BIOMETRISCHE GEGEVENS: AANBEVELING BETREFFENDE DE VERWERKING VAN BIOMETRISCHE GEGEVENS

written by Eva Dierckx | augustus 16, 2023

Steeds vaker worden biometrische gegevens gebruikt voor allerhande doeleinden. Denk maar aan het scannen van een vingerafdruk van een werknemer om toegang te kunnen krijgen tot een kantoorgebouw[1] of, verregaander, het scannen van gezichten om op die manier hun aankoopgedrag te monitoren.[2] Uiteraard zijn dit verregaande verwerkingen die niet zomaar mogen worden gedaan onder de GDPR. Daarom lichten wij toe waaraan, volgens de Gegevensbeschermingsautoriteit, voldaan moet zijn om biometrische gegevens op een correcte manier te verwerken.

Wat?

In eerste plaats dient vastgesteld te worden wat biometrische gegevens juist zijn. De GDPR definieert het begrip in art. 4.14 als volgt:

Biometrische gegevens: *"Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedrag gerelateerde kernmerken van een natuurlijk persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens."*

Met het geven van de twee voorbeelden op het einde, geeft de GDPR meteen ook de meest gekende, en begrijpelijke vormen van biometrische gegevens weer, namelijk gezichtsafbeeldingen en vingerafdruk gegevens.

De GDPR deelt de biometrische gegevens in twee categorieën in:

- Fysieke, of ook wel lichamelijke kenmerken;
- Gedragsgerelateerde kenmerken

Fysieke kenmerken zijn zeer eenvoudig. Dit zijn namelijk de fysische of fysiologische eigenschappen van een persoon, zoals gezichtsinformatie, irisscans, vingerafdrukken…

Gedragsgerelateerde kenmerken zijn moeilijker te omschrijven. De technologie staat niet stil waardoor dit in de toekomst waarschijnlijk beter uitgewerkt en vaker van toepassing zal zijn.

Een reeds bestaand voorbeeld hiervan is de identificatie aan de hand van het unieke stappatroon van personen.

Hoe?

Verwerking

Biometrische gegevens worden in twee verschillende fasen verwerkt, namelijk de inzamelingsfase en de vergelijkingsfase.

De inzamelingsfases bestaan uit twee delen:

- De eerste inzamelingsfase: hierbij wordt de referentie-informatie (bijvoorbeeld een vingerafdruk) geregistreerd. Deze informatie wordt omgezet in een template. Dit template zorgt ervoor dat in de toekomst verwerkte gegevens geverifieerd kunnen worden ten opzichte van de referentie-informatie.
- De tweede inzamelingsfase: de gegevens worden verwerkt en vergeleken met de template. Indien deze overeenstemmen oordeelt het systeem dat dit dezelfde persoon is als wie de referentie-informatie verwerkt werd (bijvoorbeeld de vingerafdruk komt overeen met deze in het systeem).

De tweede fase is de vergelijkingsfase. Hierbij wordt de ingezamelde informatie vergeleken met alle biometrische informatie die beschikbaar is in het systeem. Op deze manier kan de gebruiker geïdentificeerd worden tussen alle geregistreerde personen.

Opslag van gegevens

Er zijn drie manieren om biometrische informatie op te slaan:

- Type 1: Beheer van het template door de betrokkene zelf. De betrokkene bewaart de template waarbij er geen koppeling mogelijk is met andere informaticasystemen. Dit kan bijvoorbeeld een badge zijn om toegang te krijgen tot een gebouw. Dit is de werkwijze die principieel aangewend dient te worden. Er kan slechts zeer uitzonderlijk van afgeweken worden.
- Type 2: Gedeeld beheer. Er is een centrale template databank die door de verwerkingsverantwoordelijke beheerd wordt zonder dat deze er gebruik van kan maken zonder toestemming van de betrokkene.
- Type 3: exclusief beheer door de verwerkingsverantwoordelijke. Dit is de meest verregaande optie. Hiervoor dienen dan ook de meest strenge voorwaarden in acht genomen te worden.

Rechtsgrond

Voor het verwerken van biometrische gegevens is het belangrijk dat er, net zoals bij iedere verwerking, een rechtsgrond is op basis waarvan de gegevens verwerk worden.

In de praktijk zal de rechtsgrond meestal de uitdrukkelijk toestemming van de betrokkene zijn. Hierbij is het zeer belangrijk dat de toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig wordt gegeven.

In uitzonderlijke gevallen zal de rechtsgrond het zwaarwegend algemeen belang zijn. Dit dient echter zeer restrictief toegepast te worden. Enkel wanneer het gebruik van biometrische gegevens onvermijdelijk is, zal er hiervan sprake kunnen zijn indien dit bij wet voorzien wordt.

Algemeen

Net zoals bij iedere verwerking zijn ook de volgende algemene zaken belangrijk:

- Doelbinding;
- Proportionaliteit;
- Beveiliging;
- Opslagbeperking;
- Transparantieverplichting;

Gegevensbeschermingseffectbeoordeling

In geval er sprake is van een verwerking van biometrische gegevens met oog op de unieke identificatie van personen in een privéruimte die toegankelijk is voor het publiek of in een openbare ruimte, zal er steeds een gegevensbeschermingseffectbeoordeling moeten worden uitgevoerd. Het is dan

ook aangeraden, gelet op het inherente risico voor de rechten en vrijheden van de betrokkenen dat komt kijken bij het verwerken van biometrische gegevens om een gegevenseffectenberschermingsbeoordeling uit te voeren omdat het uitlaten hiervan slechts in uitzonderlijke gevallen gerechtvaardigd zal zijn.[3]

Besluit

Voor het verwerken van biometrische gegevens zal men dus steeds de beschermingsregels van de GDPR in acht moeten houden.

Indien u na het lezen van dit artikel vragen hebt omtrent de verwerking van biometrische gegevens, of de verwerking van persoonsgegevens in het algemeen, kan u contact opnemen via gdpr@studio-legale.be of op 03 216 70 70.

Gebruikte bronnen

Juridische bronnen:

- Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;
- Aanbeveling Gegevensbeschermingsautoriteit betreffende de verwerking van biometrische gegevens;
- Beslissing 01/2019 van 16 januari 2019 van de Gegevensbeschermingsautoriteit.

Nieuws:

- CARDINAELS, “Privacywaakhond dreigt met onderzoek naar Carrefour”, https://www.tijd.be/ondernemen/retail/privacywaakhond-dreigt-met-onderzoek-naar-carrefour/10198789.html.

[1] Autoriteit Persoonsgegevens, “Boete voor bedrijf voor verwerken vingerafdrukken werknemers, 30 april 2020, https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers.

[2] X., “Face Recognition in retail”, https://www.raydiant.com/blog/everything-about-facial-recognition-in-retail

[3] Punt 6 van beslissing nr. 01/2019 van de gegevensbeschermingsautoriteit; Aanbeveling Gegevensbeschermingsautoriteit betreffende de verwerking van biometrische gegevens, 36-37,

https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.01-2021-van-1-december-2021.pdf