. De implicaties die deze kwalificatie heeft op de verwerking worden uitvoerig toegelicht in Hoofdstuk III van deze aanbeveling.

2.2 Concrete invulling van het begrip biometrische gegevens

De AVG onderscheidt twee categorieën informatie die als biometrische gegevens kunnen worden beschouwd. De eerste heeft betrekking op lichamelijke eigenschappen – namelijk de fysische of fysiologische kenmerken van een persoon. De invulling van deze categorie is vrij eenvoudig en stemt overeen met wat de meeste mensen begrijpen onder biometrische gegevens, zoals bijvoorbeeld gezichtsinformatie, vingerafdrukken en irisscans.

De tweede categorie, gedragsgerelateerde informatie, is aanzienlijk ruimer. Elk gedragsmatig kenmerk dat de unieke identificatie van een persoon toelaat wordt logischerwijze geacht een biometrische gegeven te zijn. De verwerkingsmogelijkheden inzake gedragsgerelateerde informatie evolueren echter

[12] Overweging 51 AVG.

in snel tempo. Het is bijgevolg niet mogelijk om een exhaustieve lijst van gevatte verwerkingen op te stellen. Het zal dus steeds nodig zijn om aan de hand van concrete elementen na te gaan of er al dan niet sprake is van een verwerking van gedragsgerelateerde gegevens die de unieke identificatie van personen toelaat.

Voorbeelden gedragsgerelateerde biometrische gegevens
Het gebruik van toetsenbord-, touchscreen en muispatronen ter authenticatie van personen (kent grote belangstelling in de bankensector.[13]
Identificatie aan de hand van het unieke stappatroon van personen (in het engels *gait recognition*).[14]

2.3 Biometrische templates

De werking van een biometrisch systeem wordt opgesplitst in twee fasen van inzameling van de informatie en twee manieren om de ingezamelde informatie te vergelijken (de twee functies van biometrische systemen).

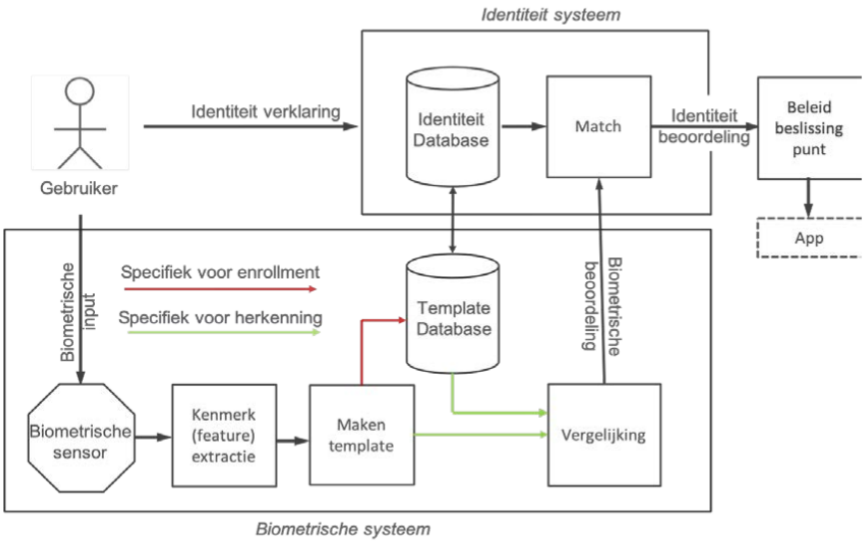
INZAMELINGSFASES

De eerste inzamelingsfase, zogenaamd de inschrijving (of de registratie), is het ogenblik waarop een biometrisch kenmerk van de betrokkene wordt ingezameld en geregistreerd op een drager voor informatieopslag (hetzij een individuele drager zoals een badge of token, hetzij in een databank). Deze referentie-informatie zal ofwel het ruwe biometrische gegeven zijn (zoals bijvoorbeeld de afbeelding van het gezicht, de hand, de iris of de digitale vingerafdruk), ofwel het geheel aan gecodeerde informatie, verkregen uit de individuele en unieke kenmerken van het ruwe gegeven met de bedoeling de identiteit van een individu te verifiëren of vast te stellen (een template). Hoewel deze templates onderscheiden zijn van de ruwe biometrische gegevens vallen zij zonder meer onder toepassingsgebied van de AVG. Daarenboven merkt de Autoriteit op dat het overeenkomstig artikel 5.1, f) *j°* artikel 32 AVG, en rekening houdend met het principe van '*privacy by design*'[15] niet langer mogelijk zal zijn om rechtmatig een beroep te doen op een systeem dat de referentie-informatie opslaat in haar onbewerkte vorm (lees: het ruwe biometrische gegeven). Tijdens de eerste inzamelingsfase zullen de ruwe biometrische gegevens steeds omgezet moeten worden naar templates waarna de ruwe gegevens onmiddellijk verwijderd moeten worden.

Tijdens de tweede inzamelingsfase toont het individu opnieuw zijn biometrische kenmerken aan het systeem dat hem moet authentiseren. Op dat ogenblik wordt een tweede biometrisch staal genomen

[13] Zie: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/inspired/behavioral-biometrics.
[14] Zie: https://www.biometricupdate.com/201311/explainer-gait-recognition.
[15] Zie art. 25 AVG.

(een persoon houdt bijvoorbeeld zijn vinger voor de sensor) en deze informatie (het ruwe gegeven of de template) wordt dan vergeleken met de referentie-informatie om na te gaan of deze overeenstemmen. Als de informatie die ingezameld wordt tijdens de tweede inzameling overeenstemt met de referentie-informatie (positieve koppeling) beschouwt het systeem de persoon die zich aanbiedt als diegene die vooraf werd geregistreerd bij de inschrijvingsfase.



Schematisch model van een biometrisch systeem voor de verificatie van de *identiteit* bestaande uit een registratie- en verificatiefase.

Afhankelijk van de manier waarop het template opgeslagen wordt gelden er strenge voorwaarden. De aanbeveling onderscheidt drie mogelijkheden:

- (type 1) Beheer van het template door de betrokkene zelf: het enige duurzame opslagmedium van het template wordt uitsluitend door de betrokkene bewaard, of, in voorkomend geval, in het toestel waarin de biometrische sensor geplaatst is zonder de mogelijke koppeling met andere informaticasystemen. Denk bijvoorbeeld aan een badge of token of lokale opslag in de sensor aan de ingang van het gebouw. Deze werkwijze dient principieel aangewend te worden en er kan slechts in uitzonderlijke gevallen van afgeweken worden;
- (type 2) Gedeeld beheer: Er is een centrale template database onder het beheer van de verwerkingsverantwoordelijke zonder dat deze laatste er evenwel gebruik van kan maken zonder de toestemming van de betrokkene. Zoals bijvoorbeeld wanneer toegang tot een welbepaalde template slechts verleend wordt mits invoering van een door de betrokkene gekozen wachtwoord.
- (type 3) Exclusief beheer door de verwerkingsverantwoordelijke: het template wordt in exploiteerbare vorm opgeslagen in een template database onder het exclusieve beheer van de verwerkingsverantwoordelijke. In dit geval dienen de meest stringente voorwaarden in acht genomen te worden en zal het voorafgaandelijk uitvoeren van een gegevensbeschermingseffectbeoordeling steeds noodzakelijk zijn.

De Autoriteit benadrukt dat de opslag van templates overeenkomstig de types 2 en 3 slechts in uitzonderlijke omstandigheden mogelijk zal zijn. Denk bijvoorbeeld aan authenticatie in kritieke omgevingen waar het verlies van een token of badge (exclusief beheer door de betrokkene) bijzonder ernstige gevolgen zou hebben (bijvoorbeeld: toegang tot een operatiekwartier of kerncentrale).

Tot slot wenst de Autoriteit er in deze context op te wijzen dat deze aanbeveling in principe geen betrekking heeft op het volledig lokaal gebruik door de gebruiker van authenticatie aan de hand van biometrische systemen. Dergelijke verwerkingen van biometrische gegevens vallen immers onder de huishoudelijke exceptie overeenkomstig artikel 2.2, c) AVG. Denk in dit kader bijvoorbeeld aan de persoonlijke authenticatie via smartphones of andere elektronische toestellen waar gezichtsherkenningssoftware en vingerafdruksensors steeds vaker optreden als alternatief voor de traditionele pincode. De voorwaarden en modaliteiten van de huishoudelijke exceptie worden uitvoerig toegelicht onder rubriek III.1.3.3.

VERGELIJKINGSFASE

Er bestaan twee manieren om de informatie te vergelijken die verkregen werd tijdens de inzamelingsfasen en zij vormen de twee belangrijkste functies van de biometrie: de identificatiefunctie en de verificatiefunctie. Hoewel deze beide functies aangewend kunnen worden in het raam van de authenticatie geniet de verificatiefunctie zonder meer de voorkeur (aangezien de biometrische referentie-informatie niet noodzakelijkerwijze opgeslagen moet worden in een centrale database), en zal de identificatiefunctie slechts in uitzonderlijke en gemotiveerde gevallen aangewend kunnen worden.

De identificatiefunctie bestaat erin de informatie van de tweede fase te vergelijken met al de biometrische informatie die beschikbaar is in het biometrisch systeem en die per definitie opgeslagen is in een databank (‘*one-to-many comparison*’). Deze functie zal in de eerste plaats toelaten de gebruiker te identificeren tussen alle geregistreerde personen en kan in een latere fase dienen om hem te authentiseren.

De verificatiefunctie bestaat erin om de informatie van de tweede fase te vergelijken met de vooraf geregistreerde informatie toebehorend aan één enkele persoon (‘*one-to-one comparison*’). Deze functie leent zich in het bijzonder voor situaties waar de persoon zich wenst te authentiseren en dus bereid is om vrijwillig een element kenbaar te maken dat toelaat om hem te identificeren op basis van de vergelijking tussen de vooraf vastgestelde referentie-informatie en het staal van de nieuwe inzameling.

III. Toepassing van de gegevensbeschermingsprincipes op het verwerken van biometrische gegevens

1. Rechtsgrond

1.1 Waarom een rechtsgrond?

De verwerking van persoonsgegevens is in beginsel enkel toegestaan als die gebaseerd is op een van de zes rechtsgronden voorzien in artikel 6 van de AVG. Wanneer er sprake is van een verwerking van bijzondere categorieën persoonsgegevens zal er eveneens beroep moeten worden gedaan op een van de uitzonderingsgronden voorzien in artikel 9.2 AVG. De aanwezigheid van een uitzonderingsgrond doet in dat geval dienst als rechtsgrond voor de verwerking. U kan geen gegevens verwerken zonder rechtsgrond, u moet er dus voor zorgen dat u er één hebt vooraleer u met uw verwerking aanvangt.

Het is ook van essentieel belang dat u zich afvraagt wat uw rechtsgrond is, aangezien de voorwaarden van elk van de rechtsgronden verschillende zijn. De keuze van uw rechtsgrond heeft gevolgen voor de rechten van de betrokkenen, waarvan u de bijzonderheden moet kennen, niet alleen om hen correct te kunnen informeren, maar ook om de effectieve uitoefening van hun rechten te waarborgen.

De kwalificatie van het begrip 'biometrische gegevens' als een bijzondere categorie van persoonsgegevens in de zin van artikel 9.1 AVG heeft belangrijke gevolgen voor het bepalen van de rechtsgrond en brengt met zich mee dat de richtlijnen inzake de verwerking van biometrische gegevens in het raam van authenticatie van personen van de Commissie voor de bescherming van de persoonlijke levenssfeer niet langer van toepassing zijn. Dit wordt uitvoerig toegelicht onder rubriek III.1.3.

1.2 Kan de rechtsgrond gewijzigd worden?

De rechtsgrond kan niet gewijzigd worden tijdens de verwerking. Dit betekent dat als de verwerkingsverantwoordelijke zich op een ongeschikte rechtsgrond beroept, of als de gekozen rechtsgrond "vervalt" omdat de voorwaarden ervan niet, of niet langer vervuld zijn, de verwerking niet verdergezet kan worden.

Indien een verwerking bijvoorbeeld gebaseerd is op (expliciete) toestemming, moet u, van zodra de persoon zijn toestemming intrekt, alle gegevensverwerkingen die op deze rechtsgrond gebaseerd zijn,

stopzetten, tenzij u dezelfde gegevens blijft verwerken in het kader van een ander doeleinde waarvoor u een andere geldige rechtsgrond hebt.

1.3 Welke rechtsgrond gebruiken voor de verwerking van biometrische gegevens?

Er bestaat geen hiërarchie tussen de rechtsgronden die de AVG voorziet. Het is aan u om aan te tonen dat uw verwerking geldig gebaseerd is op een van de uitzonderingsgronden overeenkomstig artikel 9.2 AVG aangezien de in deze aanbeveling geviseerde verwerkingen steeds betrekking hebben op bijzondere categorieën van persoonsgegevens, namelijk biometrische gegevens. In dit opzicht dient wel opgemerkt te worden dat uit de richtlijnen van de Groep 29 en de EDPB blijkt dat een dubbele rechtsgrond alleen vereist is indien de uitzonderingsgrond vermeld in artikel 9.2 AVG minder beschermend is dan de rechtsgronden vermeld in artikel 6 AVG. Zulks zal bijvoorbeeld het geval zijn wanneer de verwerkingsverantwoordelijke zich beroept op artikel 9.2, e) AVG: voor gevoelige gegevens die door de betrokkene zelf openbaar zijn gemaakt moet er ook beroep worden gedaan op een rechtsgrond van artikel 6 AVG. Wanneer de verwerking echter wordt gesteund op artikel 9.2, a) AVG (de expliciete toestemming), of artikel 9.2, g) AVG (zwaarwegend algemeen belang) is dit niet nodig.

Verder, zoals vermeld in overweging 132 AVG, wordt in bepaalde specifieke wetten de rechtsgrond gespecificeerd waarop de verwerkingsverantwoordelijken zich moeten baseren om gegevens te mogen verwerken. Het is dus uw verantwoordelijkheid om na te gaan of u op basis van een specifieke wet verplicht bent een specifieke rechtsgrond te gebruiken.

Vergeet niet om in ieder geval, overeenkomstig de vereisten van artikel 13 of artikel 14 van de AVG, de betrokkenen te informeren over de rechtsgrond van uw verwerkingen. Op welke rechtsgrond u zich ook baseert, u dient deze aan de betrokkenen mee te delen.

Tot slot, desondanks het gebrek aan enige hiërarchie, blijken sommige rechtsgronden meer aangepast dan andere aan de realiteit van de verwerking van biometrische gegevens onder de AVG. Het zal met andere woorden, gelet op de voorwaarden die er aan verbonden zijn, moeilijk zijn om zich in deze context te gaan steunen op bepaalde rechtsgronden. Inzake de in deze aanbeveling beoogde verwerkingen verdienen twee rechtsgronden, gelet op hun praktisch belang, verdere toelichting. Meer bepaald gaat het over de expliciete toestemming (art. 9.2, a) AVG) en het zwaarwegende algemeen belang (art. 9.2, g) AVG).

Artikel 9.4 AVG laat aan de Lidstaten de mogelijkheid om bijkomende voorwaarden, waaronder beperkingen, met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of

gegevens over gezondheid te handhaven of in te voeren. Dergelijke bepalingen kunnen dan dienen als rechtsgrond voor de verwerking.[16] Dit zal met name noodzakelijk zijn wanneer de verwerkingsverantwoordelijke zich wil steunen op het zwaarwegend algemeen belang. Dit wordt uitvoerig toegelicht onder rubriek III.1.3.2.

1.3.1 Uitdrukkelijke toestemming

De uitdrukkelijke toestemming dient opgesplitst te worden in twee onderdelen. In de eerste plaats moet er **geldige** toestemming zijn voor de verwerking, en daarnaast moet deze toestemming **uitdrukkelijk** zijn.[17]

GELDIGE TOESTEMMING

Artikel 4.11) AVG stelt dat er enkel sprake kan zijn van toestemming van de betrokkene indien er sprake is van een (1) vrije, (2) specifieke, (3) geïnformeerde en (4) ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.

In de volgende secties zal kort verduidelijkt worden hoe deze elementen beoordeeld dienen te worden.

Ten eerste, het element 'vrij' impliceert dat er een echte keuze moet zijn voor de betrokkene. Als algemene regel geldt dat wanneer de betrokkene geen echte keuze heeft, zich verplicht voelt om toestemming te geven of negatieve gevolgen zou ondervinden door niet toe te stemmen, er onder de AVG geen sprake kan zijn van geldige toestemming. Als zodanig wordt toestemming niet geacht vrij gegeven te zijn indien de betrokkene zijn of haar toestemming niet zonder nadelige gevolgen kan weigeren of intrekken. De AVG besteedt ook aandacht aan het – in deze context belangrijke – concept van een wanverhouding tussen de verwerkingsverantwoordelijke en de betrokkene.

Een wanverhouding doet zich onder andere voor in het kader van de arbeidsverhouding. Gezien de afhankelijkheid die het gevolg is van de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de betrokkene zijn/haar toestemming voor gegevenswerking zou kunnen onthouden zonder angst of reële dreiging van nadelige gevolgen voortkomend uit die weigering. Het is onwaarschijnlijk dat de

[16] Zie bv: art. 29 Wet van 16 mei 2018, *houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (Uitvoeringswet Algemene verordening gegevensbescherming) (hierna UAVG)) (Nederland) en art. 8.II.9 Loi n° 78-17 van 6 januari 1978 *relative à l'informatique, aux fichiers et aux libertés* (Frankrijk).

[17] Voor volledige informatie over toestemming verwijzen we naar de EDPB-richtsnoeren 05/2020 *inzake toestemming overeenkomstig Verordening 2016/679*, die beschikbaar is via volgende link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_nl.pdf.

werknemer vrijelijk zou kunnen reageren op een verzoek voor toestemming van zijn/haar werkgever voor bijvoorbeeld het activeren van vingerprint authenticatiesystemen voor de toegang tot lokalen of gevoelige gegevens. Om die reden is de Autoriteit van mening dat het voor werkgevers problematisch is om (biometrische) persoonsgegevens van werknemers te verwerken op basis van (expliciete) toestemming, aangezien het onwaarschijnlijk is dat deze vrijelijk wordt verleend.

Wanverhoudingen tussen de betrokkene en de verwerkingsverantwoordelijke zijn echter niet beperkt tot arbeidsrelaties. Zoals hierboven reeds aangehaald is er sprake van een wanverhouding telkens wanneer de machtsverhouding tussen de verwerkingsverantwoordelijke en de betrokkene het vrije karakter van de toestemming in het gedrang brengt. Een belangrijk voorbeeld is de gegevensverwerking door de overheid, die evenwel buiten het bestek van deze aanbeveling valt. Daarnaast kan er ook gedacht worden aan de verhouding tussen een school en haar leerlingen of situaties waar de aanbieder van een dienst of goed een (quasi-) monopolie heeft. Ook in deze gevallen is er immers sprake van een feitelijke machtsverhouding aangezien het onwaarschijnlijk is dat de betrokkene zijn/haar toestemming weigert te geven zonder angst voor nadelige gevolgen.

Concreet zal de verwerkingsverantwoordelijke die biometrische gegevens in de zin van de AVG wil verwerken steeds moeten nagaan of er sprake is van machtsverhouding rekening houdend met de feitelijke situatie. Het is met andere woorden niet zo dat het ontbreken van een officiële machtsverhouding het bestaan ervan *de facto* uitsluit. Er dient ter zake steeds een beoordeling *in concreto* te gebeuren.

Voorbeeld

Op 22 augustus 2019 heeft de Zweedse toezichthoudende autoriteit (*Datainspektionen*) een school een boete van 200 000 SEK (ongeveer 20 000 EUR) opgelegd voor het gebruik van een gezichtsherkenningssoftware om toezicht te houden op de aanwezigheid van leerlingen. Hoewel de school haar verwerking gebaseerd had op de toestemming, oordeelde de Zweedse toezichthoudende autoriteit dat deze toestemming niet geldig was gezien de machtsverhouding tussen de verwerkingsverantwoordelijke en de betrokkenen.[18]

Daarnaast moet er bij de beoordeling of de toestemming vrijelijk is gegeven, onder meer rekening worden gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.[19] Artikel 7.4 AVG beoogt te waarborgen dat

[18] Zie: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_nl.

[19] Art. 7.4 AVG: " *Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst."* Zie ook overweging 43, AVG, die luidt: "[...] *De toestemming wordt geacht niet vrijelijk te zijn verleend indien*

het doel van de verwerking van persoonsgegevens niet wordt verhuld door de toestemming voor deze verwerking te koppelen aan de uitvoering van een overeenkomst waarvoor deze persoonsgegevens niet noodzakelijk zijn. Als zodanig verzekert de AVG dat de verwerking van persoonsgegevens waarvoor toestemming wordt gevraagd, niet direct of indirect de tegenprestatie voor een overeenkomst kan zijn. Dwang om in te stemmen met het gebruik van persoonsgegevens in aanvulling op hetgeen strikt noodzakelijk is voor de verwezenlijking van de doeleinden, beperkt immers de keuze van de betrokkene en staat vrije toestemming in de weg.

De bewijslast om aan te tonen dat er geen sprake is van een dergelijke conditionaliteit rust op de verwerkingsverantwoordelijke. Dit bewijs kan bijvoorbeeld worden geleverd door aan te tonen dat zijn organisatie de betrokkenen een echte keuze biedt tussen een dienst die een toestemming omvat voor het gebruik van persoonsgegevens voor aanvullende doeleinden enerzijds, en een gelijkwaardige dienst die aangeboden wordt door dezelfde verwerkingsverantwoordelijke die geen toestemming omvat voor het gebruik van gegevens voor aanvullende doeleinden anderzijds.[20]

In tweede instantie moet de toestemming specifiek zijn. Deze specificiteit heeft ingevolge artikel 6.1, a) AVG betrekking op het (de) doeleinde(n) van de verwerking. Deze eis beoogt te zorgen voor een zekere mate van controle en transparantie voor de betrokkene en is nauw verwant met de eis van 'geïnformeerde' toestemming.

Overeenkomstig artikel 5.1, b) AVG, wordt het verkrijgen van een rechtmatige toestemming altijd voorafgegaan door de vaststelling van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde voor de beoogde verwerkingsactiviteit (zie *infra* rubriek III. 2). "*De noodzaak van specifieke toestemming in combinatie met de notie van doelbinding (…) functioneert als een bescherming tegen de geleidelijke verbreding of vervaging van doeleinden waarvoor* (biometrische) *gegevens worden verwerkt nadat een betrokkene heeft ingestemd met de oorspronkelijke verzameling van de gegevens. Dit verschijnsel, ook wel 'function creep' genoemd, is een risico voor betrokkenen, omdat het kan leiden tot onvoorzien gebruik van persoonsgegevens door de verwerkingsverantwoordelijke of door derden*".[21] Zeker wanneer de verwerking slaat op bijzondere categorieën van gegevens, waaronder biometrische gegevens, is het pertinent om '*function creep*' uit te sluiten. De betrokkenen verlenen hun toestemming met het idee dat zij controle kunnen uitoefenen en dat hun gegevens uitsluitend worden verwerkt voor het (de) vermelde doeleinde(n). Indien een verwerkingsverantwoordelijke op basis van (expliciete) toestemming gegevens verwerkt, en de gegevens ook wil verwerken voor andere doeleinden, moet

geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering."

[20] EDPB-richtsnoeren 05/2020 *inzake toestemming overeenkomstig Verordening 2016/679*, p. 10-12 en zie eveneens Advies 06/2014 van de Groep 29 *over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG* (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_nl.pdf).

[21] EDPB-richtsnoeren 05/2020 *inzake toestemming overeenkomstig Verordening 2016/679*, punt 56.

deze verwerkingsverantwoordelijke vragen om een aanvullende toestemming voor die andere doeleinden, tenzij er een andere rechtsgrond is die beter toegesneden is op de situatie.

Ten derde eist de AVG dat de toestemming geïnformeerd moet zijn, wat inhoudt dat de persoon die zijn toestemming geeft perfect moet begrijpen waarvoor en waartoe hij zijn toestemming geeft. Transparantie is een van de fundamentele beginselen van de AVG, en is nauw verwant aan de beginselen van behoorlijkheid en rechtmatigheid. Het verstrekken van informatie aan betrokkenen voorafgaand aan het verkrijgen van hun toestemming is noodzakelijk om hen in staat te stellen om geïnformeerde beslissingen te nemen, te begrijpen waarmee ze instemmen en bijvoorbeeld hun recht tot intrekking van hun toestemming uit te oefenen. Indien de verwerkingsverantwoordelijke geen begrijpelijke informatie verstrekt, wordt de controle van de betrokkene slechts schijn en is de toestemming geen rechtmatige grond voor de verwerking.

Het volgt uit de richtsnoeren van de EDPB dat ten minste de volgende informatie nodig is voor het verkrijgen van rechtmatige toestemming:

- de identiteit van de verwerkingsverantwoordelijke;
- het doel van elk van de verwerkingen waarvoor toestemming wordt gevraagd;
- welk(e) (soort) gegevens worden verzameld en gebruikt;
- het bestaan van het recht om toestemming in te trekken;
- informatie over het gebruik van de gegevens voor geautomatiseerde besluitvorming overeenkomstig artikel 22.2, c) AVG, indien van toepassing;
- informatie over de risico's van een doorgifte van persoonsgegevens aan een derde land of een internationale organisatie bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen, zoals beschreven in de artikelen 45 en 46 AVG.

Deze informatie moet verstrekt worden in duidelijke en eenvoudige taal: een uitgebreide privacyverklaring in juridisch jargon is uit den boze.[22]

Bovendien moet het verzoek om toestemming afzonderlijk van alle andere verzoeken worden voorgelegd.

Een vierde en laatste voorwaarde is dat de toestemming ondubbelzinnig moet zijn. De AVG stelt uitdrukkelijk dat voor toestemming een verklaring of een ondubbelzinnige actieve handeling van de betrokkene is vereist. Er mag met andere woorden geen redelijke twijfel bestaan over de intentie van de betrokkene om toestemming te geven voor de voorgestelde verwerking van zijn of haar persoonsgegevens. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve

[22] Voor meer informatie zie *infra* rubriek III.6 en de Groep 29 richtsnoeren *inzake transparantie overeenkomstig Verordening (EU) 2016/679* (Te downloaden via: https://ec.europa.eu/newsroom/article29/items/622227.

niet als toestemming gelden. De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde of dezelfde doeleinde(n) dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend.[23]

De ondubbelzinnigheid van de toestemming houdt tevens in dat de betrokkenen de keuzemogelijkheden waarover ze beschikken duidelijk moeten kunnen begrijpen en, indien er meerdere keuzemogelijkheden zijn, moet de keuze om in te stemmen met de verwerking van hun biometrische gegevens duidelijk onderscheiden zijn van elke andere keuze.

UITDRUKKELIJKE TOESTEMMING

Uitdrukkelijke toestemming overeenkomstig artikel 9.2, a) AVG is vereist in bepaalde situaties waarin zich een ernstig risico voor de gegevensbescherming voordoet en waarbij derhalve een hoog niveau van individuele controle over persoonsgegevens passend wordt geacht.

De term 'uitdrukkelijk' verwijst naar de manier waarop de toestemming door de betrokkene tot uitdrukking wordt gebracht. Het betekent dat de betrokkene een uitdrukkelijke verklaring van toestemming moet opstellen. Een voor de hand liggende manier om ervoor te zorgen dat de toestemming uitdrukkelijk is, is het bevestigen van toestemming in een schriftelijke verklaring. In voorkomende gevallen zou de verwerkingsverantwoordelijke ervoor kunnen zorgen dat de schriftelijke verklaring door de betrokkene wordt ondertekend, om elke mogelijke twijfel weg te nemen en mogelijk gebrek aan bewijs in de toekomst uit te sluiten.

Een dergelijke ondertekende verklaring is echter niet de enige manier om een uitdrukkelijke toestemming te verkrijgen, en het is niet zo dat de AVG bepaalt dat in alle omstandigheden waarin geldige uitdrukkelijke toestemming nodig is, een schriftelijke en ondertekende verklaring vereist is. In de digitale of online context bijvoorbeeld kan een betrokkene de vereiste verklaring verstrekken door het invullen van een elektronisch formulier, door het versturen van een e-mail, door het uploaden van een gescand document waarop zijn handtekening staat, of door middel van een elektronische handtekening. In theorie kan het gebruik van mondelinge verklaringen ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen; het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het registreren van de verklaring voldaan werd aan alle voorwaarden voor een geldige uitdrukkelijke toestemming.

[23] Overweging 32 AVG.

Voorbeeld

Op 4 december 2019 heeft de Nederlandse toezichthoudende autoriteit (hierna "Autoriteit Persoonsgegevens") een administratieve boete van 725 000 EUR opgelegd aan een onderneming voor de onrechtmatige verwerking van de vingerafdrukken van haar werknemers. De Autoriteit Persoonsgegevens heeft daartoe vastgesteld dat de verwerkingsverantwoordelijke zich ten onrechte heeft beroepen op de uitdrukkelijke toestemming als uitzonderingsgrond. Medewerkers zijn immers afhankelijk van hun werkgever en als zodanig is er steeds sprake van een machtsverhouding dewelke een rechtsgeldige toestemming in de weg staat. Ter zijde en in secundaire orde oordeelde de Autoriteit Persoonsgegevens dat er hoe dan ook geen sprake was van een vrije, specifieke, geïnformeerde en uitdrukkelijke toestemming overeenkomstig artikel 4.11) AVG.

GELDIGE TOESTEMMING OVEREENKOMSTIG ARTIKEL 7 AVG

Zelfs wanneer er sprake is van een vrije, specifieke, geïnformeerde, ondubbelzinnige en uitdrukkelijke toestemming zal de verwerkingsverantwoordelijke bijkomstig de voorwaarden overeenkomstig artikel 7.1 en 7.3 AVG in acht moeten nemen.

Artikel 7.1 AVG[24] stelt dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Om aan deze eis te voldoen, staat het de verwerkingsverantwoordelijke vrij om te opteren voor de meest passende methode. Zodoende kan de verwerkingsverantwoordelijke, in het geval van een klacht van de betrokkene of bij een controle door de toezichthoudende autoriteit, op een eenvoudige manier aantonen dat hij gehandeld heeft in overeenstemming met de bepalingen van de AVG.

De verplichting om de toestemming te kunnen aantonen geldt zolang de verwerking plaatsvindt. Nadat die verwerking is afgelopen, mag het bewijs van de toestemming niet langer worden bewaard dan nodig is voor de naleving van deze wettelijke verplichting of voor de instelling, uitoefening of onderbouwing van een rechtsvordering, zoals voorzien in artikel 17.3, b) en e) van de AVG.

Daarnaast heeft de betrokkene overeenkomstig artikel 7.3 AVG het recht om zijn toestemming te allen tijde in te trekken. Vooraleer de betrokkene zijn toestemming geeft, moet hij in kennis worden gesteld van het feit dat hij zijn toestemming gratis en zonder nadelige gevolgen[25] (zoals bijvoorbeeld een vermindering van het tot dan toe geleverde niveau van dienstverlening, of zelfs de weigering daarvan) kan intrekken.

[24] Zie tevens overweging 42 AVG.
[25] Zie overweging 42 AVG.

Hoewel de AVG een prominente plaats toekent aan het intrekken van de toestemming, schrijft ze niet voor in welke vorm die intrekking moet of mag gebeuren. De EDPB stelt in dit verband: "*Wanneer toestemming echter wordt verkregen via elektronische middelen, door middel van slechts één muisklik, veeg of toetsenaanslag, moet de betrokkene deze toestemming, in de praktijk, ook even eenvoudig kunnen intrekken.*"[26] Betrokkenen verplichten om een complex pad te volgen via links naar onderliggende elektronische documenten of dat hen verplicht om een wachtwoord in te voeren, voldoet niet aan de eis dat de intrekking even eenvoudig moet kunnen plaatsvinden. Daarenboven moet de verwerkingsverantwoordelijke erop toezien dat de toestemming van een andere gebruiker niet kan worden ingetrokken zonder diens medeweten of toestemming.

Wanneer de toestemming wordt ingetrokken moeten alle verwerkingsactiviteiten die betrekking hebben op die persoon stopgezet worden. Zulks heeft evenwel geen invloed op de rechtmatigheid van de verwerking (op basis van die toestemming) vóór de intrekking ervan. Tevens zal de verwerkingsverantwoordelijke moeten nagaan of het bewaren van de gegevens die voor de betrokken verwerking werden aangewend al dan niet gerechtvaardigd is, zelfs indien de betrokkene geen verzoek tot verwijdering heeft ingediend. Immers, overeenkomstig artikel 5.1, e) AVG moet het bewaren van persoonsgegevens beperkt worden tot het nagestreefde doeleinde (zie *infra* rubriek III.5).

Slechts wanneer de gegevens van de betrokkene noodzakelijk zijn bij het uitvoeren van een verwerking voor andere doeleinden waarvoor tevens een geldige rechtsgrond bestaat, zullen de gegevens eventueel bewaard kunnen worden. Is dit niet het geval dan moeten ze verwijderd worden.

1.3.2 Zwaarwegend algemeen belang

Overeenkomstig artikel 9.2, g) AVG kunnen biometrische gegevens slechts verwerkt worden wanneer deze *verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.* Deze uitzonderingsgrond speelt een belangrijke rol met name wanneer – bijvoorbeeld door het bestaan van een machtsverhouding tussen de verwerkingsverantwoordelijke en de betrokkene – er geen beroep kan worden gedaan op de uitdrukkelijke toestemming overeenkomstig artikel 9.2, a) AVG. Dit impliceert inderdaad dat de uitdrukkelijke toestemming steeds de voorkeur geniet en dat een verwerkingsverantwoordelijke zich slechts in welbepaalde, door de wet gespecifieerde gevallen, zal kunnen beroepen op het zwaarwegend algemeen belang als rechtsgrond voor de verwerking van biometrische gegevens.

[26] EDPB-richtsnoeren 05/2020 *inzake toestemming overeenkomstig Verordening 2016/679*, p. 25.

Voorbeeld

De enige wet die op heden uitdrukkelijk voorziet in de verwerking van biometrische gegevens is de wet van 19 juli 1991 *betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten*, uitgevoerd bij het koninklijk besluit van 25 maart 2003 *betreffende de identiteitskaarten.*

In dit kader kan er op Europees niveau ook gewezen worden op de Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 *betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten*. Deze verordening voorziet tevens in de verwerking van een gezichtsopname en een vingerafdruk.

In tegenstelling tot een aantal van onze buurlanden, heeft de Belgische wetgever er niet voor gekozen om te voorzien in een algemene wettelijk grondslag die de verwerking van biometrische gegevens in het raam van de unieke identificatie of authenticatie van een persoon voor beveiligingsdoeleinden toelaat.

Voorbeeld

Artikel 29 UAVG, de Nederlandse uitvoeringswet van de AVG, bepaalt dat, gelet op artikel 9.2, g) AVG, het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing is, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Dit brengt evenwel met zich mee dat elke verwerking van biometrische gegevens in het raam van de authenticatie van personen, voor zover er geen beroep kan worden gedaan op de expliciete toestemming en met uitzondering van de verwerking van de biometrische gegevens in het kader van de eID (elektronische identiteitskaart) en het paspoort, op heden zonder rechtsgrond is. Immers, een verwerking steunen op redenen van algemeen zwaarwegend belang, zonder enige bepaling in het Unie- of lidstatelijk recht die daarin voorziet, lijkt onverenigbaar met de geest van artikel 9.2.g) AVG.

Om deze reden is de Autoriteit tevens van oordeel dat een algemeen geformuleerde verplichting in hoofde van de verwerkingsverantwoordelijke om 'afdoende veiligheidsmaatregelen te voorzien' niet kan worden geacht het gebruik van biometrische gegevens te verantwoorden. Hoewel de Autoriteit aanvaardt dat de verwerking van biometrische gegevens voor de identificatie of authenticatie van personen in bepaalde gevallen gerechtvaardigd kan zijn, zal er steeds moeten worden voorzien in een wettelijke bepaling (algemeen of sectoraal) die, gelet op artikel 9.2, g) AVG, de verwerking van biometrische gegevens in bepaalde gevallen mogelijk stelt. In die zin wil de Autoriteit benadrukken dat het loutere bestaan van een wettelijke bepaling geen vrijgeleide is voor de verwerking van biometrische

gegevens en dat zij de verwerkingsverantwoordelijke geenszins ontslaat van zijn verplichting om de noodzaak en de evenredigheid van de gegevensverwerking te onderbouwen. De verwerkingsverantwoordelijke zal met andere woorden moeten nagaan of de door hem nagestreefde doeleinden zodanig zijn dat het gebruik van biometrie **onvermijdelijk** is.

Voorbeeld

Op 12 augustus 2019 werd de schoenenwinkel Manfield door de rechtbank van Amsterdam veroordeeld voor het gebruik van een kassasysteem dat werkt op basis van een vingerscan. Manfield voerde aan dat zulks toegelaten was op grond van artikel 24 AVG *j°* artikel 9.2, g) AVG aangezien het gebruik van een vingerscanautorisatiesysteem noodzakelijk is voor het beveiligen van gevoelige informatie, te weten financiële informatie en persoonsgegevens van zowel werknemers als cliënteel. Daarnaast zou een dergelijk systeem verhinderen dat er gefraudeerd wordt met de kassa's. De rechter heeft deze argumenten verworpen en stelde dat het gebruik van biometrie voor authenticatie of beveiligingsdoeleinden slechts in uitzonderlijke gevallen de proportionaliteitstoets zal doorstaan. *In casu* had Manfield onvoldoende aangetoond dat er geen minder verregaande alternatieven voorhanden waren om dezelfde doelstellingen te bewerkstelligen.[27]

Altijd zal het vereist zijn om de behartigde (zwaarwegende) belangen te gaan afwegen tegen de risico's voor de rechten en vrijheden van de betrokkenen. Daartoe kan er bijvoorbeeld nagegaan worden op welke wijze de beoogde verwerking de maatschappij beïnvloedt, zowel in de 'diepte' (de omvang van het voor- of nadeel dat wordt ervaren door de verwerking) als in de 'breedte' (het aantal mensen dat een voor- of nadeel ervaart). Ter illustratie, in het bovenstaande voorbeeld is er sprake van een relatief groot nadeel (het verplicht afgeven van vingerafdrukken) voor een (verhoudingsgewijze) relatief grote groep betrokkenen (alle werknemers van de schoenenwinkel) dat niet in verhouding staat met het voordeel dat door slechts één persoon (de eigenaar van de winkel) wordt ervaren. Vergelijk dit met de situatie waar er gebruik wordt gemaakt van biometrische authenticatie teneinde toegang te verschaffen tot de lokalen van een kerncentrale. Het door de werknemers (verhoudingsgewijs een relatief kleine groep betrokkenen) ervaren nadeel weegt niet op tegen het voordeel dat wordt genoten door de hele bevolking (de beveiliging van cruciale infrastructuur).

Dit alles betekent concreet dat de Belgische wetgever, gelet op artikel 9.2, g) AVG, de modaliteiten van de verwerking van biometrische gegevens expliciet bij wet moet regelen in zoverre de wetgever een dergelijk gebruik van biometrische gegevens wil (blijven) toestaan. Daartoe kunnen de betrokken sectoren, organisaties of beroepsinstanties een gemotiveerde aanvraag indienen waaruit blijkt dat de verwerking proportioneel en noodzakelijk is in het kader van de beoogde doelstellingen, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en er passende en

[27] De volledige uitspraak is te raadplegen via de volgende link: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:6005.

specifieke maatregelen worden getroffen ter bescherming van de grondrechten en fundamentele belangen van de betrokkene. De Autoriteit benadrukt dat wetgevende initiatieven in dit kader, overeenkomstig artikel 23 van de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, steeds ter advies moeten worden voorgelegd aan het Kenniscentrum van de Autoriteit. Daarbij zal er worden nagegaan of de wettelijke bepaling in overeenstemming is met de AVG, en meer bepaald of de beoogde verwerking inderdaad noodzakelijk is om redenen van zwaarwegend algemeen belang.

Deze nieuwe vereisten geven aanleiding tot een breuk met het regime vóór de inwerkingtreding van de AVG. Daarom, rekening houdend met de beginselen van behoorlijk bestuur, wordt er met ingang van de publicatie van deze aanbeveling voorzien in een overgangsperiode van één jaar gedurende dewelke de verwerking van biometrische gegevens overeenkomstig de oude norm gedoogd zal worden en er door de Autoriteit niet proactief zal worden opgetreden. Deze periode van één jaar moet de verwerkingsverantwoordelijken en de wetgever in staat te stellen om te voorzien in een wettelijke basis teneinde de geviseerde verwerkingen in overeenstemming te brengen met de bepalingen van de AVG zoals toegelicht in deze aanbeveling.

1.3.3 De huishoudelijke exceptie

Een zeer specifieke, evenwel alomtegenwoordige toepassing van het gebruik van biometrische gegevens speelt zich af in het kader van de persoonlijke authenticatie via smartphones en andere elektronische toestellen waar gezichtsherkenningssoftware en vingerafdruksensors steeds vaker optreden als alternatief voor de traditionele pincode. Gezien het belang in de praktijk van dergelijke toepassingen en de ambiguïteit die er vaak mee gepaard gaat verdient dit onderwerp enige toelichting.

De Autoriteit merkt op dat er een onderscheid moet worden gemaakt tussen, enerzijds, biometrische gegevens die op het apparaat zelf zijn opgeslagen en, anderzijds, biometrische gegevens die op andere locaties zijn opgeslagen. De impact van dit onderscheid is aanzienlijk, want voor de eerste categorie kan de huishoudelijke exceptie overeenkomstig artikel 2.2, c) AVG van toepassing zijn. Wanneer de biometrische gegevens evenwel niet (enkel) op het apparaat worden bewaard, of wanneer zij tevens worden meegedeeld aan derden, is dit niet het geval en zal de verwerkingsverantwoordelijke aldus moeten aantonen dat een van de uitzonderingsgronden opgesomd in artikel 9.2 AVG voorhanden is.

Artikel 2.2, c) AVG bepaalt dat de verordening niet van toepassing is "*op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit*". Wanneer de biometrische gegevens (lees: de aangemaakte templates die authenticatie via gezichtsherkenning of een vingerafdruk mogelijk maken) exclusief op het apparaat worden bewaard, heeft dit tot gevolg dat het biometrische authenticatieproces lokaal en autonoom kan

plaatsvinden zonder externe toegang. Een gegevensverwerking in die zin – geïnitieerd door de betrokkene en gerealiseerd onder zijn controle – kan onder bepaalde voorwaarden onder de huishoudelijke exceptie vallen, wat inhoudt dat de regels van de AVG niet van toepassing zijn.[28]

Vooraleer zich te kunnen beroepen op de huishoudelijke exceptie zal de aanbieder van een bepaald apparaat, of een bepaalde dienst evenwel moeten aantonen dat aan de volgende vijf voorwaarden is voldaan:

- de betrokkene gebruikt dit apparaat privé – zijn biometrische gegevens kunnen slechts door hemzelf gebruikt worden om het apparaat te ontgrendelen of om toegang te krijgen tot applicaties die hij zelf heeft gedownload;
- het is de betrokkene die zelfstandig besluit om gebruik te maken van de mogelijkheid tot biometrische authenticatie die in zijn apparaat is geïntegreerd. Dit impliceert dat:
    - werkgevers die biometrische authenticatieprocedures opleggen aan hun werknemers, bijvoorbeeld via apparaten die worden verstrekt in het kader van hun professionele activiteit, zich niet kunnen beroepen op de huishoudelijke exceptie;
    - de aanbieders van een bepaald apparaat, of van een bepaalde dienst, steeds, zonder enige beperking, moeten voorzien in een alternatief voor biometrische authenticatie (zoals bijvoorbeeld het gebruik van een traditionele pincode). Is zulks niet het geval, dan wordt de desbetreffende aanbieder onverkort aangemerkt als verwerkingsverantwoordelijke overeenkomstig artikel 4.7) AVG ten aanzien van de verwerkte biometrische gegevens;
- de biometrische template moet, nadat deze door de betrokkene werd aangemaakt, opgeslagen worden op het apparaat, in een gepartitioneerde omgeving die een hoog niveau van beveiliging biedt tegen de verzending van informatie vanuit deze omgeving. Wanneer de template aldus opgeslagen wordt buiten het apparaat, of indien de template toegankelijk is voor derden (bijvoorbeeld de aanbieder van het apparaat of de dienst of de ontwikkelaar van een applicatie) kan er geen sprake zijn van de huishoudelijke exceptie;
- de biometrische template dient te worden versleuteld overeenkomstig de stand van de techniek;
- de enige informatie die tijdens de toegangscontrole mag worden meegedeeld, is of de biometrische authenticatie is geslaagd of mislukt.

In zoverre er aan de bovengenoemde voorwaarden is voldaan zal de aanbieder van het apparaat of van de dienst niet verantwoordelijk worden gehouden voor de desbetreffende verwerking van biometrische gegevens. Desalniettemin heeft de toepasbaarheid van de exceptie in deze context geenszins tot gevolg dat de aanbieder zonder meer vrijgesteld wordt van al zijn verplichtingen onder de AVG. Logischerwijze blijft de aanbieder verantwoordelijk voor de verwerking van persoonsgegevens die plaatsvindt via zijn apparaat of dienst. Aangezien de toegang tot het apparaat of de dienst desgevallend

[28] Deze zienswijze wordt gedeeld door de Franse gegevensbeschermingsautoriteit (CNIL), zie: https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees.

gebeurt via biometrische authenticatie is de beveiliging van de betrokken applicatie van het allergrootste belang. Als zodanig zal de aanbieder de betrouwbaarheid van zijn biometrische authenticatietechnologieën moeten aantonen door, onder andere, te verzekeren dat:

- het percentage van vals-positieve[29]/ vals-negatieve[30] resultaten aangepast is aan het vereiste beveiligingsniveau van een bepaalde dienst (bijvoorbeeld, voor wat betreft bijzonder gevoelige toepassingen, zoals toegang tot een smartphone, bankgegevens of versleutelde documenten, zal er een laag percentage vals-positieve resultaten aangetoond moeten worden);
- de biometrische technologieën minstens bestand zijn tegen aanvallen die overeenkomstig de stand der techniek als triviaal moeten worden beschouwd (bijvoorbeeld het gebruik van een foto teneinde gezichtsherkenningssoft-, hardware te misleiden);
- het aantal toegestane biometrische authenticatiepogingen is beperkt (bijvoorbeeld na drie mislukte pogingen zal de betrokkene slechts toegang kunnen krijgen tot de applicatie door een pincode in te geven).

Het spreekt voor zich dat indien er niet werd voldaan aan de vijf bovenstaande voorwaarden, of indien de veiligheid van het betrokken biometrische authenticatiesysteem niet kan worden aangetoond, de verwerking van biometrische gegevens zonder meer onder het toepassingsgebied van de AVG zal vallen.

2. Doelbinding[31]

Het principe van doelbinding is neergelegd in artikel 5.1, b) AVG en bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en dat ze vervolgens niet verder op een met een van die doeleinden onverenigbare wijze mogen worden verwerkt.

Twee bouwstenen dienen te worden onderscheiden: (1) het specifiëren van (een) welbepaald(e), uitdrukkelijk omschreven en gerechtvaardigd(e) doeleinde(n) voor de beoogde verwerking en (2) een element van compatibiliteit hetwelk inhoudt dat verdere verwerking enkel toegestaan is voor zover zulks niet onverenigbaar is met het (de) doeleinde(n) waarvoor de gegevens oorspronkelijk werden verzameld. Aangezien het gekozen het (de) doeleinde(n) in belangrijke mate mee zal (zullen) bepalen op welke rechtsgrond voor de verwerking er zal moeten worden gesteund, spreekt het voor zich dat het (de) doeleinde(n) bepaald moet(en) zijn vóór de verwerking kan aanvangen.[32]

[29] Een situatie waarbij er onterecht toegang wordt verleend tot het apparaat of de dienst.
[30] Een situatie waarbij de toegang tot het apparaat of de dienst onterecht wordt geweigerd.
[31] Voor een uitgebreide uiteenzetting ter zake zie: Groep 29, '*Opinion 03/2013 on purpose limitation*', te raadplegen via: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (enkel beschikbaar in het Engels).
[32] Zulks blijkt onder meer uit de verplichting van de 'geïnformeerde' toestemming (zie *supra*) en zie ook art. 6.1, a) AVG.

Persoonsgegevens kunnen alleen verwerkt worden voor reële of bestaande doeleinden, of voor doeleinden die, in het licht van de werkelijke activiteit van de verwerkingsverantwoordelijke, realiseerbaar zijn in de nabije toekomst.

2.1 Initië(e)l(e) doeleinde(n)

Een verwerkingsverantwoordelijke moet voor elke gegevensverwerking die hij beoogt het (de) doeleinde(n) bepalen. Dit wil zeggen dat er vastgelegd dient te worden wat hij concreet wil bereiken door het gebruik van bepaalde persoonsgegevens.

Deze bepaling van de verwerkingsdoeleinden is essentieel voor de verplichte proportionaliteitstoets aangaande de verwerking (teneinde te verzekeren dat de verwerkte gegevens, en de concrete verwerking ervan evenredig zijn met de nagestreefde doeleinden). Deze verwerkingsdoeleinden moeten duidelijk afgebakend worden en stellen de verwerkingsverantwoordelijke in staat om de meest passende verwerkingsactiviteiten te kiezen. Met andere woorden, de loutere vaststelling van een doeleinde, net zomin als bijvoorbeeld het identificeren van een zwaarwegend belang, heeft niet automatisch tot gevolg dat de beoogde verwerking van biometrische gegevens gerechtvaardigd is.

Hieronder enkele voorbeelden van doeleinden voor de verwerking van biometrische gegevens:

- Authenticatie van personen voor beveiligingsdoeleinden;
- Authenticatie van personen in het kader van betalingen, of voor toegang tot private apparaten of applicaties;
- Tijdsregistratie in een werk-gerelateerde context;
- Direct marketing[33];
- Screening (a.d.h.v. gezichtsherkennings- of individualiseringssoftware) van openbare plaatsen in het kader van misdaadpreventie[34];
- DNA-onderzoek binnen de medisch sector;
- Commercieel DNA-onderzoek met het oogmerk het etnisch erfgoed en/of de genetische specificiteit van een persoon vast te stellen[35].

[33] Direct marketing *an sich* als doeleinde is bijzonder ruim en dient zonder meer gespecifieerd te worden in elk concreet geval. Daar dit evenwel buiten de scope van deze aanbeveling zou vallen verwijst de Autoriteit ter zake naar de aanbeveling nr. 01/2020 *betreffende de verwerking van persoonsgegevens voor direct marketingdoeleinden* (te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2020.pdf).

[34] De verwerkingen van biometrische gegevens die in dit kader plaatsvinden zullen evenwel slechts zelden onder het toepassingsgebied van de AVG vallen daar zij gebruikelijk uitgevoerd worden door politie- en/of inlichtingendiensten.

[35] Privaat DNA-onderzoek is geëvolueerd tot een miljardenindustrie. Ondanks het verbod ervan in Frankrijk (zie: https://www.statnews.com/2019/11/14/france-consumer-genetic-testing-ban/) wordt er in de Europese Unie op heden gewerkt aan een ethisch framework en richtlijnen inzake het gebruik van private testkits en de advertising ervan (project SIENNA, zie: https://www.sienna-project.eu/).

Eens de doeleinden werden vastgesteld moeten ze nauwkeurig worden ingeschreven in het register van de verwerkingsactiviteiten (zie *supra* rubriek II.1.2) alsook in het document dat gebruikt wordt om de vereiste informatie te verstrekken aan de betrokkenen (de nauwkeurige mededeling van de verwerkingsdoeleinden is immers van essentieel belang om te kunnen voldoen aan de transparantieverplichting overeenkomstig de artikelen 13 en 14 AVG waaruit volgt dat de betrokkenen geïnformeerd dienen te worden over de verwerkingsdoeleinden).

2.2 Verder(e) doeleinde(n)

De tweede verplichting die voortvloeit uit artikel 5.1.b) AVG houdt in dat de persoonsgegevens die voor een welbepaald en uitdrukkelijke doeleinde werden verzameld en verwerkt, niet verder verwerkt mogen worden op een met dat doeleinde onverenigbare wijze. Dit betekent dat er voor elk nieuw doeleinde dat niet compatibel is met het oorspronkelijke doeleinde een eigen rechtsgrond geïdentificeerd moet worden.

Overweging 50 AVG bepaalt ter zake dat: "*Om na te gaan of een doel van verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, moet de verwerkingsverantwoordelijke, nadat hij aan alle voorschriften inzake rechtmatigheid van de oorspronkelijke verwerking heeft voldaan, onder meer rekening houden met: een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking; het kader waarin de gegevens zijn verzameld; met name de redelijke verwachtingen van de betrokkenen op basis van hun verhouding met de verwerkingsverantwoordelijke betreffende het verdere gebruik ervan; de aard van de persoonsgegevens; de gevolgen van de voorgenomen verdere verwerking voor de betrokkenen; en passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerkingen.*"

Dit onderzoek naar verenigbaarheid moet uitgevoerd worden door de eerste verwerkingsverantwoordelijke, zowel voor zijn verwerkingsactiviteiten als de verwerkingsactiviteiten die worden beoogd door derden, verwerkingsverantwoordelijken, aan wie de oorspronkelijke verwerkingsverantwoordelijke van plan is de gegevens door te geven. Een dergelijke situatie kan zich bijvoorbeeld voordoen wanneer een werkgever, die gebruik maakt van gezichtsherkenningssoftware voor de toegang tot zijn lokalen, de biometrische gegevens die daartoe verwerkt worden doorgeeft aan de ontwikkelaar van de betrokken software die ze op zijn beurt gebruikt voor de verbetering van zijn technologieën of wanneer de aanbieder van commerciële DNA-tests de resultaten van de betrokkenen tevens zou aanwenden voor genetisch of etnografisch onderzoek.

Gezien de bijzonder strenge voorwaarden die gelden ten aanzien van de verwerking van biometrische gegevens zal het in de praktijk evenwel zeer moeilijk blijken om een dergelijke compatibiliteit te gaan

aantonen. De verdere verwerking van biometrische gegevens zal dus quasi altijd moeten steunen op een eigen, specifieke rechtsgrond.

Wanneer de verdere verwerking toch verenigbaar zou zijn met het (de) oorspronkelijke doel(einden) specifieert artikel 13.3 AVG dat: "*Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2*."

3. Proportionaliteit

Proportionaliteit, zonder evenwel expliciet genoemd te worden in de tekst van de AVG, is een van de kernbeginselen van het Europese (gegevensbeschermings)recht. De verplichte proportionaliteitstoetsing blijkt indirect uit artikel 5.1, a) (behoorlijkheid) en c) (minimale gegevensverwerking) AVG en impliceert evenredigheid bij het afwegen van de respectieve belangen van enerzijds de verwerkingsverantwoordelijke en, anderzijds, de betrokkenen. Daartoe moet de verwerkingsverantwoordelijke zich steeds afvragen of de door hem beoogde verwerkingsactiviteiten (1) geschikt (is de maatregel relevant voor het realiseren van de doeleinden?), (2) noodzakelijk (is de maatregel nodig voor het realiseren van de doeleinden?) en, (3) niet-excessief (gaat de maatregel verder dan wat noodzakelijk is voor het realiseren van de doeleinden?) zijn.

Meer concreet schuilt de verplichte proportionaliteitstoetsing in het nakomen van de verplichtingen die worden opgelegd door de AVG. Slechts wanneer de verwerkingsverantwoordelijke op afdoende wijze kan aantonen dat alle beginselen van de gegevensbescherming werden gerespecteerd kan er sprake zijn van een rechtmatige en aldus proportionele gegevensverwerking. Denk bijvoorbeeld aan de identificatie van een passende rechtsgrond, het duidelijk omschrijven van de doeleinden, het verzekeren dat er niet meer gegevens verwerkt worden dan noodzakelijk voor deze doeleinden, de keuze van de specifieke verwerkingsactiviteiten, het nakomen van de transparantieverplichting, ervoor zorgen dat de gegevens niet langer verwerkt en bewaard worden dan nodig is, de garantie van de integriteit van de gegevensverwerking, het in acht nemen van de principes van '*privacy by design*' en '*privacy by default*', …

In het bijzonder voor wat betreft de verwerking van biometrische gegevens speelt de notie proportionaliteit een belangrijke rol. Immers, overeenkomstig artikel 5.1, c) AVG moeten persoonsgegevens toereikend zijn, ter zake dienend en beperkt worden tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De verwerking van persoonsgegevens mag aldus slechts plaatsvinden voor zover het doel van de verwerking redelijkerwijze niet op een andere manier kan worden bereikt. In de context van de verwerking van biometrische gegevens betekent dit dat zelfs

indien er een rechtsgrond werd geïdentificeerd en de doeleinden duidelijk zijn omschreven de verwerking niet zonder meer kan plaatsvinden. Er moet immers worden nagegaan of er geen minder verregaande (de verwerking van biometrische gegevens zal steeds de laatste remedie zijn) oplossingen zijn.

Voorbeeld

In augustus 2019 kondigde de Gentse school Sint-Bavo aan dat leerlingen en personeelsleden in de nabije toekomst voor allerhande zaken (cafetaria, kopieermachines,…) zouden kunnen betalen via een handpalmscan. De school steunde zich daarvoor op de uitdrukkelijke toestemming van de ouders en de leerlingen en beoogde de afschaffing van papieren maaltijdbonnetjes en cash geld (mede om te vermijden dat kinderen met teveel geld op zak moeten rondlopen). Degenen die weigerden zouden gebruik kunnen maken van alternatieve betaalmethodes. Naar aanleiding evenwel van een negatief advies werd alsnog afgestapt van het idee aangezien er een duidelijk onevenwicht bestaat tussen de risicovolle verwerking van biometrische gegevens en het betalen van kleine bedragen in een schoolcontext. *In casu* kan er geoordeeld worden dat hoewel de maatregel geschikt is voor het bereiken van de beoogde doeleinden, er onvoldoende werd aangetoond dat zij effectief noodzakelijk is en dat er geen mindere verdergaande oplossingen zijn.[36]

In het geval dat de verwerkingsverantwoordelijke kan aantonen dat de verwerking van biometrische gegevens het meest geschikte middel is om de veiligheid te waarborgen, zal hij tevens het gebruik van een bepaald biometrisch kenmerk moeten documenteren en verantwoorden. In het bijzonder voor wat betreft de biometrische authenticatie van personen, benadrukt de Autoriteit dat de verwerkingsverantwoordelijke zich moet beperken tot authenticatie op basis van morfologische kenmerken van de betrokkenen (bijvoorbeeld gezichtsherkenning, handpalm- of vingerafdrukscans, irisherkenning), ermee rekening houdend evenwel dat het gebruik van biometrische systemen op basis van morfologische kenmerken die geen sporen achterlaten (bijvoorbeeld gezichts- of irisherkenning) minder risico's inhoudt voor de betrokkenen dan het gebruik van bijvoorbeeld vingerafdruk- of handpalmscans. Voor wat betreft de verwerking van biologische monsters (bijvoorbeeld speeksel, urine of bloed) zullen steeds de strengste voorwaarden gelden.[37]

Ook de wijze van opslag van het biometrische template in het kader van authenticatie van personen (zie *supra* rubriek II.2.3) speelt een belangrijke rol in het kader van de proportionaliteitstoets. Immers, zoals hierboven reeds werd toegelicht zal de opslag van templates onder gedeeld beheer, of onder het exclusieve beheer van de verwerkingsverantwoordelijke slechts in uitzonderlijke gevallen mogelijk zijn.

[36] Zie o.a.: https://tweakers.net/nieuws/156660/belgische-school-laat-leerlingen-hun-lunch-afrekenen-met-scan-van-handpalm.html en https://www.nieuwsblad.be/cnt/dmf20190911_04603325.
[37] De verwerking van biologisch monsters speelt zich voornamelijk af in medische sector of in het kader van commercieel aangeboden DNA-tests.

De opslag van de template onder het exclusieve beheer van de betrokkene (bijvoorbeeld in een token of badge) blijft gelden als de principiële regel.

Tot slot, indien de authenticatie absoluut moet gebeuren aan de hand van een biometrisch systeem, dient het gebruik hiervan steeds beperkt te worden tot de ruimten/diensten die dergelijke bijzondere maatregelen rechtvaardigen. Wat bijvoorbeeld de toegangscontrole betreft, kan een site bepaalde ruimten omvatten die vrij toegankelijk zijn en andere die het gebruik van de biometrie rechtvaardigen. De toegang aan de hand van biometrische systemen moet als zodanig beperkt worden tot deze ruimten en de verwerkte biometrische gegevens moeten beperkt blijven tot de personen die gemachtigd zijn om deze ruimten te betreden. Om de toegang tot een ruimte te beperken tot een bepaalde groep individuen is het daarenboven niet steeds noodzakelijk om gegevens te verwerken die een directe identificatie toelaten (zoals de naam) van de personen die beschikken over een recht op toegang. Zolang een persoon dus beschikt over een recht op toegang en de biometrie toelaat dit te controleren is het onnodig de biometrische informatie te koppelen aan bijkomende identificatiemiddelen.

4. Beveiliging van de verwerking

Overeenkomstig artikel 5.1, f) *jº* artikel 32 AVG treft elke verwerkingsverantwoordelijke, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Zulke maatregelen kunnen onder meer omvatten:

a. Maatregelen betreffende de biometrische gegevens[38]:

- de biometrische gegevens, inclusief de templates, versleutelen aan de hand van een cryptografisch algoritme overeenkomstig de stand der techniek;
- een integriteitscode koppelen aan de biometrische gegevens (bijvoorbeeld met een elektronische handtekening);
- fraudeopsporingsmaatregelen integreren;
- de externe toegang tot de biometrische gegevens verbieden;
- ervoor zorgen dat de kopie van de gegevens die worden verzameld tijdens de tweede inzamelingsfase niet langer wordt bewaard dan de tijd die nodig is om de ingezamelde gegevens te vergelijken met de referentie-informatie;
- het implementeren van een doeltreffend systeem voor de verwijdering en vernietiging van de biometrische gegevens na afloop van de bewaartermijn;

[38] Inzake de biometrische authenticatie van personen werd in die zin reeds gespecifieerd dat het op heden niet verantwoordbaar zal zijn om te werken met een systeem waar de referentie-informatie in haar onbewerkte vorm wordt opgeslagen (verplichting om te werken aan de hand van biometrische templates) en dat de verificatiefunctie de voorkeur geniet boven de identificatiefunctie daar het bij deze laatste steeds noodzakelijk zal zijn om de referentie-informatie in een centrale databank op te slaan (zie *supra* rubriek II.2.3).

b. Organisatorische maatregelen:

- het duidelijk afbakenen en opleiden van de personen binnen een onderneming die toegang hebben tot de biometrische systemen/gegevens;
- het responsabiliseren van de betrokkenen inzake het gebruik en de toepassing van biometrische systemen;
- het kosteloos ter beschikking stellen van alternatieve authenticatieprocedures voor personen bij wie de registratie of de lezing van de biometrische gegevens ingevolgde een handicap of een andere omstandigheid onmogelijk is of ernstig wordt bemoeilijkt;
- de veiligheid, betrouwbaarheid en veerkracht van het systeem testen vóór de implementatie, en ná elke wijziging;
- het vaststellen van een back-upsysteem en herstelprocedures in het geval van systeemstoring;
- het vaststellen van een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de genomen maatregelen ter beveiliging van de verwerking;

c. Maatregelen inzake de apparatuur en software:

- het up-to-date houden van de biometrische systemen teneinde deze te beschermen tegen ongeoorloofde toegang en/of vals negatieve/positieve resultaten te verminderen (zulks houdt tevens in dat het de verantwoordelijkheid is van de verwerkingsverantwoordelijke om na te gaan dat de door de ontwikkelaar van de hard- of software aangebrachte wijzigingen de beveiliging van het systeem niet in het gedrang brengen);
- voorzien in een waarschuwingsprocedure, of de automatische verwijdering van de gegevens ingeval het systeem een (poging tot) ongeoorloofde toegang vaststelt;
- ervoor zorgen dat de biometrische gegevens afzonderlijk worden opgeslagen en dat de uitvoeringsomgeving van de biometrische applicatie afgescheiden is van de overige netwerken.

In dit kader moet eveneens verwezen worden naar artikel 25 AVG betreffende de gegevensbescherming door ontwerp (‘*privacy by design*’) en door standaardinstellingen (‘*privacy by default*’).

Privacy by design wil concreet beteken dat de beginselen inzake gegevensbescherming overeenkomstig artikel 5 AVG reeds worden geïntegreerd in het gegevensverwerkingsproces vóór de aanvang van de verwerkingsactiviteiten.[39] *Privacy by design* moet met andere woorden opgevat worden als de benadering waarbij deze kernbeginselen toegepast worden als fundamentele ontwerpprincipes doorheen het gehele systeemontwikkelingsproces zodanig dat de risico’s voor de betrokkenen geminimaliseerd worden van bij het begin. Zodoende dienen de producenten van biometrische systemen te worden gestimuleerd om bij de ontwikkeling en uitwerking ervan rekening te houden met het recht op bescherming van persoonsgegevens en, met inachtneming van de stand der techniek, erop

[39] De Europese Toezichthouder voor gegevensbescherming (dikwijls aangeduid met de Engels afkorting “EDPS”) definieert ‘*privacy by design*’ als volgt: *“privacy and data protection by design aims at building privacy and data protection into the design specifications and architecture of information and communication systems.”* Zie EDPS, Opinion 7/2015 on the challenges of big data, p. 14 (te raadplegen via: https://edps.europa.eu/data-protection/our-work/publications/opinions/meeting-challenges-big-data_en.

toe te zien dat de verwerkingsverantwoordelijken in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.[40]

Privacy by default houdt in dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft om ervoor te zorgen dat alleen de persoonsgegevens worden verwerkt die noodzakelijk zijn voor de gespecifieerde doeleinden. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan en beoogt de onrechtmatige, onverwachte of onredelijke verwerking van gegevens te voorkomen.

Het is in deze context onontbeerlijk dat de verwerkingsverantwoordelijke de technologische evoluties ter zake nauwgezet opvolgt teneinde de veiligheidsmaatregelen hierop af te stemmen. De Autoriteit wil er dan ook op wijzen dat de verwerkingsverantwoordelijke op grond van artikel 5.2 AVG verantwoordelijk is, en aldus aansprakelijk kan worden gesteld voor de schade die zou te wijten zijn aan de niet-naleving van de veiligheidsmaatregelen.[41]

5. Opslagbeperking

Overeenkomstig artikel 5. 1. e) AVG moeten persoonsgegevens "*worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is*". Concreet wil dit zeggen dat eens het doeleinde van de verwerking is vervuld, of wanneer de rechtsgrond vervalt (bijvoorbeeld door de intrekking van de toestemming door de betrokkenen, of het wegvallen van het zwaarwegend algemeen belang), de betrokken biometrische gegevens verwijderd moeten worden[42]. Dit sluit evenwel niet uit dat de gegevens langer worden bewaard ingevolge een wettelijke verplichting of wanneer deze gegevens noodzakelijk zijn in het kader van een rechtsvordering.

Wanneer de verwerking van biometrische gegevens plaatsvindt op grond van een wettelijke verplichting in hoofde van de verwerkingsverantwoordelijke moet de in de wet opgenomen bewaartermijn worden gerespecteerd.

Aangaande de biometrische authenticatie, zoals reeds toegelicht onder rubriek II.2.3, wenst de Autoriteit erop te wijzen dat de ruwe biometrische gegevens die worden verzameld in het kader van de eerste inzamelingsfase van een biometrisch systeem (registratiefase) onmiddellijk verwijderd moeten worden van zodra de biometrische template werd aangemaakt. Daarnaast mogen de gegevens die

[40] Zie overweging 78 AVG.
[41] Zie overweging 74 AVG.
[42] Zo moeten bijvoorbeeld de gegevens die werden gebruikt om de toegang tot een arbeidsplaats te beheren, verwijderd worden zodra de gebruiker zijn toegangsrecht tot die ruimte verliest.

worden verzameld tijdens de tweede inzamelingsfase niet langer worden bewaard dan de tijd die nodig is om de ingezamelde gegevens te vergelijken met de referentie-informatie.

6. Transparantieverplichting[43]

Overweging 38 AVG bepaalt dat: "*Overeenkomstig het transparantiebeginsel moet informatie en communicatie in verband met de verwerking van persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt. Dat beginsel betreft met name het informeren van de betrokkenen over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de natuurlijke personen in kwestie en hun recht om bevestiging en mededeling te krijgen van hun persoonsgegevens die worden verwerkt. Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot deze verwerking kunnen uitoefenen. Meer bepaald dienen de specifieke doeleinden waarvoor de persoonsgegevens worden verwerkt, expliciet en gerechtvaardigd te zijn en te zijn vastgesteld wanneer de persoonsgegevens worden verzameld.*"[44]

De belangrijkste artikelen van de AVG die betrekking hebben op transparantie, omdat ze van toepassing zijn op de rechten van betrokkenen, zijn te vinden in hoofdstuk III (Rechten van de betrokkene). Artikel 12 AVG bevat de algemene voorschriften die van toepassing zijn op: de verstrekking van informatie aan betrokkenen (artikelen 13 – 14 AVG), de communicatie met betrokkenen over de uitoefening van hun rechten (artikelen 15 – 22 AVG) en de communicatie over inbreuken in verband met persoonsgegevens (artikel 34 AVG).

Het spreekt voor zich dat ook voor wat de betreft de verwerking van persoonsgegevens de verplichtingen inzake transparantie nauwgezet nageleefd moeten worden.

7. Gegevensbeschermingseffectbeoordeling

Overeenkomstig artikel 35.1 AVG zal de verwerkingsverantwoordelijke vóór de verwerking een beoordeling moeten uitvoeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens wanneer de verwerking, in het bijzonder wanneer er nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

[43] Voor een omvattende uiteenzetting inzake het transparantiebeginsel zie Groep 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679.* Te downloaden via: https://ec.europa.eu/newsroom/article29/items/622227.
[44] Overweging 38 AVG.

Artikel 35.4 AVG bepaalt bijkomstig dat elke toezichthoudende autoriteit een lijst dient op te stellen en te publiceren met de verwerkingsactiviteiten waarvoor een gegevensbeschermingseffectbeoordeling is vereist. In afwachting van de oprichting van de Autoriteit heeft de Commissie voor de bescherming van de persoonlijke levenssfeer de aanbeveling nr. 01/2018 aangenomen inzake de modaliteiten van het uitvoeren van een gegevensbeschermingseffectbeoordeling, hierbij rekening houdend met de bepalingen van artikel 35 AVG en de richtlijnen van de Groep 29. Deze aanbeveling werd vervolgens aangevuld door de beslissing nr. 01/2019[45] van het Algemeen Secretariaat van de Autoriteit dewelke een lijst bevat van de verwerkingsactiviteiten waarvoor een gegevensbeschermingseffectbeoordeling is vereist.

Zoals blijkt uit punt 6 van de beslissing nr. 01/2019 zal er steeds een gegevensbeschermingseffectbeoordeling uitgevoerd moeten worden wanneer de verwerking gebruik maakt van biometrische gegevens met het oog op de unieke identificatie van betrokkenen die zich in een openbare ruimte bevinden of in privéruimten die toegankelijk zijn voor het publiek. De Autoriteit wil evenwel benadrukken dat ook de verwerking van biometrische gegevens voor andere doeleinden dan deze die uitdrukkelijk opgenomen zijn in de beslissing desgevallend onderworpen is aan de verplichting van het uitvoeren van een gegevensbeschermingseffectbeoordeling. Sterker nog, gezien het hoge inherente risico voor de rechten en vrijheden van de betrokkenen die de verwerking van biometrische gegevens impliceert, zal het nalaten een gegevensbeschermingseffectbeoordeling uit te voeren slechts in uitzonderlijke gevallen gerechtvaardigd zijn.

Ter zake, voor wat betreft de modaliteiten inzake de uitvoering van een gegevensbeschermingseffectbeoordeling, verwijst de Autoriteit naar de aanbeveling nr. 01/2018[46], de beslissing nr. 01/2019 en de handleiding GEB[47].

[45] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-nr.-01-2019-van-16-januari-2019.pdf.
[46] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2018.pdf.
[47] Te raadplegen via: https://www.gegevensbeschermingsautoriteit.be/publications/handleiding-gegevensbeschermingseffectbeoordeling.pdf.