



Samenvatting onderzoek [VERTROUWELIJK]

De Autoriteit Persoonsgegevens (AP) heeft het bedrijf [VERTROUWELIJK] een boete opgelegd van 725.000 euro voor het onrechtmatig afnemen van vingerafdrukken van haar medewerkers en het gebruik van vingerscans. In deze samenvatting van het onderzoek leest u hoe de AP tot dit besluit is gekomen.

Aanleiding van het onderzoek

Op 5 juli 2018 heeft de AP een melding ontvangen dat bij [VERTROUWELIJK] werknemers verplicht zijn om hun vingerafdruk te laten scannen. [VERTROUWELIJK]. Uit de melding bleek dat werknemers bij [VERTROUWELIJK] met behulp van een vingerafdruk in- en uit moesten klokkken.

Naar aanleiding van dit signaal is de AP eind oktober 2018 een onderzoek gestart naar de naleving door [VERTROUWELIJK] van artikel 9 van de Algemene verordening gegevensbescherming (AVG). Dit artikel gaat onder meer over het verbod op de verwerking van biometrische gegevens, zoals een vingerafdruk. De AP heeft daarom onder meer een onderzoek ter plaatse bij [VERTROUWELIJK] verricht.

Waarom heeft de AP dit opgepakt?

Het waarborgen van de privacy van een individu is van groot belang bij de inzet van biometrie. Biometrische gegevens, zoals een vingerafdruk, zijn namelijk bijzondere persoonsgegevens in de zin van artikel 9 AVG. 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 mensen. Unieke lichaamskenmerken zoals een vingerafdruk zijn bovendien te herleiden naar één individu. Ook bevatten biometrische gegevens vaak meer informatie dan strikt noodzakelijk is voor bijvoorbeeld identificatie.

Het verwerken van biometrische persoonsgegevens verdient specifieke bescherming. Op grond van artikel 9 AVG is de verwerking van biometrische gegevens daarom verboden, tenzij een van de limitatief opgesomde uitzonderingen van artikel 9, lid 2, AVG zich voordoet.

Feitelijke bevindingen van het onderzoek

Volgens [VERTROUWELIJK] was de reden voor het invoeren van de vingerscanapparatuur het terugdringen van misbruik bij het in- en uitklokken. Daarnaast zouden er praktische voordelen zijn. Zoals het feit dat er geen kosten voor de medewerkers zijn voor de aanschaf, verlies of beschadiging van een 'druppel', waarmee ook in- en uitgeklokt kan worden bij [VERTROUWELIJK]. Andere redenen voor het invoeren van de vingerscanapparatuur waren dat dit systeem een sluitende aanwezigheidsregistratie biedt, dat het systeem met vingerscanners het verouderde systeem met druppelscanners moest vervangen en dat het in de toekomst veiligheidsrisico's zou kunnen adresseren.

[VERTROUWELIJK] gebruikt de vingerscansoftware voor aanwezigheids- en tijdregistratie en – op basis daarvan – voor de salarisadministratie. De druppels en de vingerscan kunnen naast elkaar worden gebruikt. Medewerkers zijn dus niet verplicht om met hun vingerafdruk in- of uit te klokkken.

Medewerkers hebben voor het inscannen van hun vingerafdruk van minimaal twee vingers afdrukken moeten afgeven. Na het vastleggen van de vingerafdruk zijn de templates van die vingerafdrukken opgeslagen als tekstbestand. Deze templates van vingerafdrukken zijn bewaard. Sinds de invoering van



het systeem in 2017 zijn van in totaal 337 werknemers vingerafdruktemplates opgeslagen en deze zijn niet verwijderd bij uitdiensttreding.

In de arbeidsovereenkomst was geen informatie opgenomen over het gebruik van vingerafdrukken. Medewerkers waren slechts via het personeelshandboek van juli 2017 geïnformeerd dat [VERTROUWELIJK] de intentie had om volledig met de vingerafdruk in te klokken. Voor veel medewerkers kwam het vastleggen van een vingerafdruk dan ook als een verrassing.

Verder beschikte [VERTROUWELIJK] niet over beleid, procedures of andere documentatie waarmee zij konden aantonen dat zij uitdrukkelijke toestemming vroegen voor het afnemen van vingerafdrukken en het gebruik van de vingerscans. Ook werd geen bewijs gevonden dat medewerkers hiervoor toestemming hadden gegeven of dit hadden geweigerd. Medewerkers tekenen slechts voor ontvangst van een druppel. Sommige medewerkers gaven aan dat het laten inscannen van de vingerafdruk verplicht was en er geen toestemming was gevraagd. Twee medewerkers hebben aangegeven dat zij mondeling toestemming hebben gegeven. Ook hebben enkele werknemers aangegeven 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 liet inscannen.

De vingerscanapparatuur was sinds begin 2017 actief bij [VERTROUWELIJK]. De eerste vingerafdruktemplates zijn vastgelegd en opgeslagen op 23 januari 2017. Vanaf dat moment zijn regelmatig templates opgeslagen. De laatste vastgelegde en opgeslagen vingerafdruktemplates van werknemers dateren van 8 november 2018. Van begin 2017 tot 25 mei 2018 zijn er van 250 werknemers vingerafdrukken vastgelegd en opgeslagen. In de periode na de invoering van de AVG (vanaf 25 mei 2018) tot 8 november 2018 zijn er van nog meer werknemers vingerafdrukken vastgelegd en opgeslagen. In totaal komt dat op 337 (voormalige) vingerafdrukken. Sinds 8 november 2018 is [VERTROUWELIJK] gestopt met het vastleggen en dus ook opslaan van de vingerafdrukken van nieuwe medewerkers.

Als een werknemer uit dienst gaat, worden zijn/haar gegevens en vingerafdruktemplates wel bewaard, maar geblokkeerd in het softwareprogramma. Op 18 maart 2019 heeft de AP geconstateerd dat de vingerafdruktemplates van medewerkers die hun vingerafdruk hebben laten vastleggen en die op dat moment in dienst waren, actief waren in het softwareprogramma en de scanstations, zodat zij met hun vingerafdruk konden in- en uitklokken. Deze templates van vingerafdrukken die sinds begin 2017 vastgelegd zijn, werden 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. [VERTROUWELIJK] heeft in ieder geval tot 16 april 2019 de vingerafdruktemplates van haar (voormalige) werknemers bewaard. Net daarna heeft [VERTROUWELIJK] de opgeslagen vingerafdruktemplates van al haar (voormalige) werknemers verwijderd uit de systemen en logbestanden als onderbouwing daarvoor verstrekt.

Beoordeling van de feiten

Volgens artikel 4, lid 14, AVG omvatten biometrische gegevens persoonsgegevens die onder andere het resultaat zijn van een specifieke technische bewerking van de fysieke kenmerken van een natuurlijke persoon. En op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd. Vingerafdrukgegevens worden daarbij expliciet genoemd als voorbeeld van biometrische gegevens.



Biometrische gegevens zijn op grond van artikel 9, lid 1, AVG bijzondere persoonsgegevens. De verwerking van bijzondere persoonsgegevens is op grond van artikel 9, lid 1, AVG in beginsel verboden. Het verbod is niet van toepassing als aan één van de in artikel 9, lid 2, AVG genoemde uitzonderingsgronden op het verwerkingsverbod is voldaan. De eerste voor deze casus relevante uitzondering is vermeld in artikel 9, lid 2, onder a, AVG. De tweede uitzonderingsmogelijkheid volgt uit artikel 9, lid 2, onder g, AVG wat verder is ingevuld door de Nederlandse wetgever in artikel 29 Uitvoeringswet AVG. Het betreft verwerkingen op grond van 'uitdrukkelijke toestemming' of die 'noodzakelijk voor authenticatie of beveiligingsdoeleinden' zijn.

Uitzondering: uitdrukkelijke toestemming

Op grond van artikel 4, onderdeel 11, AVG is toestemming een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee iemand met een verklaring of een ondubbelzinnige actieve handeling een verwerking van zijn/haar persoonsgegevens aanvaardt.

Uitdrukkelijke toestemming is vereist in bepaalde situaties waarin zich een ernstig risico voor gegevensbescherming voordoet. En waarbij een hoog niveau van individuele controle over persoonsgegevens passend is. De term 'uitdrukkelijk' verwijst naar de manier waarop toestemming door de betrokken personen is gegeven. Het betekent dat iemand een uitdrukkelijke verklaring van toestemming moet geven. Bijvoorbeeld schriftelijke toestemming, ondertekening, het versturen van een e-mail om toestemming te geven of toestemming met tweetrapsverificatie.

[VERTROUWELIJK] beschikte niet over beleid, procedures of andere documentatie waarmee zij konden aantonen dat zij uitdrukkelijke toestemming vroegen voor het afnemen van vingerafdrukken en het gebruik van de vingerscans. Ook werd geen bewijs gevonden dat medewerkers hiervoor toestemming hadden gegeven of dit hadden geweigerd. Werknemers zijn slechts via het personeelshandboek van juli 2017 geïnformeerd dat [VERTROUWELIJK] de intentie had om volledig met de vingerafdruk te gaan inklokken. Uit onderzoek van AP is gebleken dat het vastleggen van de vingerafdrukken niet was aangekondigd bij de medewerkers en dat zij hierover geen informatie hebben ontvangen. 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. [VERTROUWELIJK] heeft niet aangetoond dat haar werknemers voldoende geïnformeerd waren over de verwerking van de biometrische gegevens, noch dat haar werknemers (uitdrukkelijke) toestemming hebben gegeven voor de verwerking van hun biometrische gegevens.

Ook al zou er wel sprake zijn van toestemming, dan zou deze ook nog eens 'vrijelijk gegeven' moeten zijn. Dit betekent dat er geen dwang achter mag zitten of dat toestemming een voorwaarde is voor iets anders. Werknemers hebben echter aangegeven dat het scannen van de vingerafdruk verplicht was. Ook hebben enkele werknemers aangegeven 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 liet inscannen. Ondanks dat [VERTROUWELIJK] vindt dat er een keuzevrijheid voor werknemers was om al dan niet in- en uit te kloppen met behulp van hun vingerafdruk, hebben verschillende werknemers het als een verplichting ervaren om hun vingerafdruk te laten vastleggen. 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 kon verlenen. [VERTROUWELIJK] heeft bovendien niet aangetoond dat er in dit geval vrijelijk toestemming is verleend. Om deze reden wordt eventueel gegeven toestemming van de medewerkers van [VERTROUWELIJK] als niet vrijelijk gegeven beschouwd.



De uitzonderingsmogelijkheid uit artikel 9, lid 2, onder a, AVG op het verbod van verwerking van biometrische gegevens op basis van uitdrukkelijke toestemming van de betrokkene gaat in dit geval dus niet op.

Noodzakelijk voor authenticatie of beveiligingsdoeleinden

De verwerking van biometrische gegevens zou verder toegestaan kunnen zijn indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Daarvoor moet er een afweging worden gemaakt of identificatie door middel van biometrie noodzakelijk en proportioneel is voor authenticatie of beveiligingsdoeleinden. 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. Voor de werkzaamheden bij [VERTROUWELIJK], [VERTROUWELIJK], is de noodzaak van de beveiliging niet zodanig hoog dat werknemers met biometrie toegang moeten kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Daarnaast kunnen andere minder ingrijpende manieren, dit ook bewerkstelligen. [VERTROUWELIJK] kan zich wat betreft de verwerking van vingerafdrukken daarom niet beroepen op de uitzonderingsmogelijkheid van artikel 9, lid 2, onder g, AVG in samenhang met artikel 29 UAVG.

Het verwerken van vingerafdrukken zonder dat een van de limitatief opgesomde uitzonderingen van toepassing is, leidt tot een overtreding van artikel 9 AVG. Op grond van de bevindingen van het onderzoek wordt geconcludeerd dat bij [VERTROUWELIJK] bijzondere persoonsgegevens, namelijk biometrische gegevens, van medewerkers zijn verwerkt. Er is niet gebleken dat een van de uitzonderingsgronden in artikel 9, lid 2, AVG zich voordoet. Daarmee handelt [VERTROUWELIJK] in strijd met het verbod uit artikel 9, lid 1, AVG.

Sanctie

[VERTROUWELIJK] heeft van 25 mei 2018 tot en met 16 april 2019 het verbod van artikel 9, lid 1, AVG overtreden door biometrische gegevens van haar werknemers te verwerken. De AP legt voor deze overtreding aan [VERTROUWELIJK] een boete op van € 725.000,- op grond van artikel 58, lid 2, aanhef en onder i en artikel 83, lid 5, AVG, gelezen in samenhang met artikel 14 lid 3 UAVG.