AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
[VERTROUWELIJK]

Datum
4 december 2019

Ons kenmerk
[VERTROUWELIJK]

Contactpersoon
[VERTROUWELIJK]

Onderwerp
Besluit tot het opleggen van een bestuurlijke boete

Geachte [VERTROUWELIJK],

De Autoriteit Persoonsgegevens (AP) heeft besloten aan [VERTROUWELIJK] een **bestuurlijke boete** van **€725.000,-** op te leggen. De AP is van oordeel dat [VERTROUWELIJK] van 25 mei 2018 tot en met 16 april 2019 het verbod van artikel 9, eerste lid, van de Algemene Verordening Gegevensbescherming heeft overtreden door biometrische gegevens van haar werknemers te verwerken.

Hierna wordt het besluit nader toegelicht. Hoofdstuk 1 betreft een inleiding en hoofdstuk 2 beschrijft het wettelijk kader. In hoofdstuk 3 beoordeelt de AP of er sprake is van verwerking van biometrische gegevens, verwerkingsverantwoordelijkheid en de overtreding. In hoofdstuk 4 wordt de (hoogte van de) bestuurlijke boete uitgewerkt en hoofdstuk 5 bevat het dictum en de rechtsmiddelenclausule.

Datum
4 december 2019

Ons kenmerk
[VERTROUWELIJK]

1. Inleiding

1.1 Betrokken rechtspersonen en aanleiding onderzoek

[VERTROUWELIJK] is een bedrijf dat statutair gevestigd is op [VERTROUWELIJK]. [VERTROUWELIJK] is ingeschreven in het handelsregister van de Kamer van Koophandel onder het nummer [VERTROUWELIJK]. [VERTROUWELIJK].

Op 5 juli 2018 heeft de AP een melding ontvangen dat bij [VERTROUWELIJK] werknemers verplicht zijn om hun vingerafdruk te laten scannen. Uit de melding maakten toezichthouders van de AP op dat werknemers met behulp van een vingerafdruk in- en uitklokken ten behoeve van tijdsregistratie. Naar aanleiding van dit signaal is de AP een ambtshalve onderzoek gestart naar de naleving door [VERTROUWELIJK] van artikel 9 van de Algemene Verordening Gegevensbescherming (AVG), dat onder meer ziet op het gebruik van de verwerking van biometrische gegevens, zoals een vingerafdruk.

1.2 Procesverloop

Op 6 september en 12 oktober 2018 heeft de AP telefonisch contact opgenomen met de signaalgever om vragen te stellen over zijn melding over (de verplichting tot) het gebruik en de locaties van de vingerscanapparatuur bij [VERTROUWELIJK]. Naar aanleiding daarvan heeft de AP op 22 oktober 2018 van de signaalgever stukken ontvangen.

De AP heeft op 6 november 2018 een onaangekondigd onderzoek uitgevoerd bij [VERTROUWELIJK]. De verslagen over dit onderzoek en de afgenomen verklaringen van medewerkers zijn 11 februari 2019 toegezonden aan [VERTROUWELIJK]. [VERTROUWELIJK] heeft aangegeven geen opmerkingen te hebben naar aanleiding van deze stukken.

Op 18 maart 2019 heeft de AP opnieuw onderzoek ten kantore van [VERTROUWELIJK] uitgevoerd. De verslagen over dit onderzoek en de afgenomen verklaringen van medewerkers zijn 9 mei 2019 toegezonden aan [VERTROUWELIJK].

De AP heeft op 13 juni 2019 een conceptrapport aan [VERTROUWELIJK] verzonden. [VERTROUWELIJK] heeft hierop op 3 juli 2019 haar zienswijze gegeven. Met inachtneming van deze reactie heeft de AP het definitieve rapport vastgesteld. Dit rapport is bij brief van 4 september 2019 aan [VERTROUWELIJK] toegezonden.

Bij brief van 16 september 2019 heef de AP aan [VERTROUWELIJK] een voornemen tot handhaving verzonden. Daartoe tevens bij brief van 16 september 2019 door de AP in de gelegenheid gesteld, heeft [VERTROUWELIJK] op 21 oktober 2019 schriftelijk haar zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde definitieve rapport.

2.Wettelijk kader

2.1 Reikwijdte AVG

Ingevolge artikel 2, eerste lid, van de AVG is deze verordening van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Ingevolge artikel 3, eerste lid, van de AVG is deze verordening van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

Ingevolge artikel 4 van de AVG wordt voor de toepassing van deze verordening verstaan onder:
1. "Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); […].
2. "Verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés […].
7. "Verwerkingsverantwoordelijke": een […] rechtspersoon die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; […].

2.2 Verbod op verwerking biometrische gegevens

Artikel 9, eerste lid, van de AVG definieert bijzondere persoonsgegevens als volgt, voor zover hier relevant: "[…] persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid […]"

Ingevolge artikel 4, veertiende lid, van de AVG zijn biometrische gegevens 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.

Ingevolge artikel 9, eerste lid, van de AVG is de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon verboden.

Uitzonderingen op het verbod om bijzondere persoonsgegevens te verwerken staan vermeld in artikel 9, tweede lid, van de AVG, voor zover hier relevant:

"Lid 1 is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:
a) de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven;
[...]
g) de verwerking is noodzakelijk 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;
[...]"

Ingevolge artikel 4, elfde lid, van de AVG wordt toestemming omschreven als elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.

Ingevolge artikel 7, eerste lid, van de AVG moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens als de verwerking berust op toestemming. Op grond van artikel 7, derde lid, van de AVG heeft de betrokkene het recht zijn toestemming te allen tijde in te trekken. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld.

Ingevolge artikel 29 van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is gelet op artikel 9, tweede lid, onderdeel g, van de verordening, het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

2.3 Bestuurlijke boete

Ingevolge artikel 58, tweede lid, aanhef en onder i, in samenhang met artikel 83, vijfde lid, aanhef en onder b, van de AVG en artikel 14, derde lid, van de UAVG is de AP bevoegd om ten aanzien van inbreuken op de AVG een bestuurlijke boete op te leggen.

2.3.1 AVG

Ingevolge artikel 83, eerste lid, van de AVG zorgt elke toezichthoudende autoriteit ervoor dat de administratieve geldboeten die uit hoofde van dit artikel worden opgelegd voor de in de leden 4, 5 en 6 vermelde inbreuken op deze verordening in elke zaak doeltreffend, evenredig en afschrikkend zijn.
Ingevolge het tweede lid worden administratieve geldboeten, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, tweede lid, onder a tot en met h en onder j, bedoelde maatregelen.

Uit het vijfde lid, aanhef en onder a, volgt dat een inbreuk op de basisbeginselen inzake verwerking zoals in artikel 9 van de AVG overeenkomstig lid 2 onderworpen is aan een administratieve geldboete tot €20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

2.3.2 UAVG

Ingevolge artikel 14, derde lid, van de UAVG kan de AP in geval van overtreding van het bepaalde in artikel 83, vierde, vijfde of zesde lid, van de verordening een bestuurlijke boete opleggen van ten hoogste de in deze leden genoemde bedragen.

3.Beoordeling

3.1 Verwerking van biometrische persoonsgegevens

3.1.1 Feiten

Bij [VERTROUWELIJK] zijn vijf scanstations aanwezig en actief, waarvan drie met vingerscanner. Eén van die drie wordt gebruikt voor het testen en voor het vastleggen van vingerafdrukken, de andere twee voor in- en uitklokken [VERTROUWELIJK]. Al deze scanstations wisselen gegevens uit met een softwareprogramma, waarmee naast controle op aan- en afwezigheid men inzicht kan krijgen in werktijden, ziekteverzuim en overuren.[1]

[VERTROUWELIJK] heeft verklaard dat van haar werknemers van twee vingers vingerafdrukken zijn gemaakt en vastgelegd. Het scanstation berekent een template van de vingerafdruk en slaat deze op in het softwareprogramma. Dit betekent dat met behulp van een fotografische scan unieke puntjes geïdentificeerd worden in de lijnen van de afdruk. De puntjes tezamen vormen de basis voor een wiskundige berekening om de kwaliteit van de vingerafdruktemplate te berekenen.[2]

[VERTROUWELIJK] laat vingerafdrukken van werknemers vastleggen zodra men in dienst komt, zodat men kan inklokken.[3] Uit verklaringen van de werknemers van [VERTROUWELIJK] blijkt dat zij zijn opgeroepen om langs te komen voor het afnemen van de vingerafdruk.[4]

De AP heeft op 18 maart 2019 tijdens het onderzoek bij [VERTROUWELIJK] vastgesteld dat [VERTROUWELIJK] een digitale map bezit met daarin alle vingerafdruktemplates van vingerafdrukken

[1] Verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018, schermafbeelding website leverancier van 29 januari 2019 en verslag technisch onderzoek inclusief bijlagen A t/m H (bijlage G (digitale inhoud map bio_templates) en bijlage H (digitale foto-bestanden) van 19 maart 2019.
[2] Verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[3] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018.
[4] Eerste drie gespreksverslagen met medewerkers van [VERTROUWELIJK] van 7 november 2018 en gespreksverslagen met medewerkers van [VERTROUWELIJK] van 19 maart 2019.

van werknemers die ooit bij [VERTROUWELIJK] zijn gescand. Deze templates zijn opgeslagen als tekstbestanden.[5]

De AP heeft vastgesteld dat uit de inhoud van deze map is af te leiden wat de periode is waarbinnen vingerafdrukken van werknemers zijn vastgelegd. In deze map staan de vingerafdruktemplates opgeslagen als [VERTROUWELIJK]-bestanden. De [VERTROUWELIJK]-bestanden horen bij werknemers die in dienst zijn van [VERTROUWELIJK]. De [VERTROUWELIJK]-bestanden horen bij voormalige werknemers van [VERTROUWELIJK]. Wanneer de vingerafdruktemplates van de desbetreffende werknemer zijn gemaakt, is af te leiden uit de datum in de afzonderlijke tekstbestanden van de templates. Voor [VERTROUWELIJK]-bestanden geldt bovendien dat de opslagdatum overeenkomt met de datum van vastlegging van de vingerafdruk, die in het tekstbestand zelf staat.

De eerste vingerafdruktemplates zijn opgeslagen op 23 januari 2017. Vanaf dat moment zijn regelmatig templates opgeslagen. De laatste vingerafdruktemplates van werknemers dateren van 8 november 2018. Uit de opslagdata van de [VERTROUWELIJK]-bestanden volgt dat van 39 werknemers na 25 mei 2018 vingerafdruktemplates zijn gemaakt. Uit de opslagdata van de [VERTROUWELIJK]-bestanden volgt dat na 25 mei 2018 van 31 werknemers vingerafdruktemplates zijn gemaakt. Uit de inhoud van de [VERTROUWELIJK]-bestanden is af te leiden dat van 17 werknemers na 25 mei 2018 vingerafdruktemplates zijn gemaakt. In totaal zijn er na 25 mei 2018 dus van (39+31+17=) 87 werknemers vingerafdrukken vastgelegd en opgeslagen. De AP heeft vastgesteld dat op 18 maart 2019 in totaal 1348 vingerafdruktemplates (als [VERTROUWELIJK]-bestanden) in deze map zijn opgeslagen. Omdat per werknemer vier vingerafdruktemplates zijn opgeslagen, zijn dit dus de vingerafdrukken van (1348:4=) 337 (voormalige) werknemers van [VERTROUWELIJK].[6]

[VERTROUWELIJK] heeft verklaard dat van werknemers die hun vingerafdruk hebben laten vastleggen en die op 18 maart 2019 in dienst waren, de vingerafdruktemplates op 18 maart 2019 ook echt actief waren in het softwareprogramma en de scanstations.[7] De AP heeft dit mede vastgesteld door een personeelskaart van een werknemer die op dat moment in dienst was te controleren. Op de desbetreffende personeelskaart zijn vingerafdruktemplates actief. Ook blijkt uit de personeelskaart dat er een kwaliteitsaanduiding van de vingerscans staat en dat de vingerafdrukken van deze werknemer op 8 november 2018 zijn vastgelegd.[8]

[VERTROUWELIJK] heeft voorts verklaard dat van werknemers die uit dienst zijn en op 18 maart 2019 als zodanig verwerkt zijn in het softwareprogramma, er geen vingerafdruktemplates meer aanwezig zijn in het softwareprogramma en de scanstations. Als een werknemers uit dienst gaat, worden zijn/haar gegevens volgens [VERTROUWELIJK] wel bewaard, maar geblokkeerd in het softwareprogramma.[9] Dit heeft

[5] Verslag technisch onderzoek inclusief bijlagen A t/m H (bijlage G (digitale inhoud map bio_templates) van 19 maart 2019.
[6] Verslag technisch onderzoek inclusief bijlagen A t/m H (bijlage G (digitale inhoud map bio_templates) van 19 maart 2019.
[7] Verslag technisch onderzoek inclusief bijlagen A t/m H van 19 maart 2019.
[8] Verslag technisch onderzoek inclusief bijlagen A t/m H, bijlage E (afdruk van bestand “mensen in dienst met vingerscan.pptx”) p. 9, van 19 maart 2019.
[9] Gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018.

[VERTROUWELIJK] mede aan de AP geïllustreerd aan de hand van een aantal personeelskaarten van personen die op 18 maart 2019 uit dienst waren.[10]

De AP heeft op 18 maart 2019 160 schermafdrukken van personeelskaarten gemaakt van werknemers waarvan vingerafdruktemplates in zowel het softwareprogramma als de scanstations actief waren.[11] Ook [VERTROUWELIJK] kwam door het aantal [VERTROUWELIJK]-bestanden in de desbetreffende map tot de conclusie dat op 18 maart 2019 van 160 werknemers vingerafdruktemplates actief waren in het softwareprogramma en de scanstations.[12]

Op grond van het bovenstaande concludeert de AP dat na het vastleggen van de vingerafdruk de templates van die vingerafdrukken worden opgeslagen als tekstbestand in een digitale map. Deze templates van vingerafdrukken die sinds begin 2017 vastgelegd zijn, worden daar dus nog altijd bewaard. Dit geldt ook voor vingerafdruktemplates van werknemers die uit dienst zijn, hoewel deze dan worden geblokkeerd en dus niet meer actief zijn in het softwareprogramma en de scanstations.

Productiemedewerkers van [VERTROUWELIJK] kunnen voor het in- en uitklokken alleen hun vingerafdruk en de druppel (een identificatieplaatje) afzonderlijk en naast elkaar gebruiken en doen dit ook regelmatig. Aan de hand van het template in het softwareprogramma wordt hun identiteit op het apparaat bevestigd. Uit de tijdregistratie in het softwareprogramma is niet op te maken of met een vingerafdruk of een druppel is in- of uitgeklokt.[13]

[VERTROUWELIJK] heeft verklaard dat de vingerscanapparatuur op 6 november 2018 pas sinds een klein jaar continu in gebruik is.[14] Meerdere werknemers van [VERTROUWELIJK] hebben verklaard dat de scanstations vanaf 2017 gebruikt worden.[15]

Tijdens het bezoek op 18 maart 2019 heeft [VERTROUWELIJK] aangegeven dat na het bezoek van de AP op 6 november 2018 [VERTROUWELIJK] gestopt is met het scannen van de vingerafdrukken van (nieuwe) werknemers, omdat men niet meer weet of het nu wel of niet toegestaan is.[16] De AP heeft op 18 maart 2019 ook geconstateerd dat [VERTROUWELIJK] sinds 8 november 2018 geen nieuwe vingerafdrukken meer heeft vastgelegd.

[VERTROUWELIJK] heeft op 16 april 2019 instructies ontvangen van de leverancier over het verwijderen van de software en de daarin opgenomen bestanden. [VERTROUWELIJK] heeft verklaard dat zij vlak

[10] Verslag technisch onderzoek inclusief bijlagen A t/m H van 19 maart 2019, p. 2 en 3.
[11] Verslag technisch onderzoek inclusief bijlagen A t/m H, bijlage E (afdruk van bestand "mensen in dienst met vingerscan.pptx"), van 19 maart 2019.
[12] Verslag technisch onderzoek inclusief bijlagen A t/m H (bijlage G (digitale inhoud map bio_templates) van 19 maart 2019.
[13] Eerste drie gespreksverslagen met medewerkers van [VERTROUWELIJK] van 7 november 2018, gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018, gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018 en verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[14] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018.
[15] Tweede en derde gespreksverslag met medewerkers van [VERTROUWELIJK] van 7 november 2018 en gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018.
[16] Verslag van ambtshandelingen onderzoek ter plaatse bij [VERTROUWELIJK] (d.d. 6 november 2018) van 12 november 2018.

daarna de biometrische gegevens van haar (voormalige) werknemers heeft verwijderd en heeft logbestanden als bewijs voor de verwijdering verstrekt.[17] Uit de logbestanden kan worden opgemaakt dat de biometrische gegevens daadwerkelijk zijn verwijderd maar de exacte datum waarop dit is gebeurd kan hieruit niet worden afgeleid.[18] Gelet hierop gaat de AP ervan uit dat de overtreding in ieder geval tot en met 16 april 2019 heeft voortgeduurd.

3.1.2 Beoordeling

Volgens artikel 4, eerste lid, van de AVG betreffen persoonsgegevens 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, door bijvoorbeeld een of meer elementen die kenmerkend zijn voor de fysieke of fysiologische identiteit van die natuurlijke persoon.

Op grond van artikel 4, veertiende lid, van de AVG, omvatten biometrische gegevens persoonsgegevens die onder andere het resultaat zijn van een specifieke technische bewerking met betrekking tot de fysieke kenmerken van een natuurlijke persoon, op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd. Vingerafdrukgegevens worden daarbij expliciet genoemd als voorbeeld van biometrische gegevens.

Artikel 4, tweede lid, van de AVG, definieert het begrip verwerking als een bewerking van persoonsgegevens, zoals het verzamelen, vastleggen, opslaan, opvragen, raadplegen of gebruiken daarvan.

De AP heeft vastgesteld dat [VERTROUWELIJK] vingerafdrukken van 337 (voormalige) werknemers heeft opgeslagen van 23 januari 2017 tot en met in ieder geval 16 april 2019. Zoals uit de feiten blijkt zijn deze vingerafdrukken opgeslagen als templates en blijven ze daar opgeslagen, zelfs als werknemers al uit dienst zijn. Van werknemers die (nog wel) in dienst zijn, zijn de vingerafdruktemplates gekoppeld aan een softwareprogramma, zodat zij kunnen in- en uitklokken met hun vingerafdruk. Werknemers van [VERTROUWELIJK] gebruiken sinds 2017 regelmatig hun vingerafdruk op het vingerscanapparaat om in- en uit te klokken, waarbij aan de hand van het template in het softwareprogramma hun identiteit wordt bevestigd. Alleen al door het vastleggen van vingerafdrukken van werknemers, kan er dus verdere verwerking van de vingerafdruk plaatsvinden, zoals het gebruik van de vingerafdruk om in- en uit- te klokken.

De AP komt tot het oordeel dat met de door [VERTROUWELIJK] opgeslagen gegevens natuurlijke personen, namelijk haar werknemers, kunnen worden geïdentificeerd. De gegevens zijn het resultaat van een specifieke technische bewerking met betrekking tot de fysieke kenmerken van een natuurlijke persoon (de vingerafdruk), op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is dat aan werknemers wordt bevestigd via het vingerscanapparaat. Derhalve is er sprake van biometrische gegevens in de zin van artikel 4, onderdeel veertien, van de AVG. Voor zover [VERTROUWELIJK] betoogt

[17] Schriftelijke reactie van [VERTROUWELIJK] van 13 november 2019, vraag 2 en bijlage 2.
[18] Schriftelijke reactie van [VERTROUWELIJK] van 13 november 2019, vraag 1 en logbestand.

dat de code, die op basis van de vingerafdruk wordt gemaakt, niet te herleiden is naar een werknemer deelt de AP deze conclusie van [VERTROUWELIJK] niet.[19]

[VERTROUWELIJK] heeft de vingerafdrukgegevens digitaal opgeslagen en verwerkt deze mede door middel van de vingerscanapparatuur bij het maken van de vingerafdruk en als werknemers hun vinger scannen om te kunnen in- en uitklokken. De AP komt tot het oordeel dat [VERTROUWELIJK] hierdoor biometrische gegevens (gedeeltelijk) geautomatiseerd heeft verwerkt in de zin van artikel 4, onderdeel twee, van de AVG.

3.1.3 Conclusie

[VERTROUWELIJK] had op 25 mei 2018 biometrische gegevens opgeslagen van 250 werknemers welke geleidelijk zijn aangevuld tot 337 werknemers. [VERTROUWELIJK] heeft tot en met in ieder geval 16 april 2019 de biometrische gegeven verwerkt. Gelet op het voorgaande komt de AP tot de conclusie dat [VERTROUWELIJK] biometrische gegevens van werknemers vanaf 25 mei 2018 tot en met 16 april 2019 heeft verwerkt in de zin van artikel 4, onderdeel veertien, van de AVG.

3.2 Verwerkingsverantwoordelijke

De AP is van oordeel dat [VERTROUWELIJK] de doelen en de middelen voor de verwerking van de biometrische gegevens heeft bepaald. [VERTROUWELIJK] heeft de beslissing genomen om de vingerscanapparatuur als middel in gebruik te nemen (en te financieren) om biometrische gegevens van haar werknemers te verwerken.[20]

[VERTROUWELIJK] heeft daarnaast het doel van de verwerking bepaalt, namelijk het terugdringen van misbruik bij in- en uitklokken ten behoeve van tijdregistratie. Volgens [VERTROUWELIJK] en is in het verleden regelmatig voorgekomen dat één werknemer voor twee werknemers inklokte terwijl maar één persoon aanwezig was. Er waren volgens [VERTROUWELIJK] ook praktische doeleinden. Zo zijn er geen kosten voor aanschaf, verlies of beschadiging van druppels.[21] Medewerkers noemen voorts als reden dat het systeem een sluitende aanwezigheidsregistratie biedt, dat het systeem met vingerscanners het verouderde systeem met druppel-scanners moet vervangen en dat het in de toekomst onderdeel kan zijn van de veiligheid van het computernetwerk (hackpogingen, bedrijfsspionage).[22]

[19] Zie ook Rb. Amsterdam 12 augustus 2019, ECLI:NL:RBAMS:2019:6005, waarin is geoordeeld dat een vingerafdruk die omgezet was naar een code een (biometrisch) persoonsgegeven is in de zin van de AVG.
[20] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018, gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018, overzichtslijst en gekopieerde documenten bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018 document nr. 17 en nr. 18, en verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[21] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018 en verslag van ambtshandelingen onderzoek ter plaatse (d.d. 18 maart 2019) bij [VERTROUWELIJK] van 19 maart 2019.
[22] Gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018 en verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.

Op grond van het bovenstaande merkt de AP [VERTROUWELIJK] aan als verwerkingsverantwoordelijke als bedoeld in artikel 4, onderdeel 7, van de AVG.

3.3 Verbod op verwerking biometrische gegevens

3.3.1 Inleiding

In de afgelopen jaren is het belang van biometrische gegevens voor de identificatie van personen sterk toegenomen. Nieuw ten opzichte van eerdere wetgeving is het feit dat de AVG biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van een persoon, ook aanmerkt als een bijzondere categorie van persoonsgegevens.[23]

Persoonsgegevens die bijzonder gevoelig zijn verdienen specifieke bescherming, omdat de verwerking ervan hoge risico's kan meebrengen voor grondrechten en fundamentele vrijheden. De verwerking van bijzondere categorieën van persoonsgegevens is daarom op grond van artikel 9, eerste lid, van de AVG verboden, tenzij een wettelijke uitzondering van toepassing is.[24]

De AP toetst in het navolgende of [VERTROUWELIJK] een geslaagd beroep kan doen op voor deze casus relevante uitzonderingen zoals bedoeld in artikel 9, tweede lid, onder a en g, van de AVG. Dit betreft verwerkingen op grond van respectievelijk "uitdrukkelijke toestemming" of die "noodzakelijk voor authenticatie of beveiligingsdoeleinden" zijn.

3.3.2 Feiten

In de arbeidsovereenkomsten die [VERTROUWELIJK] hanteert is geen informatie opgenomen over het gebruik van vingerafdrukken.[25] De destijds toepasselijke personeelshandboeken, gedateerd op juli 2017, melden het volgende: "[VERTROUWELIJK]".[26]

De AP heeft op 6 november 2018 een kopie ontvangen van een conceptversie van aanpassingen aan het personeelshandboek productie. Bovengenoemde alinea over aanwezigheidsregistratie was onveranderd gebleven.[27] In een vernieuwde versie van de handboeken, die zijn gedateerd op januari 2019, is de zin "[VERTROUWELIJK]" weggelaten.[28]

Meerdere werknemers van [VERTROUWELIJK] hebben verklaard dat het vastleggen van de vingerafdrukken als een verrassing kwam, niet was aangekondigd en dat zij hierover geen informatie hebben ontvangen.[29] De AP heeft geïnformeerd naar documentatie van beleid of procedures voor of bewijs

[23] Zie *Kamerstukken II* 2017/18, 34851, 3, p. 40 en 108 (MvT).
[24] Zie overweging 51 van de AVG.
[25] Overzichtslijst en gekopieerde documenten bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018, nr. 3, 4, 5 en 6.
[26] Overzichtslijst en gekopieerde documenten bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018, nr. 7 en 8.
[27] Overzichtslijst en gekopieerde documenten bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018, nr. 9.
[28] Overzichtslijst en gekopieerde documenten bij onderzoek ter plaatse (d.d. 18 maart 2019) van 19 maart 2019.
[29] Eerste drie gespreksverslagen met medewerkers van [VERTROUWELIJK] van 7 november 2018 en eerste gespreksverslag met medewerker van [VERTROUWELIJK] van 19 maart 2019.

van het verlenen van toestemming voor afname van vingerafdrukken en weigering daarvan. Dergelijke documentatie was niet beschikbaar.

De directeur van [VERTROUWELIJK] heeft verklaard geen idee te hebben of voor de verwerking van de vingerafdrukken toestemming wordt gevraagd aan de werknemers, maar wel dat het een vrije keuze is.[30] De [VERTROUWELIJK] heeft verklaard dat werknemers geen toestemming geven voor het gebruik van hun vingerafdruk, maar dat het scannen van de vingerafdruk niet verplicht is. Zij tekenen wel voor ontvangst van de druppel.[31]

De [VERTROUWELIJK] geeft verder aan dat er een mogelijkheid is om afname van de vingerafdrukken te weigeren. Daarvoor moet de betrokken werknemer dan het gesprek aangaan met de directeur. In de praktijk komt dit bijna niet voor. In de paar gevallen waarin dit voorgevallen is, heeft de werknemer na het gesprek met de directeur alsnog zijn of haar vingerafdruk afgegeven.[32]

Een [VERTROUWELIJK] heeft verklaard dat wat betreft toestemming naar de arbeidsovereenkomst en het personeelshandboek gekeken moet worden, op basis waarvan zij het bekend acht te zijn bij werknemers dat [VERTROUWELIJK] in de toekomst met vingerafdrukken wil gaan werken.[33]

Over het antwoord op de vraag of voor de afname van vingerafdrukken toestemming wordt gevraagd, bestaat een wisselend beeld bij werknemers op de werkvloer. Aan de ene kant geven werknemers aan dat het scannen van de vingerafdruk verplicht was. Aan de andere kant zijn er twee werknemers die verklaren dat zij mondeling toestemming hebben gegeven.[34]

Voor de toets of de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden zijn de volgende feiten van belang.

De bedrijfsactiviteiten van [VERTROUWELIJK].[35] [VERTROUWELIJK].[36]

Zoals vermeld in paragraaf 3.1.1. gebruikt [VERTROUWELIJK] een softwareprogramma voor tijdregistratie en – op basis daarvan – de administratie van salaris, verlof en ziekte. De aanwezigheid van werknemers werd in het verleden alleen geregistreerd door middel van het in- en uitklokken met druppels bij scanstations.[37]

[30] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018.
[31] Gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018.
[32] Verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[33] Gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018.
[34] Eerste drie gespreksverslagen met medewerkers van [VERTROUWELIJK] van 7 november 2018 en gespreksverslagen met medewerkers van [VERTROUWELIJK] van 19 maart 2019.
[35] KvK uittreksel [VERTROUWELIJK] van 15 oktober 2018.
[36] Verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[37] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018 en gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018.

De directeur van [VERTROUWELIJK] heeft besloten het tijdregistratiesysteem uit te breiden met de vingerscanapparatuur. Hij heeft het besluit zelfstandig genomen in zijn hoedanigheid van algemeen directeur van [VERTROUWELIJK].[38] Zoals in paragraaf 3.2 vermeld was de reden hiervoor het terugdringen van misbruik bij in- en uitklokken ten behoeve van tijdregistratie. Er waren volgens [VERTROUWELIJK] ook praktische voordelen. Zo zijn er geen kosten voor aanschaf, verlies of beschadiging van druppels. Medewerkers noemen voorts als reden dat het systeem een sluitende aanwezigheidsregistratie biedt, dat het systeem met vingerscanners het verouderde systeem met druppel-scanners moet vervangen en dat het in de toekomst onderdeel kan zijn van de veiligheid van het computernetwerk (hackpogingen, bedrijfsspionage). Door gebruik van vingeridentificatie kunnen tot slot slechts personen binnenkomen die opgeleid zijn voor het gebruik van geavanceerde apparatuur.

3.3.3 Beoordeling

3.3.3.1 Uitdrukkelijke toestemming

Op grond van artikel 4, onderdeel 11, van de AVG is toestemming een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.

Opdat toestemming met kennis van zaken wordt gegeven, moet de betrokkene onder andere geïnformeerd worden over de identiteit van de verwerkingsverantwoordelijke, het doel van de verwerking, welke (soort) gegevens worden verwerkt en het bestaan van het recht om toestemming in te trekken.[39]

Een betrokkene moet daarnaast de toestemming vrij kunnen geven. In de Richtsnoeren inzake toestemming overeenkomstig de AVG wordt hierover opgemerkt:
"*Wanverhouding doet zich ook 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 gegevensverwerking zou kunnen onthouden zonder angst of reële dreiging van nadelige gevolgen als gevolg van een weigering. Het is onwaarschijnlijk dat de werknemer vrijelijk zou kunnen reageren op een verzoek voor toestemming van zijn/haar werkgever voor, bijvoorbeeld, het activeren van toezichtsystemen zoals camera observatie op de werkvloer, of het invullen van beoordelingsformulieren, zonder druk te voelen om toestemming te verlenen. Daarom is WP29 van mening dat het voor werknemers problematisch is om persoonsgegevens van huidige of toekomstige werknemers te verwerken op basis van toestemming, omdat het onwaarschijnlijk is dat deze vrijelijk wordt verleend. Voor de merendeel van dergelijke gegevensverwerking op het werk, kan en mag de rechtsgrond geen toestemming van de werknemers zijn (artikel 6, lid 1, onder a) vanwege de aard van de relatie tussen werkgever en werknemer. Dit betekent echter niet dat werkgevers nooit kunnen vertrouwen op toestemming als een rechtsgrond voor verwerking. Er kunnen situaties zijn waarin de werkgever kan aantonen dat toestemming daadwerkelijk vrijelijk wordt verleend. Gezien de wanverhouding tussen een werkgever en zijn personeel, kunnen werknemers alleen in uitzonderlijke omstandigheden vrijelijk toestemming geven, en wel wanneer*

[38] Gespreksverslag met directeur van [VERTROUWELIJK] van 9 november 2018, gespreksverslag met [VERTROUWELIJK] bij [VERTROUWELIJK] van 9 november 2018 en verslag technisch onderzoek bij onderzoek ter plaatste (d.d. 6 november 2018) van 12 november 2018.
[39] Zie overweging 42 van de AVG, de Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 d.d. 28 november 2017 blz. 15 en artikel 7, derde lid, van de AVG.

het geen negatieve gevolgen heeft als zij al dan niet toestemming geven. […] Wanverhoudingen zijn niet beperkt tot overheidsinstanties en werknemers, ze kunnen zich ook voordoen in andere situaties. Zoals WP29 in verschillende Adviezen heeft benadrukt, kan "toestemming" alleen rechtsgeldig zijn als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen (bijvoorbeeld op aanzienlijke extra kosten) loopt wanneer hij of zij niet toestemt. Toestemming is niet vrij in gevallen waar sprake is van enig element van dwang, druk of niet kunnen uitoefenen van de vrije wil".[40]

Op grond van artikel 7, eerste lid, van de AVG moet de verwerkingsverantwoordelijke voorts kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

De voorwaarden van artikel 7 van de AVG gelden ook voor het begrip toestemming in artikel 9 van de AVG.[41] Om te voldoen aan de voorwaarde van artikel 9, tweede lid, onder a, van de AVG voor uitzondering op het verbod van verwerking van biometrische gegevens van artikel 9, eerste lid, van de AVG geldt – bovenop de voorwaarden die artikel 7 AVG stelt aan toestemming – dat de betrokkene *uitdrukkelijk* toestemming moet geven.

Volgens de Richtsnoeren inzake toestemming overeenkomstig de AVG verwijst uitdrukkelijke toestemming naar de manier waarop toestemming door de betrokkene tot uiting wordt gebracht. Hierbij kan volgens de Richtsnoeren gedacht worden aan schriftelijke toestemming, ondertekening (eventueel met elektronische handtekening), het door betrokkene versturen van een e-mail of toestemming met tweetrapsverificatie. In theorie kan het gebruik van mondelinge verklaring ook voldoende zijn om geldige uitdrukkelijke toestemming te verkrijgen, het kan echter voor de verwerkingsverantwoordelijke moeilijk te bewijzen zijn dat bij het opnemen van de verklaring voldaan is aan alle voorwaarden voor geldige uitdrukkelijke toestemming.[42]

Op grond van de volgende feiten komt de AP tot het oordeel dat [VERTROUWELIJK] niet heeft aangetoond dat haar werknemers uitdrukkelijke toestemming hebben gegeven voor de verwerking van hun biometrische gegevens. De vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting van de werknemers van [VERTROUWELIJK] is niet vast komen te staan.

[VERTROUWELIJK] heeft als verwerkingsverantwoordelijke niet aangetoond dat haar werknemers überhaupt (uitdrukkelijke) toestemming hebben gegeven voor de verwerking van de biometrische gegevens, wat op grond van artikel 7, eerste lid, van de AVG wel verplicht is. Uit paragraaf 3.3.2 blijkt immers dat bij [VERTROUWELIJK] geen documentatie van beleid of procedures voor of bewijs van het verlenen van toestemming voor het vastleggen van vingerafdrukken en weigering daarvan bestaat. Daarbij hebben verschillende werknemers verklaard dat het scannen van de vingerafdrukken verplicht was en dat daarvoor geen toestemming wordt gevraagd, ook niet in het kader van de ondertekening van de arbeidsovereenkomst of ontvangst van het personeelshandboek. Twee werknemers hebben verklaard dat

[40] Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 d.d. 28 november 2017, blz. 7-8. Laatstelijk herzien en vastgesteld door de Groep gegevensbescherming Artikel 29 op 10 april 2018.
[41] Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 d.d. 28 november 2017, blz. 23.
[42] Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 d.d. 28 november 2017, blz. 20-22.

zij voor het vastleggen van hun vingerafdruk mondeling toestemming hebben gegeven. [VERTROUWELIJK] heeft echter ook het bestaan van eventuele mondelinge verklaringen omtrent toestemming niet kunnen aantonen. [VERTROUWELIJK] heeft dus niet kunnen aantonen dat haar werknemers uitdrukkelijke toestemming in de zin van artikel 9, tweede lid, onder a, van de AVG hebben gegeven voor de verwerking van hun biometrische gegevens.

Ten overvloede merkt de AP op dat [VERTROUWELIJK] ook niet heeft kunnen aantonen dat haar werknemers voldoende geïnformeerd waren over de verwerking van de biometrische gegevens en dat zij in vrijheid hun toestemming hebben gegeven. Zoals vermeld in paragraaf 3.3.2 was er in de arbeidsovereenkomst geen informatie opgenomen over het gebruik van vingerafdrukken. Werknemers zijn slechts via het personeelshandboek van juli 2017 geïnformeerd dat [VERTROUWELIJK] de *intentie* heeft om volledig met de vingerafdruk in te gaan klokken. In het meest recente personeelshandboek van januari 2019 staat niets meer over het voornemen om volledig over te gaan op tijdsregistratie met de vingerafdruk. Meerdere werknemers van [VERTROUWELIJK] hebben daarnaast verklaard dat het vastleggen van de vingerafdrukken niet was aangekondigd en dat zij hierover geen informatie hebben ontvangen.

Daarnaast heeft [VERTROUWELIJK] niet aangetoond dat eventueel gegeven toestemmingen vrij door haar werknemers zijn gegeven. Bovendien hebben werknemers van [VERTROUWELIJK] verklaard dat het scannen van de vingerafdruk verplicht was. En hebben de [VERTROUWELIJK] en een werknemer verklaard dat bij weigering om de vingerafdruk te laten inscannen een gesprek met de directeur/bestuur volgde, waarna in de praktijk (bijna) iedereen zijn/haar vingerafdruk laat scannen.

Uit bovenstaande volgt dat – ondanks dat [VERTROUWELIJK] vindt dat er een keuzevrijheid voor werknemers was om al dan niet in- en uit te klokken met behulp van hun vingerafdruk – verschillende werknemers het als een verplichting hebben ervaren om hun vingerafdruk te laten vastleggen. Tussen de werkgever en de werknemer is er sprake van een hiërarchische verhouding. Gezien de afhankelijkheid die het gevolg is van de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de werknemer zijn of haar toestemming vrijelijk kan verlenen. [VERTROUWELIJK] heeft bovendien niet aangetoond dat er in dit geval vrijelijk toestemming is verleend.

[VERTROUWELIJK] moet ingevolge artikel 7, eerste lid, van de AVG aantonen dat een betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. De voorwaarden van artikel 7 van de AVG gelden ook voor het begrip toestemming in artikel 9 van de AVG. Op grond van het bovenstaande is de AP van oordeel dat [VERTROUWELIJK] niet heeft kunnen aantonen dat haar werknemers uitdrukkelijke toestemming in de zin van artikel 9, tweede lid, onder a, van de AVG hebben gegeven voor de verwerking van hun biometrische gegevens.

Zienswijze [VERTROUWELIJK] en reactie AP
[VERTROUWELIJK] is van mening dat de medewerkers toestemming hebben gegeven voor het gebruik van hun vingerafdrukken en dat ook nooit iemand daar bezwaar tegen heeft gemaakt. Het systeem met de druppel werd door veel werknemers ook als onhandig ervaren. [VERTROUWELIJK] is altijd zeer open

geweest over het in gebruik nemen van het vingerscansysteem en had daarmee enkel goede bedoelingen. Het is ook nooit een verplichting geweest om met de vingerscan in- en uit te klokken; dit kon ook altijd nog met de druppel. [VERTROUWELIJK] is daarmee van mening dat de werknemers vrijelijk hun toestemming hebben kunnen geven. Het is ook geenszins juist, dat werknemers die hun vingerafdruk niet wilde laten afnemen, een gesprek met de directie kregen. Niemand is volgens [VERTROUWELIJK] gedwongen de vingerscans te gebruiken en de mogelijkheid om gebruik te maken van het druppelsysteem, is altijd blijven bestaan. Sterker nog, van de 4 aanwezige druppel klokken, zijn er maar 2 additioneel uitgerust met de vingerscan optie.

[VERTROUWELIJK] geeft aan, na het eerste bezoek van de AP op 6 november 2018, direct maatregelen genomen te hebben en gestopt te zijn met het in- en uitklokken door middel van vingerafdrukken. Na die datum zijn ook geen vingerafdrukken meer vastgelegd. Na het tweede bezoek van de AP op 18 maart 2019 heeft [VERTROUWELIJK] contact gezocht met de leverancier van de vingerafdrukapparatuur en heeft de afgenomen vingerscans en het programma met betrekking tot de registratie met vingerafdrukken laten verwijderen. [VERTROUWELIJK] wilde ervoor zorgen dat zo snel mogelijk alle biometrische gegevens vernietigd zouden worden, zodat [VERTROUWELIJK] verder geen risico zou lopen. De leverancier heeft aan [VERTROUWELIJK] aangegeven dat het gebruik van de vingerscan in deze toegestaan is, omdat dit niet verplicht is en er 2 scan mogelijkheden worden aangeboden door [VERTROUWELIJK]: de vingerscan en de druppel.

De AP vat de zienswijze zo op dat [VERTROUWELIJK] van mening is dat de werknemers vrijelijk hun toestemming hebben kunnen geven voor het verwerken van de vingerafdrukken. De AP volgt de zienswijze van [VERTROUWELIJK] niet. Gezien de afhankelijkheid die het gevolg is van de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de werknemer zijn of haar toestemming vrijelijk kan verlenen. Mocht in dit uitzonderlijke geval wel sprake zijn van vrije toestemming, dan had [VERTROUWELIJK] dit moeten aantonen. [VERTROUWELIJK] heeft geen bewijs geleverd dat haar werknemers toestemming hebben gegeven voor de verwerking van de vingerafdrukken, laat staan dat de toestemming vrij en geïnformeerd is gegeven. Bovendien hebben verschillende werknemers, ondanks de keuzevrijheid voor werknemers om al dan niet in- en uit te klokken met behulp van hun vingerafdruk, het als een verplichting ervaren om hun vingerafdruk te laten vastleggen.

3.3.3.2 Noodzakelijk voor authenticatie of beveiligingsdoeleinden

Artikel 9, tweede lid, onder g, van de AVG, laat ruimte voor een uitzondering in nationaal recht op het verbod om biometrische gegevens te verwerken om redenen van zwaarwegend algemeen belang. In Nederland is daar invulling aan gegeven in artikel 29 van de UAVG, door verwerking van biometrische gegevens toe te staan indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Verder vermeldt de Memorie van Toelichting bij artikel 29 van de UAVG dat het onwenselijk is om geen nationale uitzondering voor de verwerking van biometrische gegevens op te nemen. Voorts staat hier: "*Er dient wel een afweging te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt*

dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen. Om deze afweging mogelijk te maken in omstandigheden waarin toestemming niet in vrijheid kan worden gegeven, is in het wetsvoorstel een bepaling opgenomen die een uitzondering op het verbod voor verwerking van biometrische gegevens mogelijk maakt met het oog op de identificatie van de betrokkene, indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden".[43]

Zoals de Memorie van Toelichting stelt moet er een afweging worden gemaakt of identificatie door middel van biometrie noodzakelijk en proportioneel is voor authenticatie of beveiligingsdoeleinden. [VERTROUWELIJK] had moeten afwegen of de gebouwen en informatiesystemen van [VERTROUWELIJK] zodanig beveiligd moeten zijn dat dit met biometrische gegevens dient plaats te vinden. Hiervoor geldt een strenge toets. Bij een kerncentrale mag bijvoorbeeld biometrie ingezet worden voor toegangscontrole. Daar is het belang van beveiliging heel groot en mogen maar bepaalde mensen toegang hebben. Ook had [VERTROUWELIJK] dienen af te wegen of het verwerken van vingerafdrukken van werknemers bij [VERTROUWELIJK] proportioneel is. Het gebruik van biometrische persoonsgegevens bij toegang tot bijvoorbeeld de garage van een reparatiebedrijf kan deze toets niet doorstaan. De noodzaak van beveiliging is dan immers niet zo groot dat mensen door gebruik van biometrie toegang moeten kunnen krijgen. Daarnaast kan de beveiliging ook op andere minder verregaande manieren gewaarborgd worden.

Zoals vermeld in paragraaf 3.3.2 bestaan de bedrijfsactiviteiten van [VERTROUWELIJK] onder andere uit [VERTROUWELIJK]. [VERTROUWELIJK] wordt volgens [VERTROUWELIJK] eenvoudig werk verricht, zoals [VERTROUWELIJK]. [VERTROUWELIJK] wordt volgens [VERTROUWELIJK] tevens gewerkt met geavanceerde apparatuur om deze te maken.

[VERTROUWELIJK] gebruikt het desbetreffende softwareprogramma voor tijdregistratie en – op basis daarvan – de administratie van salaris, verlof en ziekte. De aanwezigheid van werknemers werd in het verleden alleen geregistreerd door middel van het in- en uitklokken met druppels bij scanstations. De directeur van [VERTROUWELIJK] heeft zelfstandig besloten het tijdregistratiesysteem uit te breiden met de vingerscanapparatuur. Zoals in paragraaf 3.2 vermeld was reden hiervoor het terugdringen van misbruik bij in- en uitklokken ten behoeve van tijdregistratie. Er waren volgens [VERTROUWELIJK] ook praktische voordelen. Zo zijn er geen kosten voor aanschaf, verlies of beschadiging van druppels. Medewerkers noemen voorts als reden dat het systeem een sluitende aanwezigheidsregistratie biedt, dat het systeem met vingerscanners het verouderde systeem met druppel-scanners moet vervangen en dat het in de toekomst onderdeel kan zijn van de veiligheid van het computernetwerk (hackpogingen, bedrijfsspionage). Door gebruik van vingeridentificatie kunnen tot slot slechts personen kunnen binnenkomen die opgeleid zijn voor het gebruik van geavanceerde apparatuur.

[43] *Kamerstukken II* 2017/18, 34851, 3, p. 94-95 (MvT).

De AP is van oordeel dat het verwerken van biometrische gegevens in het kader van (het tegengaan van misbruik bij) tijdsregistratie, aanwezigheidscontrole en bevoegd gebruik van apparatuur bij [VERTROUWELIJK] niet noodzakelijk en proportioneel is. De eerder beschreven werkzaamheden bij [VERTROUWELIJK], waaronder [VERTROUWELIJK], benaderen namelijk eerder de werkzaamheden binnen een garage van een reparatiebedrijf, waarbij het volgens de Memorie van Toelichting bij artikel 29 van de UAVG niet noodzakelijk en proportioneel is om biometrische gegevens te verwerken. Weliswaar heeft [VERTROUWELIJK] een belang om te werken met vingerscanapparatuur voor (het tegengaan van misbruik bij) tijdsregistratie, maar gelet op dit doel en de bedrijfsactiviteiten van [VERTROUWELIJK] rechtvaardigt dat belang geen uitzondering op het verbod van verwerking van biometrische gegevens. Net als bij een garage, is ook bij [VERTROUWELIJK] de noodzaak van de beveiliging niet zodanig dat werknemers met biometrie toegang moeten kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Daarnaast kunnen andere manieren, die minder inbreuk op de privacy van werknemers maken, dit ook bewerkstelligen.

Op het conceptrapport van bevindingen van de AP heeft [VERTROUWELIJK] aangegeven het eens te zijn met de AP dat de uitzonderingsgrond 'noodzakelijk voor beveiliging of authenticatie' bij [VERTROUWELIJK] wellicht niet op gaat. Volgens [VERTROUWELIJK] is dit de hoofdreden om bij [VERTROUWELIJK] het gebruik van biometrische gegevens voor toegangscontrole te stoppen. [VERTROUWELIJK] heeft op het definitieve rapport van bevinden geen zienswijze gegeven over deze uitzonderingsgrond.

Op grond van het bovenstaande is de AP van oordeel dat bij [VERTROUWELIJK] geen noodzaak bestaat om het verbod van verwerking van biometrische gegevens in het kader van authenticatie of beveiligingsdoeleinden te rechtvaardigen. [VERTROUWELIJK] kan zich wat betreft de verwerking van vingerafdrukken derhalve niet beroepen op de uitzonderingsmogelijkheid van artikel 9, tweede lid, onder g, van de AVG in samenhang met artikel 29 van de UAVG.

3.3.4 Conclusie

Op grond van artikel 9, eerste lid, van de AVG is het in beginsel verboden om biometrische gegevens te verwerken. De AP komt tot de conclusie dat de verwerking van biometrische gegevens onder verantwoordelijkheid van [VERTROUWELIJK] niet aan de voorwaarden voor een uitzondering op het verbod van artikel 9 van de AVG voldoet, specifiek niet aan de voorwaarden als bedoeld in artikel 9, tweede lid, onder a, van de AVG of artikel 9, tweede lid, onder g, van de AVG in samenhang gelezen met artikel 29 van de UAVG. Hiermee heeft [VERTROUWELIJK] het verbod van artikel 9, eerste lid, van de AVG overtreden.

3.4 Eindconclusie

De AP komt tot de conclusie dat [VERTROUWELIJK] als verwerkingsverantwoordelijke van 25 mei 2018 tot en met 16 april 2019 het verbod van artikel 9, eerste lid, van de AVG heeft overtreden door biometrische gegevens van haar werknemers te verwerken.

4. Boete

4.1 Inleiding

[VERTROUWELIJK] heeft van 25 mei 2018 tot en met 16 april 2019 het verbod van artikel 9, eerste lid, van de AVG overtreden door biometrische gegevens van haar werknemers te verwerken.

De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan [VERTROUWELIJK] een boete op te leggen op grond van artikel 58, tweede lid, aanhef en onder i en artikel 83, vijfde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG. De AP hanteert hiervoor de Boetebeleidsregels 2019.[44]

Hierna zal de AP eerst kort de boetesystematiek uiteenzetten, gevolgd door de motivering van de boetehoogte in het onderhavige geval.

4.2 Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (Boetebeleidsregels 2019)

Ingevolge artikel 58, tweede lid, aanhef en onder i en artikel 83, vijfde lid, van de AVG, gelezen in samenhang met artikel 14, derde lid, van de UAVG, is de AP bevoegd aan [VERTROUWELIJK] in geval van een overtreding van artikel 9, eerste lid, van de AVG een bestuurlijke boete op te leggen tot € 20.000.000 of tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.

De AP heeft Boetebeleidsregels 2019 vastgesteld inzake de invulling van voornoemde bevoegdheid tot het opleggen van een bestuurlijke boete, waaronder het bepalen van de hoogte daarvan.[45]

Ingevolge artikel 2, onder 2.2, van de Boetebeleidsregels 2019 zijn de bepalingen ter zake van overtreding waarvan de AP een bestuurlijke boete kan opleggen van ten hoogste het bedrag van € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, in bijlage 2 ingedeeld in categorie I, categorie II, categorie III of categorie IV. De boetecategorieën zijn gerangschikt naar zwaarte van de overtreding, waarbij categorie I de minst zware overtredingen bevat en categorie III of IV de zwaarste overtredingen.

In bijlage 2 is artikel 9 van de AVG ingedeeld in categorie IV.

Ingevolge artikel 2, onder 2.3, stelt de AP de basisboete voor overtredingen waarvoor een wettelijk boetemaximum geldt van € 20.000.000 of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is, […] vast binnen de volgende boetebandbreedte:
Categorie IV: Boetebandbreedte tussen € 450.000 en € 1.000.000 en een basisboete van € 725.000. […].

[44] Stcrt. 2019, 14586, 14 maart 2019.
[45] Idem.

Ingevolge artikel 6 bepaalt de AP de hoogte van de boete door het bedrag van de basisboete naar boven (tot ten hoogste het maximum van de bandbreedte van de aan een overtreding gekoppelde boetecategorie) of naar beneden (tot ten laagste het minimum van die bandbreedte) bij te stellen. De basisboete wordt verhoogd of verlaagd afhankelijk van de mate waarin de factoren die zijn genoemd in artikel 7 daartoe aanleiding geven.

Ingevolge artikel 7 houdt de AP onverminderd de artikelen 3:4 en 5:46 van de Algemene wet bestuursrecht (Awb) rekening met de factoren die zijn ontleend aan artikel 83, tweede lid, van de AVG en in de Beleidsregels genoemd onder a tot en met k:
a. de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
b. de opzettelijke of nalatige aard van de inbreuk;
c. de door de verwerkingsverantwoordelijke […] genomen maatregelen om de door betrokkenen geleden schade te beperken;
d. de mate waarin de verwerkingsverantwoordelijke […] verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32 van de AVG;
e. eerdere relevante inbreuken door de verwerkingsverantwoordelijke […];
f. de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
g. de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
h. de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke […] de inbreuk heeft gemeld;
i. de naleving van de in artikel 58, tweede lid, van de AVG genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke […] in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;
j. het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 van de AVG of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42 van de AVG; en
k. elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

Het gaat in het voorliggende geval om een beoordeling van de aard, de ernst en de duur van de overtreding in het specifieke geval. In beginsel wordt daarbij binnen de bandbreedte van de aan die overtreding gekoppelde boetecategorie gebleven. De AP kan, zo nodig en afhankelijk van de mate waarin voornoemde factoren daartoe aanleiding geven, de boetebandbreedte van de naast hogere respectievelijk de naast lagere categorie toepassen. Daarnaast beoordeeld de AP bij de oplegging van een bestuurlijke boete op grond van artikel 5:46, tweede lid, van de Awb in hoeverre deze aan de overtreder kan worden verweten.

4.3 Boetehoogte

4.3.1. Aard, ernst en duur van de inbreuk

Ingevolge artikel 7, aanhef en onder a, van de Boetebeleidsregels 2019 houdt de AP rekening met de aard, de ernst en de duur van de inbreuk. Bij de beoordeling hiervan betrekt de AP onder meer de aard, de omvang of het doel van de verwerking alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade.

De AVG biedt een hoog beschermingsniveau voor bijzonder gevoelige persoonsgegevens. Persoonsgegevens die bijzonder gevoelig zijn verdienen specifieke bescherming, omdat de verwerking ervan hoge risico's kan meebrengen voor grondrechten en fundamentele vrijheden. Betrokkenen dienen daarom in hoge mate controle te hebben over hun biometrische gegevens. Uitgangspunt is dan ook dat het verwerken van bijzondere persoonsgegevens in beginsel verboden is. Daarop is slechts een beperkt aantal en in de AVG vastgestelde uitzonderingen mogelijk. Met het afnemen van vingerafdrukken en het vervolgens bewaren van biometrische gegevens heeft [VERTROUWELIJK]x in dit geval het hoge beschermingsniveau dat artikel 9, eerste lid, van de AVG biedt geschonden.

[VERTROUWELIJK] heeft van 25 mei 2018 tot en met 16 april 2019 biometrische gegevens van haar werknemers verwerkt. Deze overtreding heeft daarmee op structurele wijze plaatsgevonden en voor een langere periode voortgeduurd. Tijdens deze periode heeft [VERTROUWELIJK] ook de biometrische gegevens van voormalig werknemers bewaard, terwijl daar geen noodzaak voor was. Gedurende deze periode hebben de betrokkenen dus geen controle gehad over hun biometrische gegevens.

Enerzijds heeft [VERTROUWELIJK] de biometrische gegevens versleuteld en verklaard dat alleen een beperkt aantal mensen toegang had tot de gegevens. Anderzijds blijkt uit het feit dat [VERTROUWELIJK] op 25 mei 2018 biometrische gegevens had opgeslagen van 250 werknemers welk aantal geleidelijk is toegenomen tot 337 werknemers, er sprake was van een systematische en structurele inbreuk.

Gelet op het feit dat de overtreding ruim tien maanden heeft geduurd waarbij 337 betrokkenen zijn getroffen, is er sprake geweest van een ernstige situatie. [VERTROUWELIJK] heeft daarbij niet alleen de biometrische gegevens van huidige werknemers maar ook van voormalig werknemers zonder noodzaak langere tijd bewaard. Bovendien waren de werknemers onvoldoende geïnformeerd over de verwerking en staat niet vast staat dat zij (in vrijheid) toestemming hebben gegeven, waardoor naar het oordeel van de AP sprake is van een ernstige overtreding waarin de bijzondere gegevens van betrokkenen onder onjuiste voorwaarden zijn verwerkt.

Dit heeft tot gevolg gehad dat een grote groep werknemers van [VERTROUWELIJK] niet wist voor welke doeleinden de vingerafdrukken werden gebruikt en dat zij hun toestemming ten alle tijden konden intrekken. Betrokkenen hebben hierdoor een langere periode geen controle gehad over wat er met hun biometrische gegevens gebeurde bij [VERTROUWELIJK]. En het is juist deze controle die de AVG aan betrokkenen wil bieden, zodat betrokkenen in staat zijn om hun persoonsgegeven te beschermen en deze in vrijheid af te kunnen staan. Derhalve is de AP van mening dat sprake is van een ernstige overtreding, maar ziet hierin in dit geval geen aanleiding om het boetebedrag te verhogen of te verlagen.

4.3.2 Verwijtbaarheid

Ingevolge artikel 5:46, tweede lid, van de Awb houdt de AP bij de oplegging van een bestuurlijke boete rekening met de mate waarin deze aan de overtreder kan worden verweten.

Op grond van artikel 9, eerste lid, van de AVG is het in beginsel verboden om biometrische gegevens te verwerken. De AVG is vanaf 25 mei 2018 van toepassing en dateert uit 27 april 2016. Verwerkingsverantwoordelijken hebben tot 25 mei 2018 twee jaar de tijd gehad om hun verwerkingsactiviteiten in overeenstemming te brengen met de AP.

[VERTROUWELIJK] heeft in oktober 2016, ruim na de publicatie van de AVG, de vingerscanapparatuur afgenomen van een leverancier. Volgens [VERTROUWELIJK] heeft deze leverancier op geen enkel moment gewezen op mogelijke strijd met (toekomstige) privacyregelgeving en vertrouwde zij erop dat deze professionele partij [VERTROUWELIJK] op de hoogte zou brengen bij veranderingen. De AP is van oordeel dat deze omstandigheid [VERTROUWELIJK] niet disculpeert. Als uitgangspunt geldt dat [VERTROUWELIJK] een eigen verantwoordelijkheid heeft om zich reeds vanaf inwerkingtreding van de AVG aan de daarin gestelde regels te houden. [VERTROUWELIJK] heeft nagelaten om zelf de verwerking van de biometrische gegevens te toetsen aan de AVG of daar juridisch advies over in te winnen. In plaats daarvan ging [VERTROUWELIJK] ervan uit dat een derde partij, met een commercieel belang bij de verkoop van de apparatuur, deze verantwoordelijkheid op zich nam. Van een professionele partij als [VERTROUWELIJK] mag, mede gelet op de bijzondere aard van de persoonsgegevens, worden verwacht dat zij zich terdege van de voor haar geldende normen vergewist en deze naleeft. [VERTROUWELIJK] heeft door haar handelswijze het hoge beschermingsniveau voor bijzondere persoonsgegevens geschonden. De AP acht dit verwijtbaar.

4.3.3 Zienswijze [VERTROUWELIJK] en reactie AP

[VERTROUWELIJK] beargumenteert in haar zienswijze dat aan de hand van de factoren van artikel 83, tweede lid, van de AVG en de Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten van 3 oktober 2017 een boete niet passend is en indien desondanks wel een boete wordt opgelegd, deze door de AP gematigd moet worden. [VERTROUWELIJK] is van oordeel dat als er sprake is van een overtreding van de AVG, het niet redelijk/opportuun zou zijn om een boete op te leggen. In dit geval is volgens [VERTROUWELIJK] een berisping een passende maatregel, die voldoende doeltreffend, evenredig en afschrikkend is. De AP zet de punten uit de zienswijze van [VERTROUWELIJK] hieronder kort uiteen, voorzien van een reactie van de AP.

Voor wat betreft de aard, ernst en de duur van de inbreuk is [VERTROUWELIJK] allereerst van mening dat deze inbreuk in de concrete omstandigheden van het geval geen significant risico voor de rechten van de betrokkenen inhoudt en geen afbreuk doet aan de essentie van de betrokken verplichting. [VERTROUWELIJK] heeft voor de verzameling en verwerking van de vingerafdrukken gebruik gemaakt van een professioneel bedrijf en een professioneel programma, waarbij de veiligheid van de gegevens gewaarborgd is en niet voor andere doeleinden is gebruikt. De betrokkenen hebben daarbij volgens [VERTROUWELIJK] ook geen schade geleden en zullen ook geen schade lijden, nu de betreffende gegevens inmiddels zijn vernietigd. Het aantal betrokkenen is daarnaast in deze beperkt volgens

[VERTROUWELIJK], nu het gaat om werknemers van [VERTROUWELIJK] in de periode januari 2017 tot november 2018. Direct na het eerste bezoek van de AP is [VERTROUWELIJK] gestopt met het verzamelen van vingerafdrukken en na het tweede bezoek in maart 2019, heeft [VERTROUWELIJK] ervoor gezorgd dat alle betreffende gegevens werden vernietigd. Overigens merkt [VERTROUWELIJK] voor wat betreft de duur nog op, dat de AP al op 5 juli 2018 (slechts een ruime maand nadat de AVG in werking is getreden) een melding heeft gekregen over de vingerscans. Het eerste onderzoek van de AP was pas op 6 november 2018 en het tweede onderzoek op 18 maart 2019. Indien [VERTROUWELIJK] eerder, dat wil zeggen, direct na de melding (toen de AVG net in werking was getreden), op de hoogte daarvan was gebracht, had zij eerder maatregelen kunnen nemen.

De AP volgt deze zienswijze van [VERTROUWELIJK] niet. [VERTROUWELIJK] had in dit geval moeten nalaten om de biometrische gegevens van haar werknemers te verwerken. Door dit wel te doen, heeft [VERTROUWELIJK] de essentie van deze verplichting geschonden. Doordat de werknemers van [VERTROUWELIJK] onvoldoende geïnformeerd waren over de verwerking en niet vast staat dat zij (in vrijheid) toestemming hebben gegeven, heeft [VERTROUWELIJK] met deze verwerking afbreuk gedaan aan de bescherming van de persoonsgegevens van haar werknemers. Gezien de aard, de ernst en de duur van de overtreding is er geen sprake van een kleine inbreuk[46], waardoor de AP het opleggen van een berisping onvoldoende doeltreffend, evenredig en afschrikkend acht. Dat de veiligheid van de gegevens daarbij gewaarborgd was doet daar niet aan af, omdat [VERTROUWELIJK] de biometrische gegevens sowieso niet had mogen verwerken. De AP is van mening dat er sprake is van een ernstige overtreding. Daarom acht de AP het opleggen van een bestuurlijke boete (wat zowel speciale als generale preventie ten doel heeft) in dit geval passend.

De AP vindt voorts deze overtreding van ruim tien maanden een inbreuk van structurele aard, waarbij de verwerking (het opgeslagen hebben van de gegevens) niet tot november 2018 voortduurde maar tot en met 16 april 2019. [VERTROUWELIJK] heeft de eigen verantwoordelijkheid om de AVG na te leven en die wordt niet ontnomen door de omstandigheid dat de toezichthouder een signaal over onrechtmatige verwerking heeft ontvangen en evenmin door de duur van het onderzoek van de AP.

Ten tweede is [VERTROUWELIJK] van oordeel dat van enig opzet geen sprake is geweest. Ten tijde van de aanschaf van de programmatuur voor de vingerscans (in 2016), gold nog de Wet Bescherming Persoonsgegevens. [VERTROUWELIJK] stelt bekend te zijn met de inwerkingtreding van de AVG op 25 mei 2018, maar verkeerde in de veronderstelling, dat wat zij deed, in overeenstemming was met de privacywetgeving, hetgeen haar ook steeds werd (en wordt) bevestigd door de leverancier.

De AP ziet, onder verwijzing naar paragraaf 4.3.2, op basis hiervan geen aanleiding af te zien van het opleggen van een bestuurlijke boete of het boetebedrag te verlagen. Zoals [VERTROUWELIJK] heeft verklaard was zij bekend met de inwerkingtreding van de AVG en had [VERTROUWELIJK] voldoende tijd om bijvoorbeeld juridisch advies in te winnen. Van een professionele partij als [VERTROUWELIJK] mag, mede gelet op de bijzondere aard van de persoonsgegevens, worden verwacht dat zij zich terdege van de voor haar geldende normen vergewist en deze naleeft. De AP merkt voorts op dat de overtreden

[46] Zie ook overweging 148 van de AVG.

verbodsbepaling van artikel 9, eerste lid, AVG geen opzet vereist als bestanddeel. Nu het hier gaat om een overtreding, is voor het opleggen van een bestuurlijke boete conform vaste rechtspraak niet vereist dat wordt aangetoond dat sprake is van opzet.[47] De AP mag verwijtbaarheid veronderstellen als het daderschap vaststaat.[48] Het daderschap staat niet ter discussie tussen de AP en [VERTROUWELIJK], zodat de verwijtbaarheid een gegeven is.

[VERTROUWELIJK] voert verder aan dat de betrokkenen geen schade hebben geleden en dat de biometrische gegevens beveiligd waren. Het systeem is zodanig ingericht, dat de privacy van de werknemers gewaarborgd is gebleven. De leverancier is ISO 9001 gecertificeerd en de subverwerker is ISO 9001, ISO 27007, 150 14001 en NEN 7510 gecertificeerd. Het door [VERTROUWELIJK] afgenomen product voldoet daarmee volgens [VERTROUWELIJK] aan de kwaliteitsnormen. Het gaat weliswaar om biometrische gegevens maar de code, die op basis van de vingerafdruk wordt gemaakt, is naar het oordeel van [VERTROUWELIJK] niet te herleiden naar een medewerker. Direct na het eerste bezoek van de AP heeft [VERTROUWELIJK] maatregelen genomen door te stoppen met het in/uit klokken door middel van vingerafdrukken en na het tweede bezoek van de AP zijn alle gegevens verwijderd.

De AP volgt de zienswijze van [VERTROUWELIJK] ook hierin niet. Zoals vermeld in paragraaf 3.1.2 is de AP van oordeel dat met de door [VERTROUWELIJK] opgeslagen gegevens natuurlijke personen, namelijk haar werknemers, konden worden geïdentificeerd. Dat de biometrische gegevens volgens [VERTROUWELIJK] goed beveiligd waren is in dit geval onvoldoende zwaarwegend, omdat de overtreding niet ziet op de beveiliging van de gegevens maar op het niet mogen verwerken ervan als zodanig. [VERTROUWELIJK] stelt verder weliswaar dat het in/uit klokken door middel van vingerafdrukken direct na het eerste bezoek van de AP is gestopt, maar dat maakt nog niet dat [VERTROUWELIJK] met de verwerking(en) was gestaakt. Immers, volgens artikel 4, tweede lid, van de AVG is een verwerking ook - zonder limitatief te zijn - het verzamelen, vastleggen, ordenen, structureren of het opgeslagen hebben van gegevens.

[VERTROUWELIJK] voert tot slot aan dat er geen sprake is van eerdere relevante inbreuken. [VERTROUWELIJK] heeft daarnaast steeds al haar medewerking verleend aan de AP en heeft de kwestie van meet af aan serieus opgenomen. [VERTROUWELIJK] merkt hierbij nog op, dat de AP op geen enkel moment in het traject sinds 6 november 2018, de indruk heeft gewekt dat zij mogelijk een boete zou opleggen en wat de hoogte daarvan kon zijn. Als [VERTROUWELIJK] hierop eerder door de AP was gewezen, dan had zij wel eerder advies ingewonnen en nog sneller maatregelen getroffen. Gezien het feit dat [VERTROUWELIJK] zich niet bewust was van een mogelijke inbreuk, heeft zij niet zelf een melding gedaan of contact opgezocht met de AP. [VERTROUWELIJK] voert afsluitend aan dat van enig financieel voordeel als gevolg van het gebruik van de vingerscans geen sprake is.

[47] vgl. College van Beroep voor het bedrijfsleven 29 oktober 2014, ECLI:NL:CBB:2014:395, rov. 3.5.4, 2 september 2015, ECLI:NL:CBB:2015:312, rov. 3.7 en 7 maart 2016, ECLI:NL:CBB:2016:54, rov. 8.3; Afdeling Bestuursrechtspraak van de Raad van State 29 augustus 2018, ECLI:NL:RVS:2018:2879, rov. 3.2 en 5 december 2018, ECLI:NL:RVS:2018:3969, rov. 5.1.
[48] *Kamerstukken II* 2003/04, 29 702, nr. 3, p. 134.

Ook hierin volgt de AP de zienswijze van [VERTROUWELIJK] niet. Ondanks dat de AP niet eerder dezelfde inbreuk heeft vastgesteld bij [VERTROUWELIJK] en er volgens [VERTROUWELIJK] geen sprake is van financieel voordeel, ziet de AP door de ernst van de overtreding en de verwijtbaarheid van [VERTROUWELIJK] geen aanleiding om af te zien van het opleggen van een bestuurlijke boete of om het boetebedrag te verlagen. De AP verwijst voor de motivering hiervan naar paragraaf 4.3.1 en 4.3.2. De AP is verder van oordeel dat de medewerking van [VERTROUWELIJK] niet verder is gegaan dan haar wettelijke plicht om te voldoen aan artikel 9, eerste lid, van de AVG. [VERTROUWELIJK] heeft daarmee niet op bijzondere wijze samengewerkt met de AP. Tot slot merkt de AP op dat zij tijdens de onderzoeksfase zich niet kan uiten over het handhavingsmiddel, omdat dan de feiten en het rapport nog worden onderzocht en vastgesteld. Zoals eerder vermeld, blijft het de eigen verantwoordelijkheid van [VERTROUWELIJK] om onderzoek te doen naar de geldende wetgeving en deze na te leven.

Concluderend ziet de AP in de zienswijze van [VERTROUWELIJK] geen aanleiding om af te zien van het opleggen van een bestuurlijke boete of om het boetebedrag te verlagen. De AP acht het boetebedrag van € 725.000,- evenredig en er zijn geen andere feiten en omstandigheden die nopen tot matiging van het voornoemde bedrag.

4.4 Conclusie

De AP stelt het totale boetebedrag vast op €725.000,-.

Datum
4 december 2019

Ons kenmerk
[VERTROUWELIJK]

5. Dictum

Boete

De AP legt aan [VERTROUWELIJK], wegens overtreding van artikel 9, eerste lid, van de AVG een bestuurlijke boete op ten bedrage van **€ 725.000,--** (zegge: zevenhonderdvijfentwintigduizend euro).[49]

Hoogachtend,
Autoriteit Persoonsgegevens,

w.g.

ir. M.J. Verdier
Vicevoorzitter

Rechtsmiddelenclausule
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje Bezwaar maken tegen een besluit, onderaan de pagina onder de kop Contact met de Autoriteit Persoonsgegevens. Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, postbus 93374, 2509 AJ Den Haag. Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.
Schrijf in uw bezwaarschrift ten minste:
- uw naam en adres;
- de datum van uw bezwaarschrift;
- het in deze brief genoemde kenmerk (zaaknummer); of een kopie van dit besluit bijvoegen;
- de reden(en) waarom u het niet eens bent met dit besluit;
- uw handtekening.

[49] De AP zal voornoemde vordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).