



# DE AVG EN DE VERWERKING VAN BIOMETRISCHE GEGEVENS

Inge Bremmer, juridisch adviseur Nederland ICT

## INLEIDING

Als je persoonsgegevens verwerkt heb je daarvoor een doel en een grondslag nodig. Dat geldt ook voor het verwerken van biometrische gegevens, zoals bijvoorbeeld een irisscan of vingerafdruk. Verwerk je biometrische gegevens met het oog op de unieke identificatie van een persoon? Dus bijvoorbeeld voor toegangscontrole of tijdsregistratie. Dan verandert er met de komst van de Avg het één en ander op het punt van 'grondslag'.

Wij hebben gemerkt dat er veel onrust bestaat over de (on)mogelijkheden van biometrische gegevens onder de Avg, met name ook naar aanleiding van uitspraken van staatssecretaris Van Ark in antwoord op Kamervragen.

Kortgezegd stelt de staatssecretaris dat biometrie voor authenticatiedoeleinden straks niet meer mag. Dat is deels onjuist en bovendien veel te kort door de bocht.

Graag scheppen wij duidelijkheid over hoe biometrische gegevens ook na 25 mei 2018 gebruikt kunnen worden. Om goed te begrijpen wat er nu precies veranderd gaan we na de Kamervragen eerst kort in op hoe het nu geregeld is in de huidige privacywet (Wbp).

Tot slot gaan we dieper in op de diverse juridische mogelijkheden van het verwerken van biometrische gegevens onder de Avg.

## KAMERVragen BIOMETRIE

Recent werden door staatssecretaris Van Ark [Kamervragen beantwoord over kloksystemen op basis van vingerafdrukken](#). Ten onrechte wordt in de beantwoording gesteld dat in Nederland biometrische gegevens straks slechts nog mogen worden verwerkt als het gaat om "authenticatie vanwege beveiligingsdoeleinden" en dus niet voor authenticatiedoeleinden. In de wettelijke uitzondering staat niet "vanwege", maar "of". Het zijn twee separate grondslagen: "*verbod (...) niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden*".

Ook lijkt de staatssecretaris ervan uit te gaan dat biometrische gegevens door bedrijven worden opgeslagen. De meeste bedrijven slaan echter slechts een code op (een hash). Die code kan bij het aanbieden van de vingerafdruk opnieuw worden gemaakt om vervolgens naast de opgeslagen code te worden gehouden om te authentifieren. Andersom kan de code niet worden omgezet in een vingerafdruk of zelfs maar een deel daarvan. De biometrische gegevens worden over het algemeen dus zeer beperkt verwerkt (steeds alleen tijdens het scannen om de hash te genereren).

## ONDER DE WBP: GERECHTVAARDIGD BELANG

Onder de huidige privacywet (Wbp) worden biometrische gegevens niet gezien als “bijzondere persoonsgegevens”. Dat betekent dat je biometrische gegevens bijvoorbeeld mag verwerken met een gerechtvaardigd belang. Over de verwerking van biometrische gegevens in de verhouding werkgever/werknemer, waarbij de werknemer verplicht wordt om mee te werken, schrijft de Autoriteit Persoonsgegevens op haar website:

### ***Mag mijn werkgever mij verplichten een vingerafdruk af te staan?***

*Uw werkgever kan u vragen om een vingerafdruk te geven. Bijvoorbeeld voor toegangscontrole. Soms bent u verplicht uw vingerafdruk af te staan, soms niet. Dat hangt ervan af of uw werkgever een goede reden heeft (een zogeheten gerechtvaardigd belang). En of het echt nodig is om vingerafdrukken te gebruiken.*

### ***Gerechtvaardigd belang***

*Uw werkgever kan in bepaalde gevallen een gerechtvaardigd belang hebben om uw vingerafdruk te gebruiken om u te identificeren. Bijvoorbeeld als u met uw vingerafdruk toegang krijgt tot een plek met een hoog veiligheidsrisico.*

*Het gebruik van de vingerafdruk moet hiervoor dan wel noodzakelijk zijn. Dat wil zeggen dat uw werkgever het doel, in dit geval toegangscontrole, niet op een andere manier kan bereiken.*

*Is er een andere mogelijkheid, die minder ingrijpend is voor de privacy van de werknemers?*

*Bijvoorbeeld het gebruik van een toegangspas? Dat moet uw werkgever eerst nagaan. Alleen als uw werkgever het doel niet op een andere manier kan bereiken, is er sprake van noodzaak.*

## ONDER DE AVG VERBODEN TENZIJ

In de Avg worden “biometrische gegevens met het oog op de unieke identificatie van een persoon” gezien als ‘bijzondere persoonsgegevens’. Het verwerken van bijzondere persoonsgegevens is verboden, tenzij sprake is van een uitzondering.

Voor de praktijk betekent dit dat er een beperkter aantal ‘grondslagen’ (uitzonderingen) beschikbaar is. De belangrijkste daarvan voor de praktijk zijn: uitdrukkelijke toestemming en wettelijke grondslag. “Gerechtvaardigd belang” mag niet meer als grondslag worden gebruikt. Uitdrukkelijke toestemming wel en de wettelijke uitzondering dus ook.

## TENZIJ: TOESTEMMING

De Europese toezichthouders hebben een [opinie](#) geschreven over toestemming onder de Avg. Daarbij is ook aandacht voor toestemming in de relatie werkgever/werknemer.

In deze (Engelstalige) opinie schrijven de autoriteiten persoonsgegevens onder meer:

*However this does not mean that employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for the employer to demonstrate that consent actually is freely given. Given the imbalance of power between an employer and its staff members, employees can only give free consent in exceptional circumstances, when it will have no adverse consequences at all whether or not they give consent. 20 [Example 5] A film crew is going to be filming in a certain part of an office. The employer asks all the employees who sit in that area for their consent to be filmed, as they may appear in the background of the video. Those who do not want to be filmed are not penalised in any way but instead are given equivalent desks elsewhere in the building for the duration of the filming. (onderstreping toegevoegd)*

-----

Het voorbeeld dat hier wordt genoemd is filmen in een kantoor waarbij medewerkers de mogelijkheid wordt geboden tijdelijk op een andere plek plaats te nemen. Dat is zeer vergelijkbaar met bijvoorbeeld het aanbieden ter vrije keuze aan de medewerker van de mogelijkheid van een vingerafdrukscan, met daarnaast de mogelijkheid gebruik te maken van een pasje.

Kortom: werkgevers kunnen gewoon toestemming vragen voor de verwerking van de vingerafdruk, zolang zij daarnaast een redelijk alternatief bieden. Als je als werkgever gebruik maakt van toestemming, mag je werknemers dus niet verplichten tot gebruik biometrische gegevens (en zelfs niet de schijn daarvan wekken).

Maak je gebruik van toestemming? Dan moet de toestemming onder de Avg aan de volgende eisen voldoen. Dat geldt overigens niet alleen voor het verwerken van biometrische gegevens, maar voor alle verwerkingen van persoonsgegevens die je doet op basis van toestemming.

- Specifiek:

De werknemer geeft specifiek toestemming voor het verwerken van zijn biometrische gegeven voor een vooraf bepaald doel. Het mag niet lastig zijn is te onderscheiden waar nu eigenlijk toestemming voor wordt gegeven. De toestemming mag ook niet verstopt zitten in bijvoorbeeld in de arbeidsovereenkomst of andere voorwaarden.

- Vrij:

Er mogen geen negatieve consequenties zijn (bijvoorbeeld geen borgsom betalen, druk vanuit de leidinggevende, of andere drukmiddelen) en er moet op basis van vrije keuze een redelijk alternatief beschikbaar zijn (bijvoorbeeld gebruik van een pasje of wachtwoord).

- Op informatie berustend:

De persoon moet voldoende informatie krijgen in begrijpelijke taal over bijvoorbeeld waarvoor hij toestemming geeft, aan wie, met welke risico's en zijn recht om toestemming in te trekken.

- Ondubbelzinnig:

Iemand moet actief toestemming geven. Een vooraf aangevinkt vakje telt niet en je mag ook niet impliciet afleiden dat iemand vast wel toestemming bedoeld had te geven omdat hij bijvoorbeeld gebruik is gaan maken van de dienst.

Ook moet je als werkgever kunnen bewijzen dat de verkregen toestemming aan al deze eisen voldoet.

### TENZIJ: WETTELIJKE GRONDSLAG

Naast toestemming kan je dus ook verwerken op basis van een wettelijke grondslag. En die grondslag is in Nederland in de maak. Het wetsvoorstel is al aangenomen door de Tweede Kamer en de verwachting is dat het voor 25 mei 2018 (als de Avg van toepassing wordt) ook door de Eerste Kamer zal worden aangenomen.

De wettelijke uitzondering zoals die nu staat geformuleerd in de uitvoeringswet Avg:

*“Artikel 29. Uitzonderingen inzake biometrische gegevens*

*Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.”*

Kortom: straks geldt wat ook nu (onder de Wbp) de AP al op haar website aangeeft over het verplichten van werknemers tot het geven van hun vingerafdruk: er moet sprake zijn van een “noodzaak”. Die noodzaak is straks dan nog wel beperkt tot beveiliging of authenticatie, maar dat is ook precies waar de verwerking van biometrische gegevens zich doorgaans op richt.