



AUTORITEIT
PERSOONSGEGEVENS

Handreiking

Scraping door particulieren en private organisaties



Inhoudsopgave

Samenvatting	3
1. Inleiding	4
Privacyrisico's van scraping	4
Waar gaan deze richtlijnen over?	5
2. Wat is scraping?	5
Scraping en web crawling	5
Scraping, AI en algoritmes	6
3. AVG wel/niet van toepassing	6
Huishoudelijke exceptie	7
Territoriaal toepassingsgebied	7
4. AVG-beginselen	9
5. Beginsel van rechtmatigheid	10
Rechtsgrond voor de verwerking	10
Voorwaarden voor de grondslag gerechtvaardigd belang	12
Beoordeling grondslag gerechtvaardigd belang: mee te wegen kenmerken van scraping	14
6. Bijzondere persoonsgegevens	18
Voorwaarden voor het verwerken van bijzondere persoonsgegevens	19
7. Persoonsgegevens van strafrechtelijke aard	21
8. Samenvatting rechtmatigheid en voorbeelden	22
9. DPIA & voorafgaande raadpleging	24
10. Het gebruik van scraping voor het trainen van algoritmes	24
11. Conclusie	25



Samenvatting

Scraping is het geautomatiseerde proces waarmee informatie van websites kan worden verzameld en opgeslagen. Als bij scraping (ook) persoonsgegevens worden verzameld – wat al snel het geval zal zijn – is vrijwel altijd de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat organisaties of particulieren die scraping of gescrapete gegevens willen gebruiken, zich aan de regels van de AVG moeten houden.

De Autoriteit Persoonsgegevens (AP) ziet de ontwikkeling van scrapingtechnieken op zichzelf niet als iets negatiefs. Wel kleven er aan scraping al snel grote privacyrisico's. Zo kunnen met scraping in korte tijd heel veel persoonsgegevens van heel veel mensen worden verzameld en opgeslagen. De informatie die bij het scrapen wordt vastgelegd, kan bovendien over tal van aspecten van iemands leven gaan. Ook kan de informatie allerlei gevoelige persoonsgegevens bevatten. Daarom zal het in veel gevallen niet zijn toegestaan om scraping of gescrapete persoonsgegevens te gebruiken.

De risico's van scraping zijn afhankelijk van de manier waarop (persoons)gegevens worden gescrapet, en voor welk doel de gescrapete gegevens worden gebruikt. Organisaties en particulieren die scraping of gescrapete gegevens willen gebruiken, zullen heel goed moeten nagaan of de verwerking die zij op het oog hebben rechtmatig (volgens de wet) is. Hieraan moeten zij al vanaf de ontwikkelfase voldoende aandacht besteden ('privacy by design').

Deze richtlijnen voor scraping zijn bedoeld om private organisaties en particulieren houvast te geven bij het beantwoorden van de vraag of zij gebruik mogen maken van scraping of gescrapete gegevens. De richtlijnen besteden in het bijzonder aandacht aan het AVG-beginsel van rechtmatigheid. Een belangrijk onderdeel van dit beginsel is dat voor elke verwerking van persoonsgegevens een rechtsgrond (grondslag) nodig is in de zin van artikel 6 AVG.

Wilt u als private organisatie of particulier gebruikmaken van scraping of van gescrapete gegevens, dan kunt u zich waarschijnlijk alleen eventueel beroepen op de grondslag 'gerechtvaardigd belang'. Deze grondslag heeft u óók nodig als u alleen informatie verzamelt die al op internet staat en die voor iedereen openbaar toegankelijk is. En ook als u de persoonsgegevens direct na het verzamelen uit de database verwijdert.

We bespreken welke factoren u in elk geval moet meewegen bij de beoordeling of u zich kunt beroepen op de grondslag gerechtvaardigd belang. De specifieke kenmerken van scraping maken het vaak lastig of zelfs onmogelijk om te voldoen aan de voorwaarden voor deze grondslag. Dit is uiteraard afhankelijk van de manier waarop u de verwerking inricht, het doel waarvoor u persoonsgegevens verwerkt en de waarborgen die u treft om de belangen van de betrokkenen (de mensen van wie u gegevens verwerkt) te beschermen.

Bij scraping zult u ook vaak bijzondere en/of strafrechtelijke persoonsgegevens tegenkomen, ook als dat helemaal niet uw bedoeling is. Deze soorten persoonsgegevens krijgen extra bescherming in de AVG. Als private organisatie of particulier zult u bij scraping meestal geen bijzondere of strafrechtelijke persoonsgegevens mogen verwerken. In de praktijk zal het echter vaak lastig zijn om te voorkomen dat u met scraping (ook) bijzondere en/of strafrechtelijke persoonsgegevens verwerkt. Meestal betekent dit dat u dan helemaal niet mag scrapen en/of gescrapete gegevens mag gebruiken.



1. Inleiding

Scraping is kort gezegd het geautomatiseerd verzamelen en vastleggen van informatie van webpagina's¹ (zie verder hoofdstuk 2). Organisaties gebruiken scraping voor verschillende doelen. Bijvoorbeeld om:

- informatie te verzamelen om algoritmes mee te trainen;
- vragen en klachten van (potentiële) klanten van een organisatie te verzamelen, via online kanalen zoals sociale media en reviewsites;
- online berichten over een organisatie te monitoren, zodat de organisatie daarop kan reageren voor reputatiemanagement, sales of marketing.

Deze toepassingen van scraping worden vaak als (commerciële) diensten aangeboden aan derden. Maar organisaties kunnen ook voor zichzelf scrapers inzetten. Bijvoorbeeld om hun commerciële doelen te bereiken.

Voor alle vormen van scraping geldt: zodra er persoonsgegevens² bij betrokken zijn, is (op enkele uitzonderingen na) de Algemene verordening gegevensbescherming (AVG) van toepassing.

Privacyrisico's van scraping

De Autoriteit Persoonsgegevens (AP) ziet de ontwikkeling van scrapingtechnieken op zichzelf niet als iets negatiefs. Maar scraping brengt wel verschillende privacyrisico's met zich mee. Zo kunnen met scraping in korte tijd heel veel persoonsgegevens van heel veel mensen worden verzameld en vastgelegd. De informatie die bij het scrapen wordt vastgelegd, kan bovendien over tal van aspecten van iemands leven gaan. Ook kan de informatie allerlei gevoelige en bijzondere persoonsgegevens bevatten.

Daarnaast is het zo dat betrokkenen³ vaak maar weinig kunnen doen om scraping van hun persoonsgegevens tegen te gaan. Bijvoorbeeld omdat zij niet op de hoogte zijn van de scraping. Maar ook omdat het lastig is om informatie die eenmaal op internet staat, te verwijderen of af te schermen voor scraping.

Ook bij het gebruik van algoritmes zijn er risico's. Zijn die algoritmes gebaseerd op gescrapete gegevens? Dan kan dat soms tot gevolg hebben dat niet alleen het grondrecht op bescherming van persoonsgegevens, maar ook andere grondrechten in het geding komen. Dit kan bijvoorbeeld leiden tot discriminatie.

Deze en andere factoren maken dat het vaak lastig of zelfs onmogelijk is om aan de eisen van de AVG te voldoen bij het gebruik van scraping of gescrapete persoonsgegevens. Dit is uiteraard afhankelijk van de manier waarop de verwerking is ingericht, van het doel waarvoor persoonsgegevens worden verwerkt en van de waarborgen die worden getroffen om de belangen van de betrokkenen te beschermen.

¹ Deze richtlijnen richten zich op scraping van gegevens van internet en niet op scraping van gegevens uit offline gegevensbestanden.

² Artikel 4 onder 1 AVG.

³ Artikel 4 onder 1 AVG.



Waar gaan deze richtlijnen over?

Deze richtlijnen gaan in op de juridische mogelijkheden voor het gebruik van scraping door private organisaties en particulieren. De richtlijnen zijn bedoeld als hulpmiddel om te beoordelen of de verwerking die zij voor ogen hebben, is toegestaan op grond van de AVG. De richtlijnen gaan niet over de mogelijkheden voor het gebruik van scraping door overheidsorganisaties. Ook gaan de richtlijnen niet over de vraag of scraping is toegestaan op grond van andere regels dan de AVG, zoals wetgeving op het gebied van auteursrecht, of de voorwaarden die organisaties stellen aan het gebruik van hun website.

De richtlijnen gaan vooral in op het AVG-beginsel van rechtmatigheid. Een belangrijk onderdeel van dit beginsel is dat voor elke verwerking van persoonsgegevens een grondslag nodig is in de zin van artikel 6 AVG.⁴

Private organisaties en particulieren die gebruik willen maken van scraping of van gescrapete gegevens, kunnen zich waarschijnlijk alleen eventueel beroepen op de grondslag 'gerechtvaardigd belang' (artikel 6 lid 1 onder f AVG). Deze richtlijnen gaan onder andere in op de factoren die private organisaties en particulieren in elk geval moeten meewegen bij de beoordeling of zij zich kunnen beroepen op deze grondslag. Daarnaast gaan de richtlijnen in op het verwerken van bijzondere en strafrechtelijke persoonsgegevens bij het gebruik van scraping of gescrapete persoonsgegevens, waarvoor de AVG strengere regels kent dan voor 'gewone' persoonsgegevens.

2. Wat is scraping?

Met een internetverbinding kunnen internetgebruikers informatie opvragen bij servers, waaronder websites. Dit gebeurt (achter de schermen) door een GET-request (ophaalverzoek) te versturen naar de bestemming. Deze bestemming kan onder andere een website zijn. Die wordt gekenmerkt door een URL (uniform resource locator), zoals www.autoriteitpersoonsgegevens.nl.

Vervolgens verstrekt de bevraagde server de opgevraagde informatie, eventueel binnen bepaalde voorwaarden (zoals meegezonden gebruikersnaam en wachtwoord). Die informatie kan een webpagina zijn, maar ook een document of andere data. Dit proces kan ook geautomatiseerd worden. Het proces waarbij informatie geautomatiseerd wordt vastgelegd, wordt 'scraping' genoemd.

Wat is nu het verschil tussen het gebruik van een internetzoekmachine, zoals Google, en het gebruik van een scrapingtool, zoals bedoeld in deze richtlijnen? Dat is dat het bij scraping niet alleen gaat om het doorzoeken van internet met een bepaalde zoekterm, maar om het verzamelen en vastleggen van de doorzochte informatie in een database om de gegevens vervolgens te verwerken voor een bepaald doel.

Scraping en web crawling

Soms wordt onderscheid gemaakt tussen scraping en web crawling. In deze richtlijnen gebruiken we meestal het woord 'scraping', maar daaronder verstaan we ook web crawling.

⁴ De AVG is niet altijd van toepassing op scraping. Als de AVG niet van toepassing is, geldt niet de eis van een grondslag in de zin van artikel 6 AVG. Zie verder in hoofdstuk 3.



Voor het onderscheid tussen scraping en web crawling is van belang hoe wordt bepaald van welke URL's informatie wordt verzameld. Is er sprake van een (vooraf) vastgestelde lijst van URL's, bijvoorbeeld alleen de websites van nationale kranten? Dan wordt dat proces scrapen genoemd. Wanneer de lijst van te verwerken URL's dynamisch wordt aangepast, dan heet het web crawling.

Een web crawler (of kortweg crawler) updatet de lijst met te bezoeken URL's geautomatiseerd. Dit gebeurt met spiders (kleine programmaatjes). Spiders krijgen van te voren een bepaalde instructie mee. Zoals: voeg alle URL's die je tegenkomt tijdens het crawlen toe aan de lijst van te bezoeken URL's. De opdrachten kunnen echter ook worden gebruikt om de lijst met te bezoeken URL's te beperken. Bijvoorbeeld met de instructie: volg alle links, zolang je maar binnen de domeinnaam autoriteitpersoonsgegevens.nl blijft.

Een enkele crawler kan meerdere spiders managen, die elk hun eigen taak uitvoeren. Daardoor kan een crawler gelijktijdig meerdere opdrachten uitvoeren. Afhankelijk van de instructies die spiders meekrijgen, kan het gebeuren dat met slechts een handjevol 'start-URL's' toch een groot deel van het internet wordt doorzocht. Bij crawlen, waarbij de lijst met te bezoeken URL's dus tijdens het proces dynamisch wordt aangepast, is de kans vaak extra groot dat je vooraf niet weet welke gegevens zullen worden verwerkt.

Scraping, AI en algoritmes

Bij het trainen van artificiële intelligentie (AI) en algoritmes wordt scraping vaak gebruikt om trainingsdata te verzamelen. Bijvoorbeeld voor het trainen van large language models (LLM's), zoals Chat-GPT. Daarom zie je vaak dat scraping en het trainen van AI-modellen in een adem worden genoemd. Maar het trainen van AI-modellen kan ook zonder scraping plaatsvinden. En andersom wordt scraping ook voor andere doelen gebruikt dan het trainen van algoritmes.

3. AVG wel/niet van toepassing

Bij het scrapen van persoonsgegevens moet u normaal gesproken voldoen aan de AVG.⁵ Dit betekent onder andere dat u een rechtsgrond (grondslag) als bedoeld in artikel 6 AVG nodig heeft voor het verwerken van persoonsgegevens.

In sommige gevallen is de AVG echter niet van toepassing.⁶ U moet zelf nagaan of de AVG van toepassing is op uw verwerking. Daarbij moet u in het achterhoofd houden dat de AVG een hoog beschermingsniveau toekent aan de betrokkenen. Daardoor mag u de uitzonderingen op de AVG niet ruim uitleggen.⁷

⁵ Mogelijk moet u naast de AVG met andere juridische kaders rekening houden als u scraping wilt inzetten. Bijvoorbeeld het auteursrecht of andere intellectuele-eigendomsrechten. Of dat websites in de algemene voorwaarden hebben opgenomen dat het scrapen van hun webpagina's niet is toegestaan. De Autoriteit Persoonsgegevens houdt geen toezicht op de naleving van deze regels. Hiervoor zijn andere toezichthouders aangewezen en/of geldt civiele rechtsbescherming.

⁶ Zie artikel 2 en 3 AVG. We bespreken hier alleen de uitzondering genoemd in artikel 2 lid 2 onder c AVG (de huishoudelijke exceptie) en in artikel 3 AVG (het territoriaal toepassingsgebied).

⁷ HvJ EU C-272/19, 9 juli 2020, [ECLI:EU:C:2020:535](#) (*Land Hessen*), § 68 en HvJ EU C-645/19, 15 juni 2021, [ECLI:EU:C:2021:483](#) (*Facebook Ireland/Gegevensbeschermingsautoriteit*), § 91.



In dit hoofdstuk bespreken we twee onderwerpen die te maken hebben met de toepasselijkheid van de AVG: (1) de huishoudelijke exceptie en (2) het territoriaal toepassingsgebied van de AVG.

Huishoudelijke exceptie

Verzamelt u als particulier voor uzelf persoonsgegevens uit open bronnen, zoals internet? Dan mag u deze persoonsgegevens voor 'persoonlijke of huishoudelijke doeleinden' gebruiken. Dit betekent dat u de gegevens alleen privé gebruikt en dus niet voor professionele of commerciële doeleinden. U mag de gescrapete gegevens vervolgens alleen zelf gebruiken. U mag de gegevens niet delen met anderen, behalve met een beperkte groep mensen. Zoals familieleden of vrienden.

Als u aan deze voorwaarden voldoet, kunt u als particulier gebruikmaken van een scraper die online voor u op zoek gaat naar informatie en deze informatie voor u opslaat. De AVG is in dat geval niet op u van toepassing.

Heeft u een hobbyproject dat u privé ontwikkelt en deelt met slechts een klein aantal vrienden? Dan kunt u dus gebruikmaken van scraping waarbij persoonsgegevens worden verwerkt, zolang u hierbij geen commercieel doel heeft. Let er hierbij wel op dat u de met het scrapen verzamelde data niet openbaar publiceert, ook niet in de vorm van een publieke repository, zoals op Github.

Territoriaal toepassingsgebied

De AVG is niet alleen van toepassing op Europese organisaties. In de AVG is bepaald dat onder omstandigheden ook organisaties van buiten de Europese Unie (EU) zich aan de AVG moeten houden bij het verwerken van persoonsgegevens.⁸

In twee situaties is de AVG ook van toepassing op organisaties die buiten de EU gevestigd zijn:

1. Als een organisatie goederen of diensten aanbiedt aan betrokkenen binnen de EU.
2. Als een organisatie het gedrag van betrokkenen binnen de EU monitort.

Goederen en diensten binnen de EU

Besluit een buiten de EU gevestigde organisatie om goederen of diensten aan te bieden aan burgers binnen de EU? Dan moet deze organisatie zich aan de AVG houden, ongeacht of voor deze goederen of diensten moet worden betaald.⁹ Bijvoorbeeld een Amerikaanse webshop die (ook) producten in de EU wil leveren of een Braziliaanse videostreamingdienst die (ook) in Nederland films gaat aanbieden.

Een kanttekening hierbij is dat het enkele feit dat de website van een buiten de EU gevestigde organisatie raadpleegbaar is binnen de EU, onvoldoende is om aan te nemen dat deze organisatie ook goederen of diensten aanbiedt in de EU.¹⁰ Om te bepalen of de AVG van toepassing is, is een afweging van alle omstandigheden noodzakelijk. Is het bijvoorbeeld mogelijk om als bezorgadres een adres binnen de EU te

⁸ Artikel 3 lid 2 AVG. Zie ook: [Boete van 525.000 euro voor Locatfamily.com | Autoriteit Persoonsgegevens](#).

⁹ Artikel 3 lid 2 onder a AVG.

¹⁰ Zie overweging 23 van de AVG.



gebruiken? Of kan er in euro's worden betaald?¹¹ Dat kunnen indicatoren zijn dat een organisatie diensten of goederen binnen de EU aanbiedt.

Monitoring van Europese burgers

De tweede categorie van verwerkingen waarbij ook organisaties van buiten de EU zich aan de AVG moeten houden, is het verwerken van persoonsgegevens waarbij zo'n organisatie het gedrag van mensen binnen de EU monitort.¹² Hierna leggen we uit wanneer dit het geval kan zijn bij scraping. Let op: dit is geen uitputtende beschrijving. Er kunnen dus ook andere relevante factoren op uw situatie van toepassing zijn.

Allereerst is belangrijk om te vermelden dat het niet uitmaakt of de organisatie 'monitoren van gedrag' tot doel heeft of niet. Uit de Guidelines 3/2018 van de EDPB blijkt dat het gaat om de vraag of een organisatie een specifiek doel heeft met het verwerken van de gegevens over iemands gedrag en met het opstellen van een profiel van die persoon.¹³ Het enkele feit dat een organisatie gegevens over iemand verzamelt, betekent dus niet automatisch dat de organisatie ook gedrag monitort.¹⁴

Om te bepalen of scraping als monitoring van gedrag moet worden gezien, moeten we dus kijken naar het doel waarvoor scraping wordt ingezet. Gebruikt een organisatie scraping bijvoorbeeld om informatie over het gedrag van personen (binnen de EU) te verzamelen om hun vervolgens (meer) gepersonaliseerde diensten of advertenties aan te bieden? Dan moet de verwerking voldoen aan de AVG. Ook als de verwerkingsverantwoordelijke gevestigd is buiten de EU.

Is het doel van scraping om een algoritme te trainen waarmee gebruikers buiten de EU afbeeldingen of computercode kunnen genereren? Dan valt dat in beginsel niet onder de definitie van monitoring, zoals bedoeld in artikel 3 lid 2 onder b AVG. In dat geval is de AVG niet van toepassing als de verwerkingsverantwoordelijke buiten de EU gevestigd is (en ook geen goederen of diensten aanbiedt binnen de EU).

Om te kunnen spreken over monitoring van gedrag van betrokkenen binnen de EU, is het niet noodzakelijk dat een organisatie zich bewust is van de nationaliteit of locatie van een betrokkene. Verwerkingen kunnen dus ook onder de AVG vallen als een organisatie, zonder dit zelf te weten, (ook) persoonsgegevens van mensen binnen de EU verzamelt. Bijvoorbeeld als de organisatie geen (geografisch) filter toepast op de te verzamelen data. Het ligt voor de hand dat wanneer een organisatie persoonsgegevens van .nl-websites of .eu-websites scrapet, de organisatie (ook) persoonsgegevens van mensen binnen de EU verzamelt.

Let op: verzamelt een organisatie eerst data en filtert de organisatie die pas daarna? Dan verwerkt de organisatie waarschijnlijk persoonsgegevens van mensen binnen de EU en is de AVG dus van toepassing. Het is dus van belang om het geografische filter toe te passen op de te bezoeken URL's, niet op de daarna

¹¹ Zie voor een aantal andere factoren [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\) - version adopted after public consultation | European Data Protection Board \(europa.eu\)](#), p. 19 e.v.

¹² Artikel 3 lid 2 onder b AVG.

¹³ [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\) - version adopted after public consultation | European Data Protection Board \(europa.eu\)](#), p. 22.

¹⁴ [Guidelines 3/2018 on the territorial scope of the GDPR \(Article 3\) - version adopted after public consultation | European Data Protection Board \(europa.eu\)](#), p. 22.



verzamelde data. Dit kan bijvoorbeeld door een beperkt aantal top level domains (TLD) te scrapen.¹⁵ Dit is echter geen waterdichte methode om te voorkomen dat persoonsgegevens van personen binnen de EU worden verzameld. Veel Europese betrokkenen zijn namelijk ook actief op internationale websites, bijvoorbeeld met een '.com'-TLD.

Samengevat

Als een organisatie alle (of zoveel mogelijk) websites op het internet scrapet, is het vrijwel ondenkbaar dat de organisatie geen persoonsgegevens van betrokkenen binnen de EU verwerkt. In dat geval kan dus de AVG van toepassing zijn, ook als de verwerkingsverantwoordelijke buiten de EU gevestigd is. Namelijk in een van de twee eerder beschreven situaties: 1) het aanbieden van goederen of diensten aan betrokkenen in de EU of 2) het monitoren van gedrag dat plaatsvindt binnen de EU.

4. AVG-beginselen

Als u informatie scrapet van internet, scrapet u daarbij vrijwel altijd ook persoonsgegevens. Daarom moet u, als geen sprake is van een uitzondering, bij het scrapen van informatie op internet voldoen aan de AVG. U moet al vanaf de ontwikkelfase voldoende aandacht besteden aan de regels uit de AVG. Dit noemen we privacy by design.

In artikel 5 lid 1 AVG is opgenomen aan welke beginselen verwerkingen van persoonsgegevens moeten voldoen. Dit zijn de beginselen van:

- rechtmatigheid, behoorlijkheid en transparantie;
- doelbinding;
- minimale gegevensverwerking (dataminimalisatie);
- juistheid;
- opslagbeperking;
- integriteit en vertrouwelijkheid.

Alle organisaties die persoonsgegevens verwerken, moet zich aan deze beginselen houden. En moeten kunnen aantonen dat zij zich aan deze beginselen houden. Dat is de verantwoordingsplicht.¹⁶

Verwerkt u persoonsgegevens doordat u scraping inzet? Of verwerkt u gescrapete persoonsgegevens? Dan moet u voldoen aan de eisen die de AVG aan de verwerking van persoonsgegevens stelt. Scraping heeft echter verschillende kenmerken die het lastig kunnen maken om aan al de beginselen van artikel 5 AVG te voldoen.

Bijvoorbeeld:

¹⁵ Het TLD is het laatste deel van een domeinnaam, dus bijvoorbeeld '.eu' of '.nl'.

¹⁶ Artikel 5 lid 2 AVG.



- **Transparantie:** |Het kan bij scraping moeilijk zijn om de betrokkene op een effectieve manier te informeren. Dit kan (onder andere) botsen met het transparantiebeginsel.¹⁷
- **Minimale gegevensverwerking:** Een ander risico van scraping is dat u (veel) gegevens verwerkt die niet nodig zijn voor het doel van uw verwerking. Dat botst met het beginsel van minimale gegevensverwerking.¹⁸
- **Juistheid:** Het beginsel van juistheid houdt in dat de persoonsgegevens die u verwerkt, juist moeten zijn en dat u die zo nodig actualiseert.¹⁹ Verwerkt u met scraping (veel) gegevens, die zijn verkregen uit (veel) verschillende bronnen? Dan kunt u zich waarschijnlijk moeilijk of zelfs helemaal niet een oordeel vormen over de juistheid van de gegevens. De juistheid kan verder onder druk komen te staan als de gescrapete persoonsgegevens vervolgens gedurende lange tijd worden bewaard en daardoor niet meer actueel zijn.

Aan de meeste in artikel 5 AVG genoemde beginselen wordt nadere invulling gegeven in andere artikelen van de AVG. Voldoet uw verwerking niet (meer) aan alle eisen die de AVG stelt? Dan moet u uw verwerking niet starten, aanpassen of beëindigen.

Deze richtlijnen voor scraping door private organisaties en particulieren behandelen niet alle AVG-beginselen die worden genoemd in artikel 5 AVG, maar gaan specifiek in op één van deze beginselen: het beginsel van rechtmatigheid. Dit beginsel²⁰ wordt nader (maar niet uitputtend) uitgewerkt in artikel 6 van de AVG. Hierna gaan we nader in op dit AVG-artikel: de noodzaak om een rechtsgrond te hebben voor de verwerking van 'gewone' persoonsgegevens, met in het bijzonder aandacht voor de grondslag gerechtvaardigd belang (paragraaf 5.2-5.3). Vervolgens gaan we in op de verwerking van bijzondere en strafrechtelijke persoonsgegevens (hoofdstuk 6 en 7).

5. Beginsel van rechtmatigheid

Rechtsgrond voor de verwerking

Zodra de AVG van toepassing is op een verwerking, geldt dat er een rechtsgrond moet zijn voor het verwerken van persoonsgegevens. Het is aan de verwerkingsverantwoordelijke om dit voorafgaand aan de verwerking te onderzoeken.

Bij scraping kan sprake zijn van een organisatie (een scraper) die voor een ander scrapet. Of van een organisatie die voor zichzelf scrapet, met een scrapingtool die is ontwikkeld door een andere organisatie of met een zelf ontwikkelde scrapingtool. Is sprake van een scraper die persoonsgegevens scrapet voor een ander? Of van een organisatie die de scrapingtool van een ander gebruikt? Dan zal moeten worden bepaald welke partij voor welk deel van de verwerking verwerkingsverantwoordelijke is.

¹⁷ Artikel 5 lid 1 onder a AVG.

¹⁸ Artikel 5 lid 1 onder c AVG.

¹⁹ Artikel 5 lid 1 onder d AVG.

²⁰ Artikel 5 lid 1 onder a AVG.



Hierbij is van belang wie het doel en de middelen van de gegevensverwerking bepaalt. Er zijn verschillende scenario's denkbaar:

- De scraper is zelf verwerkingsverantwoordelijke voor de hele gegevensverwerking.
- De opdrachtgever is verwerkingsverantwoordelijke en de scraper verwerker voor de hele gegevensverwerking.
- De scraper is verwerkingsverantwoordelijke voor een deel van de verwerking (bijvoorbeeld voor het verzamelen van persoonsgegevens met scraping) en de opdrachtgever voor een ander deel van de verwerking (bijvoorbeeld voor het analyseren en gebruiken van de gescrapete gegevens).
- Zowel de scraper als de opdrachtgever zijn verwerkingsverantwoordelijke. Er is dan sprake van gezamenlijke verwerkingsverantwoordelijkheid.

Wie er verwerkingsverantwoordelijke is, hangt af van de omstandigheden van het geval, waaronder de manier waarop de concrete gegevensverwerking is ingericht. De AP kan dus in zijn algemeenheid geen oordeel geven over de vraag wie er verwerkingsverantwoordelijke (en eventueel verwerker) is. De betrokken organisaties moeten hiervoor zelf een beoordeling maken die aansluit bij de feitelijke situatie. Op de website van de AP staat meer informatie over het vaststellen van de verwerkingsverantwoordelijke en de verwerker.

Verwerkingsverantwoordelijken hebben altijd een rechtsgrond nodig voor het verwerken van persoonsgegevens.

Verenigbaar gebruik

In eerste instantie kunt u misschien denken dat er geen (nieuwe) grondslag nodig is wanneer u scraping gebruikt. De persoonsgegevens staan immers al op internet. U zou dan kunnen denken dat er sprake is van een zogenoemde 'verdere verwerking' die verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld.²¹

Scraping moet echter niet worden gezien als een verenigbare verdere verwerking, maar als een nieuwe verwerking waarvoor u een grondslag nodig heeft. Hierbij is van belang dat er over het algemeen sprake is van het scrapen van bronnen van andere verwerkingsverantwoordelijken. De mogelijkheid van verenigbaar gebruik is in beginsel beperkt tot een verdere verwerking van persoonsgegevens door de verwerkingsverantwoordelijke zelf binnen de eigen bedrijfsvoering. Dit betekent dat u, als u informatie van internet wilt scrapen, hiervoor doorgaans geen beroep kunt doen op verenigbaar gebruik,²² maar dat u een (eigen) grondslag moet hebben.²³

²¹ Artikel 6 lid 4 AVG.

²² Artikel 6 lid 4 AVG.

²³ In de zin van artikel 6 lid 1 AVG.



Let op: Een grondslag heeft u óók nodig als u alleen informatie verzamelt die rechtmatig op internet is geplaatst en die voor iedereen openbaar toegankelijk is. En ook als u de persoonsgegevens direct na het verzamelen uit de database verwijdert.²⁴

AVG-grondslagen

Als private organisatie of particulier zal de grondslag ‘gerechtvaardigd belang’ doorgaans de enige grondslag zijn die eventueel in aanmerking komt.²⁵ De andere grondslagen die artikel 6 lid 1 AVG noemt (toestemming van de betrokkene, uitvoering overeenkomst, wettelijke verplichting, vitale belangen en taak van algemeen belang/openbaar gezag) zullen over het algemeen voor u niet van toepassing zijn.

Toestemming

In principe zou het vragen van toestemming aan de betrokkenen ook een geldige grondslag kunnen opleveren. Maar in de praktijk zal het bij het scrapen van persoonsgegevens van internet vaak moeilijk of zelfs ondoenlijk zijn om elke persoon van wie u de gegevens wilt scrapen, voorafgaand te identificeren en om toestemming te vragen.

Ook wanneer betrokkenen zelf hun persoonsgegevens online zetten, op een voor iedereen toegankelijke webpagina, kunt u hieruit niet afleiden dat deze betrokkenen toestemming geven voor het scrapen en/of het na de scraping verwerken van hun persoonsgegevens. Het door betrokkenen zelf voor iedereen zichtbaar plaatsen van hun gegevens op internet kunt u zien als toestemming om de gegevens te bekijken. Maar niet als toestemming om deze gegevens vervolgens te scrapen of anderszins te verwerken.

Lukt het u wel om aan betrokkenen vooraf toestemming te vragen voor het scrapen van hun persoonsgegevens? Wees u er dan van bewust dat deze toestemming alleen geldt voor de gegevens die u van die persoon verzamelt. Bevat de informatie die u scrapet ook gegevens over anderen dan degene van wie u de toestemming kreeg, bijvoorbeeld over familieleden, vrienden of collega’s van die persoon, dan is de verkregen toestemming niet voldoende.

Kunt u geen voorafgaande toestemming vragen aan iedere betrokkene? Dan rest doorgaans alleen gerechtvaardigd belang als mogelijke grondslag. De paragrafen 5.2 en 5.3 bieden u handvatten om te beoordelen of u een geslaagd beroep kunt doen op deze grondslag.

Voorwaarden voor de grondslag gerechtvaardigd belang

De grondslag gerechtvaardigd belang is opgenomen in artikel 6 lid 1 onder f van de AVG. Voor een geslaagd beroep op deze grondslag moet u aan deze drie voorwaarden voldoen:

1. Er is sprake van een gerechtvaardigd belang van u of van een derde.
2. De verwerking is noodzakelijk voor de behartiging van dit gerechtvaardigde belang.
3. De belangen of de grondrechten en de fundamentele vrijheden van de betrokkene(n) wegen niet zwaarder dan uw gerechtvaardigde belang of dat van de derde.

²⁴ Zie ook: <https://www.autoriteitpersoonsgegevens.nl/themas/internet-slimme-apparaten/persoonsgegevens-op-internet/persoonsgegevens-in-openbare-bronnen#persoonsgegevens-verzamelen-en-opnieuw-verwerken-voor-een-ander-doel>.

²⁵ Overheidsorganisaties kunnen zich bij de uitvoering van hun overheidstaken niet op deze grondslag beroepen.



Het gaat hierbij om cumulatieve voorwaarden. Het is dus vereist dat u aan alle drie de voorwaarden voldoet. Als u bijvoorbeeld wel aan de eerste voorwaarde heeft voldaan, maar niet aan de tweede of derde voorwaarde, dan zult u geen geslaagd beroep kunnen doen op de grondslag gerechtvaardigd belang.

Voorwaarde 1: gerechtvaardigd belang

Het standpunt van de Autoriteit Persoonsgegevens (AP) is dat alleen in rechte beschermde belangen kwalificeren als gerechtvaardigde belangen. Dat betekent dat het belang ergens in het recht opgenomen moet zijn. En dat het wordt erkend en beschermd. Dat mag ook in een ongeschreven rechtsregel of rechtsbeginsel zijn. Als het maar gaat om een belang waarvan we in de maatschappij vinden dat het door het recht beschermd moet worden.

Over dit standpunt heeft de Nederlandse rechter prejudiciële vragen gesteld aan het Hof van Justitie van de EU.²⁶ Wanneer het Hof zich hierover uitsprekt, is nog niet bekend. In afwachting van de uitspraak blijft de AP bij dit standpunt. Voor meer informatie, zie [Grondslag gerechtvaardigd belang](#) op de website van de AP.

Heeft u bij de verwerking van persoonsgegevens alleen een zuiver commercieel belang?²⁷ Dan kunt u volgens het standpunt van de AP geen geslaagd beroep doen op de grondslag gerechtvaardigd belang.

Heeft u (of een derde in wiens belang u de persoonsgegevens verwerkt) met de verwerking die u beoogt (naast een commercieel belang) een ander belang, dat wel door het recht wordt beschermd? Dan voldoet uw verwerking mogelijk wel aan de eerste voorwaarde voor de grondslag gerechtvaardigd belang. Bijvoorbeeld als u persoonsgegevens wilt verwerken voor fraudebestrijding of om de beveiliging van uw computersystemen te verbeteren. Of als u zich kunt beroepen op het recht op informatie vrijheid als bedoeld in artikel 11 van het Handvest van de grondrechten van de EU.²⁸

U moet er ook voor zorgen dat u betrokkenen informeert over de belangen waar u zich op beroept.²⁹ Pas nadat u de betrokkene heeft geïnformeerd over de doelen waarvoor u de persoonsgegevens verwerkt en de grondslag waarop u een beroep doet, kunt u een geslaagd beroep doen op gerechtvaardigd belang.³⁰ Dit is slechts anders indien u een geslaagd beroep kunt doen op een van de uitzonderingen op de informatieplicht. Zie verder artikel 12, 13 en 14 van de AVG en [recht op informatie](#) op de website van de AP.

Stelt u vast dat voor uw verwerking sprake is van een gerechtvaardigd belang? Dan moet u daarna bepalen of u ook aan de tweede en derde voorwaarde voldoet.

²⁶ Zie <https://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-621/22>.

²⁷ Een in rechte beschermd belang zoals fraudebestrijding kan uiteraard wel *ook* commercieel van belang zijn.

²⁸ Artikel 11 lid 1 Handvest luidt: "Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen."

²⁹ Artikel 13, lid 1 onder d, AVG, artikel 14, lid 2 onder b, AVG en HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 107 en § 126.

³⁰ Artikel 13, lid 1 onder c, AVG, artikel 14, lid 1 onder c, AVG en HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 95..



Voorwaarde 2: noodzakelijk

De tweede voorwaarde voor een geslaagd beroep op de grondslag gerechtvaardigd belang is dat de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van het belang waarop u zich beroept. Op grond van dit noodzakelijkheidsvereiste moet u voldoen aan de beginselen van subsidiariteit en proportionaliteit.

Voor meer informatie, zie [Grondslag gerechtvaardigd belang](#) op de website van de AP.

Voorwaarde 3: belangenafweging

Ten slotte moet u een belangenafweging maken. Daarbij weegt u de belangen en fundamentele rechten en vrijheden van de betrokkene(n) af tegen uw belangen of die van de derde.

Voor meer informatie, zie [Grondslag gerechtvaardigd belang](#) op de website van de AP.

Beoordeling grondslag gerechtvaardigd belang: mee te wegen kenmerken van scraping

Scraping kan voor verschillende doelen en op verschillende manieren plaatsvinden. De beoordelingen die u moet maken om vast te stellen of is voldaan aan de tweede en derde voorwaarde van de grondslag gerechtvaardigd belang, moet u maken op basis van de specifieke kenmerken van de verwerking die u voor ogen heeft. Daarbij kunt u ook door u getroffen extra waarborgen meewegen die de belangen van de betrokkene(n) beschermen en de inbreuk van de verwerking beperken.

U moet uw verwerking zorgvuldig beoordelen. Al voordat u met de verwerking start. Er is een aantal kenmerken van scraping dat u, afhankelijk van de precieze verwerking, moet betrekken bij de vraag of u een geslaagd beroep kunt doen op de grondslag gerechtvaardigd belang.³¹

Omvang en aard van de gegevensverwerking

Met scraping kunt u in korte tijd heel veel persoonsgegevens verzamelen. Niet alleen van heel veel verschillende mensen, maar ook per individu heel veel gegevens. Deze gegevens kunnen afkomstig zijn uit de meest uiteenlopende bronnen. En gaan mogelijk over tal van aspecten van iemands privéleven. Ook kunnen de gescrapete gegevens een lange tijdsperiode omvatten. Want informatie die op internet wordt gepubliceerd, blijft daar vaak staan. In algemene zin geldt: hoe breder de scraper zoekt, hoe groter de inbreuk op de persoonlijke levenssfeer van de betrokkenen. Als na verloop van tijd opnieuw wordt gescrapet om de database aan te vullen, vergroot dit ook de inbreuk.

Is de database waarin gescrapete gegevens worden opgeslagen doorzoekbaar op individuele personen? Dan vergroot dat de inbreuk aanzienlijk. Op die manier kunnen namelijk (potentieel gedetailleerde) profielen van de betrokkenen worden gemaakt. Het is belangrijk om al dit soort gevolgen voor betrokkenen na te gaan voordat u scraping inzet. En deze gevolgen mee te wegen bij de beoordeling of u kunt voldoen aan de voorwaarden voor de grondslag gerechtvaardigd belang.

³¹ Als u scraping wilt inzetten, moet uw verwerking uiteraard ook voldoen aan de andere eisen van de AVG. Ook dat moet u beoordelen voordat u met de verwerking start.



Gevoelige gegevens

Bij het scrapen van gegevens van internet is de kans groot dat u ook [gevoelige persoonsgegevens](#) verzamelt, zoals locatiegegevens of financiële gegevens. Hoe meer gevoelige gegevens u scrapet, hoe groter de privacyinbreuk is die uw verwerking maakt. Hetzelfde geldt voor de mate van gevoeligheid van de persoonsgegevens na het uitvoeren van eventuele analyses.

Hoe gevoeliger de informatie over betrokkenen is, hoe minder snel u voldoet aan de tweede en derde voorwaarde voor de grondslag gerechtvaardigd belang. Ook kunt u (bedoeld of onbedoeld) bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens verwerken. Daarover meer in hoofdstuk 6 en 7.

Verwachtingen van betrokkenen

Bij het gebruik van scraping kunnen persoonsgegevens worden gescrapet die door de betrokkene zelf openbaar en voor iedereen zichtbaar zijn gemaakt. Bijvoorbeeld als iemand berichten heeft geschreven op een openbaar forum. Of als iemand foto's van zichzelf heeft geplaatst op een voor iedereen toegankelijke socialemediapagina.

Voor die gegevens geldt dat de betrokkenen redelijkerwijs minder snel zullen (mogen) verwachten dat hun gegevens niet door anderen worden verwerkt. De inbreuk die ontstaat als anderen deze gegevens gebruiken, zal daarom normaal gesproken kleiner zijn dan bij het gebruik van gegevens die niet door betrokkenen zelf openbaar zijn gemaakt maar door een ander. Bijvoorbeeld door een sportvereniging of werkgever die de naam van een betrokkene op de website van deze organisatie plaatst. Maar ook als mensen zelf hun persoonsgegevens openbaar toegankelijk publiceren op internet, leidt dat er niet altijd toe dat de betrokkenen redelijkerwijs moeten verwachten dat hun persoonsgegevens vervolgens voor een ander doel worden verwerkt.

Bij de verwachtingen van de betrokkenen is ook relevant dat er vaak geen relatie bestaat tussen degene die de scraping uitvoert, of de gescrapete gegevens gebruikt, en degene van wie persoonsgegevens worden gescrapet. Daarnaast weten betrokkenen vaak niet precies welke gegevens allemaal over hen op internet staan. En staan er ook veel persoonsgegevens op internet die niet door de betrokkenen zelf zijn gepubliceerd. Voor veel persoonsgegevens geldt bovendien dat toen deze werden gepubliceerd op internet, scraping in de huidige vorm nog niet werd gebruikt of in elk geval minder bekend was voor veel betrokkenen.

Bij het scrapen van persoonsgegevens van internet zal het vaak moeilijk of ondoenlijk zijn om elke persoon van wie u gegevens wilt scrapen, te identificeren en te informeren over de gegevensverwerking die u wilt gaan uitvoeren. Afhankelijk van hoe de gegevensverwerking precies is ingericht, is het mogelijk dat u betrokkenen niet individueel hoeft te informeren over uw verwerking. Bijvoorbeeld omdat het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen.³²

Is dat het geval, dan moet u wel passende maatregelen nemen om de rechten, vrijheden en gerechtvaardigde belangen van de betrokkenen te beschermen. Hieronder valt in ieder geval dat u de

³² Artikel 14 lid 5 onder b AVG. Zie artikel 13 lid 4 en artikel 14 lid 5 onder a, c en d voor andere uitzonderingen op de verplichting tot informatieverstrekking aan betrokkenen.



informatie die u normaliter aan de betrokkenen zou verstrekken, openbaar moet maken. Dit kunt u bijvoorbeeld doen met een op internet gepubliceerd privacybeleid. Geef zo concreet mogelijk weer welke persoonsgegevens u verwerkt, voor welke doelen, en op basis van welke grondslag. Vermeld ook uw contactgegevens en maak duidelijk dat de betrokkenen AVG-rechten hebben, welke dat zijn en hoe ze die rechten bij u kunnen uitoefenen.

Een andere maatregel om de belangen van de betrokkenen te beschermen, kan zijn dat op de websites waarvan u persoonsgegevens scrapet ook informatie wordt geplaatst over de scraping van persoonsgegevens. Ook zouden de opdrachtgevers van het scrapen (duidelijk) op hun website kunnen aangeven dat zij gebruikmaken van scraping om persoonsgegevens te verzamelen.

Is uw gegevensverwerking zodanig dat u de betrokkenen wel persoonlijk kunt informeren voorafgaand aan de gegevensverwerking? Dan zult u de betrokkenen in beginsel moeten informeren. Zo kunnen de betrokkenen weten wat er met hun persoonsgegevens gebeurt en hier de eventuele risico's van inschatten. Door duidelijke en nuttige informatie aan de betrokkenen te verstrekken, zullen de verwachtingen van de betrokkenen beter aansluiten bij de verwerkingen die u gaat uitvoeren. Zie verder artikel 12, 13 en 14 van de AVG en [recht op informatie](#) op de website van de AP.

In hoeverre betrokkenen al dan niet op de hoogte (kunnen) zijn van de verwerking die u beoogt, speelt ook een rol bij de beoordeling of u een geslaagd beroep kunt doen op de grondslag gerechtvaardigd belang. Want: hoe minder betrokkenen kunnen verwachten dat hun persoonsgegevens voor een bepaald doel worden gescrapet, hoe zwaarder hun belang weegt bij het niet verwerken van hun gegevens ten opzichte van uw belang om deze gegevens wel te verwerken.

Gevolgen voor betrokkenen

De mogelijke gevolgen voor betrokkenen zijn sterk afhankelijk van het doel waarvoor u de scraping of de gescrapete gegevens gebruikt. Wilt u bijvoorbeeld scraping gebruiken om een statistische analyse te maken, waarbij de resultaten niet herleidbaar zijn tot individuele personen? Of wilt u met scraping een sentimentanalyse maken, om te kijken hoe een bepaald nieuw product wordt ontvangen door het Nederlandse publiek? Dan zijn de gevolgen voor de betrokkenen kleiner dan wanneer u scraping bijvoorbeeld gebruikt om profielen van mensen te maken. Of om te bepalen of u nieuwe werknemers al dan niet aanneemt op basis van hun uitingen op sociale media en online fora. In dat laatste geval heeft uw verwerking directe en potentieel grote gevolgen voor de betrokkenen.

De gevolgen voor de betrokkenen wegen zwaar mee bij de beoordeling of de verwerking voldoet aan de derde voorwaarde voor de grondslag gerechtvaardigd belang.

Zwakke positie betrokkenen

Scraping is voor de betrokkenen van wie gegevens worden verzameld niet vanzelf zichtbaar. Dit maakt dat betrokkenen in de praktijk hun AVG-rechten minder goed kunnen uitoefenen en vaak weinig kunnen doen om zich tegen het scrapen van hun gegevens te verzetten.³³ Maar ook als de betrokkenen wel op de

³³ Dit is des te meer het geval als bij scraping bepaalde standaarden niet worden nageleefd die normaal zouden voorkomen dat een website wordt gecrawld, zoals het respecteren van een robots.txt-bestand.



hoogte zijn dat hun persoonsgegevens gescrept (kunnen) gaan worden, is het niet gemakkelijk om persoonsgegevens die eenmaal op internet gepubliceerd zijn te verwijderen of onbereikbaar te (laten) maken voor scrapers.

Dit gebrek aan controle over de eigen gegevens vormt een grote inbreuk op het recht van betrokkenen op bescherming van hun persoonsgegevens. U moet dit meewegen bij de beantwoording van de vraag of u een beroep kunt doen op de grondslag gerechtvaardigd belang als u wilt scrapen of als u gebruik wilt maken van gescrepte gegevens.

De rol van waarborgen

De hiervoor genoemde kenmerken van scraping zullen bij verschillend gebruik van scraping of gescrepte gegevens in verschillende mate spelen. U kunt de gevolgen voor de betrokkenen op allerlei manieren verminderen door extra waarborgen te treffen. Deze extra waarborgen kunnen, afhankelijk van de specifieke omstandigheden van een bepaalde verwerking, een belangrijke rol spelen in de belangenafweging (derde voorwaarde voor de grondslag gerechtvaardigd belang). Het moet daarbij wel gaan om aanvullende waarborgen die u uit zichzelf neemt. En dus niet om waarborgen die op grond van de AVG sowieso al verplicht zijn.

U kunt bijvoorbeeld:

- waarborgen treffen die bijdragen aan extra transparantie;
- de persoonsgegevens zo snel mogelijk te verwijderen, anonimiseren of pseudonimiseren;
- het recht op gegevenswissing ruimer toepassen dan artikel 17 AVG vereist, bijvoorbeeld door een verzoek om wissing van iemands persoonsgegevens altijd te honoreren;
- internetstandaarden naleven, zoals het robots exclusion protocol (robots.txt), waarmee websitebeheerders aangeven welk deel van hun website mag worden bezocht door crawlers.^{34, 35}

Extra waarborgen kunnen ervoor zorgen dat u voor een verwerking een beroep kunt doen op de grondslag gerechtvaardigd belang. Dit hangt echter wel af van de precieze verwerking. Het treffen van extra waarborgen zal zeker niet altijd leiden tot een geslaagd beroep op de grondslag gerechtvaardigd belang.

Naast het hebben van een grondslag, zoals bedoeld in artikel 6 AVG, is het van belang om te onderzoeken of u bijzondere persoonsgegevens verwerkt. Hetzelfde geldt voor persoonsgegevens van strafrechtelijke aard. Als u deze gegevens verwerkt, moet u aan aanvullende eisen uit de AVG voldoen. De eisen voor bijzondere persoonsgegevens bespreken we in hoofdstuk 6. In hoofdstuk 7 gaan we in op strafrechtelijke gegevens. Deze eisen voor het verwerken van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens zijn ook een uitwerking van het beginsel van rechtmatigheid uit artikel 5 AVG.

³⁴ Zie voor meer informatie <http://www.robotstxt.org/robotstxt.html>.

³⁵ Let op: het feit dat een website geen gebruik maakt van dergelijke standaarden, betekent niet dat het u vrij staat om deze website te scrapen, zie HvJ EU C-131/12, [ECLI:EU:C:2014:317](#) (*Google Spain*), § 39.



6. Bijzondere persoonsgegevens

Sommige persoonsgegevens zijn zogenoemde bijzondere persoonsgegevens. Dit zijn persoonsgegevens die zó privacygevoelig zijn dat het grote(re) impact op iemand kan hebben als deze gegevens worden verwerkt. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands etnische afkomst, politieke opvattingen, religieuze overtuigingen, seksuele leven of gezondheid.³⁶ Het verwerken van bijzondere persoonsgegevens is verboden, tenzij er een uitzondering geldt. Dus ook het scrapen van bijzondere persoonsgegevens is in beginsel verboden.

Bijzondere persoonsgegevens: verhouding zoekmachines en scraping

Het Hof heeft bepaald dat het verwerkingsverbod op bijzondere persoonsgegevens ook van toepassing is op zoekmachines die webpagina's indexeren. Het Hof keek echter ook naar de 'verantwoordelijkheden, bevoegdheden en mogelijkheden' van de zoekmachine om deze toets uit te voeren. Op basis daarvan oordeelde het Hof dat een zoekmachine niet voorafgaand aan de verzameling hoeft te toetsen of er een mogelijke uitzonderingsgrond van toepassing is op het verbod om bijzondere persoonsgegevens te verwerken.³⁷

Tussen zoekmachines en scrapers bestaan een aantal overeenkomsten, waardoor gedacht zou kunnen worden dat de hierboven beschreven overweging ook op scrapers van toepassing is. Zo verzamelen zowel zoekmachines als scrapers gegevens van webpagina's die door derden worden beheerd.

Aan de andere kant zijn er ook (grote) verschillen tussen zoekmachines, die ook informatie verzamelen door middel van crawling, en scrapers. Zo zorgen zoekmachines ervoor dat informatie op het internet goed vindbaar is. En worden er geen extra verwerkingen toegepast op de verzamelde informatie nadat de zoekmachine deze eenmaal heeft geïndexeerd. Bij scraping daarentegen gebeurt er juist vaak nog wél veel met de verzamelde data. De gegevens kunnen bijvoorbeeld worden geanalyseerd op patronen, worden gebruikt bij het beoordelen van een financieringsaanvraag of worden gebruikt voor een sentimentanalyse.

Het is nog onzeker of scraping, op dezelfde voet als zoekmachines, kan worden geacht de vrijheid van informatie te dienen. Het is niet uitgesloten dat het Hof voor de eerste fase van het scrapen – het vinden van informatie – in de toekomst zal oordelen dat het niet van scrapers gevraagd kan worden om vast te stellen of er al dan niet bijzondere persoonsgegevens worden verwerkt. Mogelijk betekent dit dat er geen schending is van het verwerkingsverbod van artikel 9 AVG bij scrapingmethodes die (bijzondere) persoonsgegevens met een hoge graad van betrouwbaarheid kunnen herkennen en uit de dataset verwijderen voordat eventuele verdere verwerkingen plaatsvinden.³⁸ Terwijl wel bijzondere persoonsgegevens worden gescrept.

³⁶ Zie artikel 9 lid 1 AVG.

³⁷ HvJ EU 24 september 2019, C-136/17, [ECLI:EU:C:2019:773](#) (GC/CNIL), § 44-47. Let op: er moet altijd worden beoordeeld of er sprake is van een verwerking van bijzondere persoonsgegevens als een betrokkene een verwijderverzoek indient zoals bedoeld in artikel 17 AVG.

³⁸ Bij eventuele extra verwerkingen die plaatsvinden na het verzamelen van de data kunt u immers geen beroep meer doen op deze overweging van het Hof.



Let wel: in de tekst hierna gaan we uit van de situatie dat voor scraping het zwaardere beschermingsregime voor bijzondere persoonsgegevens onverkort van toepassing is.

Voorwaarden voor het verwerken van bijzondere persoonsgegevens

Bij scraping, en in het bijzonder bij scraping van sociale media, is er al snel sprake van de verwerking van bijzondere persoonsgegevens. Op sociale media is immers veel informatie te vinden over mensen. Zo kondigen sommige mensen bijvoorbeeld op sociale media aan dat zij een medische behandeling moeten ondergaan of volgen zij zichtbaar een webpagina waaruit hun religieuze overtuiging blijkt.

Wilt u scraping inzetten, dan is het van belang om vooraf goed na te gaan of u mogelijk bijzondere persoonsgegevens gaat verwerken. Daarbij moet u het begrip 'bijzondere persoonsgegevens' ruim uitleggen.³⁹ Vloeien uit de combinatie van verschillende 'normale' persoonsgegevens (indirect) bijzondere persoonsgegevens voort? Ook dan moet u voldoen aan de AVG-eisen voor de verwerking van bijzondere persoonsgegevens.⁴⁰ Het maakt daarbij niet uit of deze gegevens juist zijn. Of dat u wel of niet het doel had om deze bijzondere persoonsgegevens te verwerken.⁴¹

Het kan zo zijn dat het beschermingsregime voor bijzondere persoonsgegevens op de gehele verwerking van toepassing is. Dit is het geval als u alleen maar bijzondere persoonsgegevens verwerkt, maar óók wanneer u zowel 'normale' als bijzondere persoonsgegevens verzamelt.⁴² U moet dan voor alle persoonsgegevens een uitzondering hebben op het verbod op de verwerking van bijzondere persoonsgegevens. Dit geldt ook als u gebruikmaakt van gegevens die door een ander zijn gescrapet. Slaat u zowel gewone als bijzondere persoonsgegevens op in één database, dan is het beschermingsregime voor bijzondere persoonsgegevens van toepassing op alle gegevens in deze database.

Kunt u niet uitsluiten dat u (ook) bijzondere persoonsgegevens verwerkt? Dan geldt het (zwaardere) beschermingsregime voor bijzondere persoonsgegevens. Dit houdt in dat het verwerken van deze gegevens verboden is, tenzij u een geslaagd beroep kunt doen op een van de uitzonderingen.⁴³ Van deze uitzonderingen bespreken we er in deze richtlijnen twee: (1) uitdrukkelijke toestemming van de betrokkene en (2) kennelijke openbaarmaking van de gegevens door de betrokkene.

Uitdrukkelijke toestemming van de betrokkene

Het verbod op het verwerken van bijzondere persoonsgegevens is niet van toepassing als de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden.⁴⁴ Bij het scrapen van persoonsgegevens van internet zal het echter vaak moeilijk of ondoenlijk zijn om elke persoon van wie u gegevens wilt scrapen, voorafgaand te identificeren en om toestemming te vragen.

³⁹ HvJ EU C-184/20, 1 augustus 2022, [ECLI:EU:C:2022:601](#) (*Vyriausioji*), §124-125.

⁴⁰ HvJ EU C-184/20, 1 augustus 2022, [ECLI:EU:C:2022:601](#) (*Vyriausioji*), §120.

⁴¹ HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 69.

⁴² HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 89.

⁴³ Zie voor de uitzonderingen artikel 9 lid 2 AVG en de artikelen 22 tot en met 30 Uitvoeringswet AVG (UAVG). Uitzonderingen op het verwerkingsverbod moeten restrictief worden uitgelegd. Zie HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 76.

⁴⁴ Artikel 9 lid 2 onder a AVG en artikel 22 lid 2 onder a UAVG.



Lukt het u wél uw verwerking zo in te richten dat u de betrokkenen voorafgaand aan de verwerking om toestemming kunt vragen? Let er dan op dat:

- De betrokkenen vrij zijn om wel of niet toestemming te geven.
- De betrokkenen een uitdrukkelijke verklaring van toestemming geven.
- U de betrokkenen voorafgaand aan het vragen van toestemming informeert over:
 - uzelf als organisatie;
 - het doel van de verwerking(en) waarvoor u toestemming vraagt;
 - welke persoonsgegevens u verzamelt en gebruikt;
 - het recht dat de betrokkenen hebben om hun gegeven toestemming weer in te trekken.
- De toestemming steeds geldt voor een specifieke verwerking en een specifiek doel.
- De toestemming te allen tijde weer in te trekken is door de betrokkene.
- U de gegeven toestemming vastlegt. En u kunt laten zien op basis van welke informatie iemand toestemming heeft gegeven.⁴⁵

Kennelijke openbaarmaking van persoonsgegevens

Het verbod op het verwerken van bijzondere persoonsgegevens is ook niet van toepassing als het gaat om een verwerking van persoonsgegevens die 'kennelijk door de betrokkene openbaar zijn gemaakt'.⁴⁶ We gaan nu in op wat 'door de betrokkene openbaar gemaakt' en 'kennelijk openbaar gemaakt' precies inhouden.

Zelf openbaar gemaakt

Allereerst moeten de bijzondere persoonsgegevens door de betrokkene zelf openbaar zijn gemaakt. Bijvoorbeeld doordat de betrokkene in een openbaar toegankelijk blog over zichzelf heeft geschreven en daarbij ingaat op zijn gezondheid, seksuele geaardheid, geloofsovertuiging, et cetera. De uitzondering op het verwerkingsverbod geldt dus niet voor persoonsgegevens die door iemand anders openbaar zijn gemaakt dan degene over wie de gegevens gaan.⁴⁷

Als u gegevens van internet scrapet, moet u erop bedacht zijn dat de bijzondere persoonsgegevens die u daarbij (bedoeld of onbedoeld) verzamelt en vastlegt, niet altijd door de betrokkene zelf openbaar gemaakt zijn. Bijvoorbeeld wanneer een familielid informatie deelt over iemands medische situatie. Is dat laatste het geval, dan geldt de hier besproken uitzondering op het verwerkingsverbod dus niet.

Kennelijk openbaar gemaakt

Een andere voorwaarde is dat de bijzondere persoonsgegevens 'kennelijk' openbaar moeten zijn gemaakt. Dit houdt in dat de betrokkene de persoonsgegevens voor een breed publiek toegankelijk heeft willen maken en dat uitdrukkelijk heeft gedaan met een ondubbelzinnige, actieve handeling.⁴⁸ Oftewel: de intentie om openbaar te maken moet uitdrukkelijk blijken uit een gedraging van de betrokkene.

⁴⁵ Op de website van de AP staat meer informatie over de [grondslag toestemming](#). Ook kunt u hierover meer informatie vinden in de [EDPB-guidelines](#) over toestemming.

⁴⁶ Artikel 9 lid 2 onder e AVG.

⁴⁷ HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 75.

⁴⁸ HvJ EU C-252/21, 4 juli 2023, [ECLI:EU:C:2023:537](#) (*Meta/Bundeskartellamt*), § 77.



Bijvoorbeeld: de betrokkene heeft de bijzondere persoonsgegevens gepubliceerd in een door deze persoon zelf geschreven openbaar toegankelijk blog, in een openbare reactie op een nieuwswebsite of in een opiniestuk in een krant.

Hebben betrokkenen hun socialemediaprofiel op besloten⁴⁹ staan? Dan kunt u dit zien als een indicatie dat zij hun persoonsgegevens niet voor een breed publiek toegankelijk hebben willen maken. Is bij een socialemediaplatform de informatie uit iemands profiel volgens de standaardinstellingen openbaar? Dan kunt u daaruit niet afleiden dat de betrokkene de bijzondere persoonsgegevens voor een breed publiek toegankelijk heeft willen maken. Hier is immers geen sprake van een actieve handeling van de betrokkene. De uitzondering ‘kennelijke openbaarmaking’ geldt in deze gevallen niet.

Maar zijn de standaardinstellingen van een socialemediaplatform dat informatie niet openbaar wordt gedeeld? En kiest de betrokkene ervoor om de instellingen te veranderen, zodat de informatie die de betrokkene plaatst wel openbaar is? Dan is wél sprake van kennelijke openbaarmaking. En geldt er dus een uitzondering op het verwerkingsverbod.

Bij door een betrokkene openbaar geplaatste foto's is nog iets anders van belang. Het enkele feit dat een gezichtsafbeelding kennelijk openbaar is gemaakt door de betrokkene, betekent niet dat u de eventuele biometrische gegevens (die u met specifieke technische middelen uit een foto kunt halen) ook kunt beschouwen als kennelijk openbaar gemaakt door de betrokkene. Biometrische gegevens mag u alleen als kennelijk openbaar gemaakt beschouwen als de betrokkene zelf het biometrische sjabloon – dus niet enkel een gezichtsafbeelding – weloverwogen vrij toegankelijk heeft gemaakt in een openbare bron.⁵⁰

Als we kijken naar de hierboven besproken uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens, dan wordt duidelijk dat het bij het scrapen van informatie van internet vaak lastig of onmogelijk zal zijn om onderscheid te maken tussen gewone persoonsgegevens en bijzondere persoonsgegevens. En dat u dus al snel (ook) bijzondere persoonsgegevens scrapet, wat (behoudens uitzonderingen) verboden is. Dit kan tot gevolg hebben dat een verwerking in zijn geheel niet is toegestaan vanwege de verwerking van bijzondere persoonsgegevens.

Ook als u niet zelf gegevens scrapet, maar gebruikmaakt van door een ander gescrapete persoonsgegevens, kan het zo zijn dat uw verwerking niet is toegestaan omdat u (ook) bijzondere persoonsgegevens verwerkt en geen geslaagd beroep kunt doen op een van de uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens.

7. Persoonsgegevens van strafrechtelijke aard

Bij scraping kan er, naast de verwerking van bijzondere persoonsgegevens, sprake zijn van een verwerking van ‘persoonsgegevens van strafrechtelijke aard’ (hierna: strafrechtelijke persoonsgegevens). Ook aan deze persoonsgegevens kent de AVG extra bescherming toe, in artikel 10 AVG. Artikel 10 is net als het

⁴⁹ Oftewel: niet openbaar. Hieronder vallen bijvoorbeeld ook profielen die alleen zichtbaar zijn voor vrienden, connecties of vrienden van vrienden.

⁵⁰ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en, p. 21.



hiervoor besproken artikel 6 AVG (over de grondslagen) en artikel 9 AVG (over bijzondere persoonsgegevens) een uitwerking van het beginsel van rechtmatigheid dat wordt genoemd in artikel 5 AVG. Vandaar dat we ook artikel 10 behandelen in deze richtlijnen.

Strafrechtelijke persoonsgegevens mogen alleen worden verwerkt:

- onder toezicht van de overheid;
- wanneer dit toegestaan is op grond van Europese of Nederlandse wetgeving die passende waarborgen voor de rechten en vrijheden van de betrokkenen biedt.

In Nederland is hieraan uitwerking gegeven in artikel 31, 32 en 33 van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).⁵¹ In deze artikelen is nader bepaald in welke gevallen strafrechtelijke persoonsgegevens mogen worden verwerkt.

Ook voor scraping van strafrechtelijke persoonsgegevens geldt dat het algemene verbod op het verwerken van dit soort gegevens wordt doorbroken als de gegevens door de betrokkene zelf kennelijk openbaar zijn gemaakt. Of als de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer specifieke doeleinden.

Zie voor de aandachtspunten bij deze beide uitzonderingsgronden hoofdstuk 6 over bijzondere persoonsgegevens. Zie voor de overige mogelijke uitzonderingsgronden artikel 32 en 33 UAVG.

Net als bij bijzondere persoonsgegevens, geldt ook bij strafrechtelijke persoonsgegevens dat het bij het scrapen van informatie van internet vaak lastig of onmogelijk zal zijn om onderscheid te maken tussen gewone persoonsgegevens en strafrechtelijke persoonsgegevens. Dat betekent dat de verwerking die u beoogt niet is toegestaan als u niet kunt uitsluiten dat u (ook) strafrechtelijke persoonsgegevens verwerkt, terwijl u geen geslaagd beroep kunt doen op een van de uitzonderingen op het verwerkingsverbod. Dat geldt ook als het helemaal niet uw doel is om strafrechtelijke persoonsgegevens te verwerken.

8. Samenvatting rechtmatigheid en voorbeelden

Het gebruik van scraping of gescrapete persoonsgegevens van internet is al snel een (zeer) grote inbreuk op het recht van betrokkenen op bescherming van hun persoonsgegevens. Dit kan het moeilijk of zelfs onmogelijk maken om te voldoen aan de voorwaarden voor een geslaagd beroep op de grondslag gerechtvaardigd belang.

Een niet in rechte beschermd (zuiver) commercieel belang kan op grond van het standpunt van de AP niet worden aangemerkt als een 'gerechtvaardigd' belang in de zin van artikel 6 lid 1 onder f AVG. Ook voor organisaties die met scraping software willen ontwikkelen (zoals generatieve AI) geldt dat een (louter) commercieel belang niet kwalificeert als een gerechtvaardigd belang om persoonsgegevens te verzamelen en te gebruiken om deze software te trainen. Als de scraping ook voor andere (niet-commerciële)

⁵¹ In artikel 31, 32 en 33 UAVG wordt invulling gegeven aan de ruimte die artikel 10 AVG biedt om gegevens van strafrechtelijke aard te verwerken zonder overheidstoezicht op basis van lidstaatrechtelijke bepalingen.



belangen van uzelf of van anderen wordt ingezet, kan eventueel wel sprake zijn van een gerechtvaardigd belang. U moet dan nog steeds wel voldoen aan de tweede en derde voorwaarde van de grondslag gerechtvaardigd belang (zie paragraaf 5.2).

Bij de ontwikkeling van AI en de rechtmatigheid van het verwerken van persoonsgegevens voor AI is relevant dat op Europees niveau gewerkt wordt aan nieuwe wetgevende kaders voor AI, zoals de AI-verordening. Zie verder hoofdstuk 10.

Voldoet een verwerking aan alle drie de voorwaarden van de grondslag gerechtvaardigd belang? Dan moet u ook nagaan of u bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens verwerkt. Zoals in hoofdstuk 6 en 7 is beschreven, geldt voor dit soort gegevens een algemeen verwerkingsverbod. Daarop bestaan wel diverse uitzonderingen, maar het zal voor u in de praktijk vaak lastig of onmogelijk zijn om een geslaagd beroep te kunnen doen op deze uitzonderingen. Hoe breder en ongerichter u gegevens scrapet, hoe moeilijker het is om uit te sluiten dat u onrechtmatig bijzondere of strafrechtelijke persoonsgegevens verwerkt.

Deze richtlijnen gaan specifiek in op het beginsel van rechtmatigheid, een van de beginselen uit artikel 5 AVG. Er is in deze richtlijnen met name aandacht besteed aan de artikelen 6 AVG (grondslagen), 9 AVG (bijzondere persoonsgegevens) en 10 AVG (persoonsgegevens van strafrechtelijke aard), die invulling geven aan dit beginsel van rechtmatigheid. Als u tot het oordeel komt dat uw verwerking aan deze artikelen voldoet, moet u vervolgens uiteraard ook beoordelen of de verwerking voldoet aan alle andere beginselen en eisen van de AVG. Alleen dan kunt u de verwerking die u beoogt immers rechtmatig uitvoeren.

Alles overziend lijkt voor private organisaties alleen (zeer) gerichte scraping rechtmatig te kunnen zijn. Het is niet mogelijk om in algemene zin te zeggen welk gebruik van scraping of gescrapete gegevens wel en niet is toegestaan. Voor die beoordeling is het noodzakelijk om alle details en waarborgen van een specifieke verwerking te kennen. Maar er zijn wel verwerkingen te bedenken die kansrijker zijn om in lijn met de AVG te kunnen worden gebracht dan andere verwerkingen. Hierbij kunt u denken aan scraping van:

- openbare nieuwswebsites, om voor de eigen organisatie of het eigen werkveld relevante actualiteiten in beeld te brengen;
- eigen webpagina's door webwinkels, bijvoorbeeld met reviews van klanten, voor communicatie met eigen (potentiële) klanten;
- openbare online fora over informatiebeveiliging, om beveiligingsrisico's in beeld te brengen voor de eigen organisatie.

Deze voorbeelden zijn bedoeld ter illustratie. Uiteindelijk zal in de praktijk van geval tot geval moeten worden beoordeeld of daadwerkelijk is voldaan aan alle eisen van de AVG.

Er zijn ook voorbeelden te bedenken van verwerkingen die waarschijnlijk nooit AVG-proof kunnen worden ingericht. Zoals scraping van:



- internet om profielen van betrokkenen te maken en die vervolgens door te verkopen;
- besloten socialemedia-accounts of besloten fora;
- socialemedia-accounts van betrokkenen – ook al zijn die openbaar – om met de verzamelde informatie te bepalen of een betrokkene een aangevraagde verzekering al dan niet krijgt.

Al met al vergt het gebruik van scraping of gescrapete persoonsgegevens een zorgvuldige, voorafgaande beoordeling. Komt u tot de conclusie dat u voor uw verwerking een geslaagd beroep kunt doen op de grondslag gerechtvaardigd belang? En dat u geen persoonsgegevens verwerkt in strijd met het algemene verbod op het verwerken van bijzondere en strafrechtelijke persoonsgegevens? Dan moet u uiteraard ook beoordelen of u voldoet aan de overige eisen die de AVG stelt. Een van de manieren om (een deel van) die beoordeling vorm te geven, is een data protection impact assessment (DPIA).

9. DPIA & voorafgaande raadpleging

Op grond van artikel 5 lid 2 AVG moet u kunnen aantonen dat u persoonsgegevens op een rechtmatige, behoorlijke en transparante manier verwerkt. Dit heet de [verantwoordingsplicht](#). Daarom is het belangrijk dat u, voordat u scraping inzet, de rechtmatigheid van uw verwerking beoordeelt en de privacyrisico's in kaart brengt. Een geschikt instrument hiervoor is een data protection impact assessment (DPIA), die in veel gevallen ook verplicht is.⁵²

Met een DPIA kunt u vooraf de privacyrisico's van een gegevensverwerking in kaart brengen. En na de start van de verwerking periodiek toetsen of de verwerking nog in lijn is met de AVG. Op basis van de bevindingen in een DPIA kunt u maatregelen nemen om de privacyrisico's te verkleinen. Ook als het uitvoeren van een DPIA voor u niet verplicht is, is het aan te raden om dat toch te doen. Heeft u een functionaris gegevensbescherming (FG) in dienst? Dan moet u de FG advies vragen bij het uitvoeren van de DPIA.⁵³ Lees meer over de [DPIA](#) op de website van de AP.

Blijkt uit de uitgevoerde DPIA dat er een hoog privacyrisico is? En kunt u dit risico niet wegnemen met maatregelen? Dan moet u een [voorafgaande raadpleging aanvragen bij de AP](#). De AP beoordeelt uw voorgenomen verwerking dan. De AP laat u vervolgens weten of u wel of niet met uw verwerking mag starten en welke maatregelen u eventueel nog moet nemen voordat u mag starten.

10. Het gebruik van scraping voor het trainen van algoritmes

Gebruiken organisaties gescrapete gegevens om algoritmes te trainen? Dan bestaan er, naast het risico niet aan de AVG te voldoen, andere risico's waardoor grondrechten of andere publieke waarden in het

⁵² Artikel 35 AVG.

⁵³ Artikel 35 lid 2 AVG.



geding kunnen komen. Als organisaties geen rekening houden met dergelijke risico's, ondermijnt dat de betrouwbaarheid van deze AI-systemen.

Informatie op internet kan bijvoorbeeld vooroordelen bevatten, zoals discriminerende aannames. Wordt deze informatie gebruikt voor training van algoritmes, dan kan dit leiden tot algoritmes met discriminerende effecten. Verder is er op internet heel veel onjuiste en misleidende informatie te vinden. Dat kan bijvoorbeeld leiden tot onjuiste informatievoorziening richting burgers. Daarnaast moeten organisaties ook bij het gebruik van algoritmes letten op risico's voor grondrechten, waaronder discriminatie.

Verantwoorde ontwikkeling en ingebruikname van algoritmes vereist dus dat ontwikkelaars ook deze risico's in de gaten houden en maatregelen nemen om die te voorkomen. Daarbij moeten zij niet alleen rekening houden met de AVG, maar ook met andere juridische kaders die algoritmes (gaan) reguleren. Zoals het gelijkebehandelingsrecht. Verder zal de AI-verordening specifieke regels stellen met het oog op de ontwikkeling van betrouwbare algoritmes.

11. Conclusie

Scraping van persoonsgegevens op internet maakt al snel een grote inbreuk op het recht op bescherming van persoonsgegevens van degenen van wie de gegevens worden gescrapet. Willen private organisaties en particulieren scraping of gescrapete persoonsgegevens gebruiken?⁵⁴ Dan moet dit gebruik voldoen aan de beginselen en eisen die de AVG stelt.⁵⁵

Allereerst moeten private organisaties of particulieren onderzoeken of zij een geslaagd beroep kunnen doen op een van de grondslagen uit artikel 6 AVG. Doorgaans zal voor hen alleen de grondslag 'gerechtvaardigd belang' eventueel in aanmerking komen. Deze richtlijnen helpen private organisaties en particulieren met het beoordelen van de vraag of zij een geslaagd beroep kunnen doen op deze grondslag. Als (ook) sprake is van het verwerken van bijzondere of strafrechtelijke persoonsgegevens, moeten zij beoordelen of sprake is van een uitzondering op het verwerkingsverbod voor dit soort gegevens.

De artikelen in de AVG die zien op grondslagen,⁵⁶ bijzondere persoonsgegevens⁵⁷ en strafrechtelijke persoonsgegevens,⁵⁸ zijn alle drie uitwerkingen van het beginsel van rechtmatigheid uit artikel 5 AVG. Deze richtlijnen gaan in het bijzonder over dat beginsel. Bij scraping of het gebruik van gescrapete gegevens zal het in veel gevallen lastig zijn om aan het beginsel van rechtmatigheid te voldoen. Dit is uiteraard wel afhankelijk van het doel en de specifieke kenmerken van de verwerking en van extra waarborgen die mogelijk zijn getroffen om de belangen van betrokkenen te beschermen.

⁵⁴ Deze richtlijnen zien niet op scraping of het gebruik van gescrapete persoonsgegevens door de overheid.

⁵⁵ Tenzij de AVG niet van toepassing is op de verwerking, zie hoofdstuk 3 van deze richtlijnen.

⁵⁶ Artikel 6 AVG.

⁵⁷ Artikel 9 AVG.

⁵⁸ Artikel 10 AVG.



Komt de verwerkingsverantwoordelijke die scraping of gescrapete gegevens wil gebruiken tot de conclusie dat sprake is van een geldige grondslag? En dat de verwerking niet in strijd is met de regels voor het verwerken van bijzondere en strafrechtelijke persoonsgegevens? Dan moet de verwerkingsverantwoordelijke daarna uiteraard ook nog zorgvuldig beoordelen of de beoogde verwerking voldoet aan de andere beginselen en eisen van de AVG.