bB

# DAGVAARDING

Vandaag,_____tweeduizendentwintig,
op het verzoek van:

1. De stichting **The Privacy Collective**, statutair gevestigd te Amsterdam, en kantoorhoudende te (3511 GM) Catharijnesingel 73, Utrecht;

   te dezer zake woonplaats kiezende te (1075 BR) Amsterdam aan de Sophialaan 8, ten kantore van bureau Brandeis B.V. van wie mr. Chr. A. Alberdingk Thijm en mr. F.M. Peters door eiser als advocaat worden gesteld en als zodanig zullen optreden met het recht van substitutie;

## GEDAGVAARD:

1. De besloten vennootschap met beperkte aansprakelijkheid **Oracle Nederland B.V.**, statutair gevestigd te Utrecht en kantoorhoudende te (3543 AS) Hertogswetering 163, Utrecht, aldaar aan dat adres mijn exploot doende en afschrift dezes latende aan:

2. De besloten vennootschap met beperkte aansprakelijkheid **SFDC Netherlands B.V.**, statutair gevestigd te Amsterdam en kantoorhoudende te (1081 LA) Gustav Mahlerlaan 2970, The Edge, Amsterdam, aldaar aan dat adres mijn exploot doende en afschrift dezes latende aan:

3. De vennootschap naar vreemd recht **Oracle Corporation**, gevestigd te Redwood Shores en kantoorhoudende te (CA 94065), Redwood Shores, 500 Oracle Parkway, Californië, Verenigde Staten, zonder bekende woonplaats of bekend werkelijk verblijf in Nederland.

   Zodoende heb ik uit krachte van artikel 55 lid 1 van het Wetboek van Burgerlijke Rechtsvordering mijn exploot gedaan aan het parket van de ambtenaar van het openbaar ministerie bij de rechtbank Amsterdam, alwaar ik te (1013 MM) IJdok 163, Amsterdam, twee afschriften van deze dagvaarding, waarvan de Engelse vertaling onverwijld zal worden nagezonden, heb gelaten aan:

aldaar werkzaam en aanwezig.

Verzocht wordt dit exploot, voorzien van de vertaling van die stukken in de Engelse taal, aan **Oracle Corporation** te doen betekenen/kennisgeven overeenkomstig de artikelen 3 tot en met 6 van het Verdrag inzake de betekening en de kennisgeving in het buitenland van gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 (het "Verdrag"), en wel door betekening of kennisgeving met inachtneming van de vormen in de wetgeving van de aangezochte lidstaat voorgeschreven voor de betekening of de kennisgeving van stukken, die in dat land zijn opgemaakt en bestemd zijn voor zich aldaar bevindende personen, waarbij aan de in artikel 6 van het Verdrag bedoelde (centrale) autoriteit voorts verzocht wordt een afschrift van dit exploot te retourneren, vergezeld van de verklaring als bedoeld in artikel 6 van het Verdrag.

Voorts wordt een afschrift van dit exploot voorzien van de vertaling van die stukken in de Engelse taal onverwijld door mij per aangetekende brief en per UPS koerier gezonden aan het adres van **Oracle Corporation** voornoemd en voorts heb ik in overeenstemming met artikel 10 sub b van het Verdrag inzake de betekening en kennisgeving in het buitenland van gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 vandaag een afschrift van dit exploot zonder producties, met vertaling daarvan in de Engelse taal, toegezonden aan een daartoe in de staat Californië (Verenigde Staten van Amerika), bevoegde deurwaarder, ambtenaar of andere bevoegde persoon met het verzoek betekening of kennisgeving hiervan te doen verrichten aan **Oracle Corporation** met inachtneming van de vormen in de wetgeving van de staat Californië (Verenigde Staten van Amerika) voorgeschreven.

4. De vennootschap naar vreemd recht **Oracle America, Inc.**, gevestigd te Redwood Shores en kantoorhoudende te (CA 94065), Redwood Shores, 500 Oracle Parkway, Californië, Verenigde Staten, zonder bekende woonplaats of bekend werkelijk verblijf in Nederland.

   Zodoende heb ik uit krachte van artikel 55 lid 1 van het Wetboek van Burgerlijke Rechtsvordering mijn exploot gedaan aan het parket van de ambtenaar van het openbaar ministerie bij de rechtbank Amsterdam, alwaar ik te (1013 MM) IJdok 163, Amsterdam, twee afschriften van deze dagvaarding, waarvan de Engelse vertaling onverwijld zal worden nagezonden, heb gelaten aan:

   aldaar werkzaam en aanwezig.

   Verzocht wordt dit exploot, voorzien van de vertaling van die stukken in de Engelse taal, aan **Oracle America, Inc.**, te doen betekenen/kennisgeven overeenkomstig de artikelen 3 tot en met 6 van het Verdrag inzake de betekening en de kennisgeving in het buitenland van gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 (het "Verdrag"), en wel door betekening of kennisgeving met inachtneming van de vormen in de wetgeving van de aangezochte lidstaat voorgeschreven voor de betekening of de kennisgeving van stukken, die in dat land zijn opgemaakt en bestemd zijn voor zich aldaar

bevindende personen, waarbij aan de in artikel 6 van het Verdrag bedoelde (centrale) autoriteit voorts verzocht wordt een afschrift van dit exploot te retourneren, vergezeld van de verklaring als bedoeld in artikel 6 van het Verdrag.

Voorts wordt een afschrift van dit exploot voorzien van de vertaling van die stukken in de Engelse taal onverwijld door mij per aangetekende brief en per UPS koerier gezonden aan het adres van **Oracle America, Inc.**, voornoemd en voorts heb ik in overeenstemming met artikel 10 sub b van het Verdrag inzake de betekening en kennisgeving in het buitenland van gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 vandaag een afschrift van dit exploot zonder producties, met vertaling daarvan in de Engelse taal, toegezonden aan een daartoe in de staat Californië (Verenigde Staten van Amerika), bevoegde deurwaarder, ambtenaar of andere bevoegde persoon met het verzoek betekening of kennisgeving hiervan te doen verrichten aan **Oracle America, Inc.** met inachtneming van de vormen in de wetgeving van de staat Californië (Verenigde Staten van Amerika) voorgeschreven.

5. De vennootschap naar vreemd recht **Salesforce.com, Inc.**, gevestigd te San Francisco en kantoorhoudende te (CA 94105) San Francisco, 415 Mission Street, 3rd Floor, Salesforce Tower, Californië, Verenigde Staten, zonder bekende woonplaats of bekend werkelijk verblijf in Nederland.

   Zodoende heb ik uit krachte van artikel 55 lid 1 van het Wetboek van Burgerlijke Rechtsvordering mijn exploot gedaan aan het parket van de ambtenaar van het openbaar ministerie bij de rechtbank Amsterdam, alwaar ik te (1013 MM) IJdok 163, Amsterdam, twee afschriften van deze dagvaarding, waarvan de Engelse vertaling onverwijld zal worden nagezonden, heb gelaten aan:

   aldaar werkzaam en aanwezig.

   Verzocht wordt dit exploot, voorzien van de vertaling van die stukken in de Engelse taal, aan **Salesforce.com, Inc.**, te doen betekenen/kennisgeven overeenkomstig de artikelen 3 tot en met 6 van het Verdrag inzake de betekening en de kennisgeving in het buitenland van gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 (het "Verdrag"), en wel door betekening of kennisgeving met inachtneming van de vormen in de wetgeving van de aangezochte lidstaat voorgeschreven voor de betekening of de kennisgeving van stukken, die in dat land zijn opgemaakt en bestemd zijn voor zich aldaar bevindende personen, waarbij aan de in artikel 6 van het Verdrag bedoelde (centrale) autoriteit voorts verzocht wordt een afschrift van dit exploot te retourneren, vergezeld van de verklaring als bedoeld in artikel 6 van het Verdrag.

   Voorts wordt een afschrift van dit exploot voorzien van de vertaling van die stukken in de Engelse taal onverwijld door mij per aangetekende brief en per UPS koerier gezonden aan het adres van **Salesforce.com, Inc.**, voornoemd en voorts heb ik in overeenstemming met artikel 10 sub b van het Verdrag inzake de betekening en kennisgeving in het buitenland van

gerechtelijke en buitengerechtelijke stukken in burgerlijke- en handelszaken van 15 november 1965 vandaag een afschrift van dit exploot zonder producties, met vertaling daarvan in de Engelse taal, toegezonden aan een daartoe in de staat San Francisco (Verenigde Staten van Amerika), bevoegde deurwaarder, ambtenaar of andere bevoegde persoon met het verzoek betekening of kennisgeving hiervan te doen verrichten aan **Salesforce.com, Inc.** met inachtneming van de vormen in de wetgeving van de staat San Francisco (Verenigde Staten van Amerika) voorgeschreven.

**OM:**

Op **woensdag 9 december tweeduizendtwintig om 10.00 uur** niet in persoon maar vertegenwoordigd door een advocaat te verschijnen ter terechtzitting van de rechtbank Amsterdam, team Civiel recht, afdeling handelszaken, alsdan te houden in één van de lokalen van het gerechtsgebouw aan de Parnassusweg 220 te (1076 AV) Amsterdam.

**MET AANZEGGING DAT:**

a. indien een gedaagde verzuimt advocaat te stellen of het hierna te noemen griffierecht niet tijdig betaalt, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechter verstek tegen die gedaagde zal verlenen en de hierna omschreven vordering zal toewijzen, tenzij deze hem onrechtmatig of ongegrond voorkomt;

b. indien ten minste één van de gedaagden in het geding verschijnt en het griffierecht tijdig heeft voldaan, tussen alle partijen één vonnis zal worden gewezen, dat als een vonnis op tegenspraak wordt beschouwd;

c. bij verschijning in het geding van ieder van de gedaagden een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning;

d. de hoogte van de griffierechten is vermeld in de meest recente bijlage behorend bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website: www.kbvg.nl/griffierechtentabel;

e. van een persoon die onvermogend is, een bij of krachtens de wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:

   1e een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand, dan wel

2e een verklaring van het bestuur van de raad voor rechtsbijstand, bedoeld in artikel 7, derde lid, onderdeel e, van de Wet op de rechtsbijstand waaruit blijkt dat zijn inkomen niet meer bedraagt dan de inkomens bedoeld in de algemene maatregel van bestuur krachtens artikel 35, tweede lid, van die wet.

f. van gedaagden die bij dezelfde advocaat verschijnen en gelijkluidende conclusies nemen of gelijkluidend verweer voeren, op basis van artikel 15 van de Wet griffierechten burgerlijke zaken slechts eenmaal een gezamenlijk griffierecht wordt geheven.

g. de producties behorende bij deze dagvaarding onverwijld zullen worden nagezonden.

**MET MEDEDELING DAT**:

eiser binnen twee dagen na indiening van de dagvaarding het exploot van dagvaarding ter griffie indient en gelijktijdig aantekening maakt van de dagvaarding in het centraal register voor collectieve acties als bedoeld in artikel 305a, zevende lid, van Boek 3 van het Burgerlijk Wetboek, www.rechtspraak.nl/Registers/centraal-register-voor-collectieve-vorderingen. De aantekening zal vergezeld gaan van een afschrift van de dagvaarding.

bB

## Inhoud

**Begrippen en afkortingen** ..... **10**
Technische begrippen ..... 10
Afkortingen ..... 11
**1 Inleiding** ..... **12**
1.1 Kern van de zaak ..... 12
1.2 Leeswijzer ..... 13
1.3 Belang van de zaak ..... 15
**2 Partijen** ..... **19**
2.1 Stichting The Privacy Collective ..... 19
2.2 Oracle en Salesforce ..... 21
**3 De handelwijze van Oracle en Salesforce** ..... **24**
3.1 Wat is een DMP? ..... 24
3.2 De handelingen die Oracle en Salesforce verrichten ..... 24
3.2.1 Het plaatsen van cookies ..... 27
3.2.2 Het verzamelen van gegevens ..... 30
3.2.3 Het creëren van profielen ..... 32
3.2.4 Het verrijken van profielen met informatie uit andere bronnen ..... 35
3.2.5 Het gebruik van profielen voor RTB ..... 43
3.2.6 Cookie syncing: het koppelen van cookies om internetgebruikers nog beter te volgen ..... 46
3.3 Onderzoek naar de handelingen van Oracle en Salesforce ..... 47
3.3.1 Onderzoek Dr. Bashir ..... 47
3.3.2 Inzage in segmenten van Oracle ..... 50
3.4 Datalekken bij Oracle en Salesforce ..... 50
**4 Juridisch kader** ..... **52**
4.1 Inleiding ..... 52
4.2 Schending artikelen 7, 8 en 11 van het Handvest ..... 54
4.3 Toepasselijkheid AVG en artikel 11.7a Tw ..... 60
4.3.1 Verwerking van persoonsgegevens ..... 60
4.3.2 Artikel 11.7a Tw ..... 67
4.4 Verantwoordelijkheid ..... 69
4.4.1 De “verwerkingsverantwoordelijke” ..... 71
4.4.2 Ruime uitleg ..... 73
4.4.3 Oracle en Salesforce zijn verwerkingsverantwoordelijke ..... 74
4.5 Territoriale toepasselijkheid ..... 78
4.5.1 Territoriale toepasselijkheid AVG ..... 78
4.5.2 Territoriale toepasselijkheid artikel 11.7a Tw ..... 83
4.6 Schending AVG en Tw ..... 83

4.6.1 Geautomatiseerde besluitvorming waaronder profilering ..... 84
4.6.2 Rechtmatigheid – verwerking niet rechtmatig, geen geldige toestemming ..... 90
4.6.3 Verwerking niet transparant ..... 103
4.6.4 Verwerking in strijd met dataminimalisatie ..... 120
4.6.5 Verboden doorgifte aan de Verenigde Staten ..... 126
4.6.6 Overige inbreuken ..... 129
4.7 Oracle beschermt persoonsgegevens onvoldoende, blijkens een datalek in 2020 ..... 138
4.7.1 Beveiligingsplicht ..... 138
4.7.2 Datalek is inbreuk in verband met beveiliging ..... 139
4.7.3 Conclusie ten aanzien van beveiliging ..... 140
**5 Aansprakelijkheid en schade ..... 140**
5.1 Primair: Aansprakelijkheid op grond van de AVG ..... 140
5.2 Schenden AVG, toerekenbaarheid en relativiteit ..... 143
5.2.1 Uitgangspunt: Oracle en Salesforce worden vermoed persoonsgegevens te verwerken (artikel 11.7a lid 4 Tw) ..... 143
5.2.2 Uitgangspunt: Oracle en Salesforce zijn verwerkingsverantwoordelijke in de zin van de AVG ..... 144
5.2.3 Uitgangspunt: bewijslast naleving beginselen AVG rust op Oracle en Salesforce ..... 145
5.3 Causaal verband tussen schade en schending van de AVG wordt aangenomen ..... 146
5.4 Enkele betrokkenheid voldoende voor medeaansprakelijkheid ..... 146
5.5 Recht op schadevergoeding op grond van artikel 82 AVG ..... 146
5.5.1 Inleiding ..... 146
5.5.2 Schadebegrip in het kader van de AVG ..... 147
5.5.3 Immateriële schadevergoeding ..... 148
5.5.4 Berekening hoogte immateriële schadevergoeding ..... 151
5.5.5 Materiële schadevergoeding ..... 157
5.6 Aansprakelijkheid van Oracle vanwege Datalek ..... 162
5.7 Subsidiair: Overige aansprakelijkheidsgronden ..... 163
5.7.1 Aansprakelijkheid op grond van de onrechtmatige daad ..... 163
5.7.2 Artikel 6:162 BW dient AVG-conform te worden uitgelegd ..... 163
5.7.3 Onrechtmatige daad, relativiteit en toerekenbaarheid ..... 164
5.7.4 Toerekening ..... 165
5.7.5 Causaal verband ..... 165
5.7.6 Schade ..... 167
5.8 Ongerechtvaardigde verrijking ..... 170
5.8.1 Inleiding ..... 170
5.8.2 Verrijking ..... 170
5.8.3 Verarming ..... 175

5.8.4 Causaal verband is aanwezig ..... 177
5.8.5 Ongerechtvaardigde verrijking ..... 178
5.8.6 Omvang van de vordering ..... 179
5.9 Hoofdelijke aansprakelijkheid ..... 179
5.9.1 Hoofdelijke aansprakelijkheid op grond van de AVG ..... 179
5.9.2 Hoofdelijke aansprakelijkheid op grond van het BW ..... 179
**6 Toelichting op het petitum ..... 181**
6.1 Wet afwikkeling massaschade in collectieve actie ..... 181
6.2 Omschrijving groepen Gedupeerden ..... 182
6.3 Exclusieve belangenbehartiger ..... 183
6.4 Toelichting vorderingen ..... 183
6.5 Mogelijke constructies voor het betalen van schade en/of het schikken ..... 185
6.6 Vergoeding Financier ..... 186
6.7 Proceskostenveroordeling ..... 187
6.7.1 Proceskostenopgave ..... 187
6.7.2 Artikel 1018l lid 2 Rv ..... 188
6.7.3 Artikel 237 Rv ..... 188
6.8 Buitengerechtelijke kostenveroordeling ..... 188
**7 Bewijs ..... 189**
7.1 Inleiding ..... 189
7.2 Bewijsrechtelijke uitgangspunten ..... 190
7.3 Subsidiair: verzoek tot het leveren van bewijs door een deskundigenbericht te bevelen ex artikel 194 Rv ..... 190
7.4 Subsidiair: andere mogelijkheden om noodzakelijke informatie te verkrijgen in onderhavige zaak ..... 191
7.5 Waarheidsplicht (artikel 21 Rv) ..... 193
7.6 Bewijsverrichtingen op grond van artikel 22 Rv ..... 193
7.7 Vordering tot het verstrekken van informatie door Oracle en Salesforce ..... 194
7.8 Stichting biedt bewijs aan ..... 196
**8 Ontvankelijkheid van de Stichting ..... 196**
8.1 Algemeen: de recente herziening van artikel 3:305a BW en het thans geldende normenkader ..... 196
8.2 Gelijksoortigheidsvereiste ..... 197
8.3 Statutenvereiste ..... 198
8.4 Waarborgvereiste ..... 199
8.4.1 (i) Stichting is representatief voor de groep Gedupeerden ..... 200
8.4.2 (ii) De eisen van art. 3:305a lid 2 sub a tot en met e BW ..... 201
8.4.3 Stichting voldoet aan eisen van de Claimcode ..... 206
8.5 Aanvullende ontvankelijkheidseisen ..... 211

8.5.1 Inleiding ..... 211
8.5.2 Geen winstoogmerk ..... 211
8.5.3 Voldoende nauwe band met de Nederlandse rechtssfeer ..... 211
8.5.4 Stichting heeft Oracle en Salesforce uitgenodigd voor overleg ..... 212
8.6 Conclusie ..... 212
**9 Rechtsmacht en toepasselijk recht ..... 213**
9.1 Rechtsmacht ..... 213
9.1.1 Primair: 79 lid 2 GDPR ..... 213
9.1.2 Subsidiair: artikel 2 jo. artikel 7 Wetboek van Burgerlijke Rechtsvordering ..... 213
9.2 Toepasselijk recht ..... 214
**10 Bekende verweren en weerlegging ..... 215**
10.1 Verweren Oracle ..... 215
10.2 Verweren Salesforce ..... 217
**11 Petitum ..... 218**
**Productieoverzicht ..... 224**

## BEGRIPPEN EN AFKORTINGEN

### Technische begrippen

| Begrip | Definitie |
|---|---|
| **Ad tech** of **Advertising technology** | Verzamelnaam voor ondernemingen die zich bezig houden met het aanbieden van advertenties via internet |
| **Advertentieruimte** | Deel van een webpagina dat gereserveerd is voor het tonen van advertenties |
| **Advertiser** of **Marketer** | Adverteerder, de partij die advertentieruimte inkoopt |
| **Publisher** | Houder van een website en verkoper van advertentieruimte |
| **Ad exchange** | Veilinghuis waarin advertentieruimte wordt verhandeld |
| **Bid request** | Verzoek van een Publisher om te bieden op advertentieruimte. Het bid request wordt, samen met persoonsgegevens van de internetgebruiker, verstuurd naar een of meer Ad exchanges, die het verzoek doorsturen naar Advertisers |
| **DSP** of **Demand Side Platform** | Gespecialiseerd in het inkopen van de meest geschikte advertentieruimte namens Advertisers |
| **SSP** of **Supply Side Platform** | Gespecialiseerd in het verkopen van advertentieruimte namens een Publisher |
| **RTB** of **Real Time Bidding** | Het proces waarbij advertentieruimte wordt verhandeld via Ad exchanges. Publishers (middels SSPs) bieden advertentieruime op hun websites te koop aan, Advertisers (middels DSPs) bieden erop om advertenties te tonen |
| **DMP** of **Data Management Platform** | Gespecialiseerd in het verzamelen, beheren en verrijken van gegevens over internetgebruikers, het plaatsen van cookies en uitwisselen van gegevens door middel van cookie syncing, en het maken van profielen om de internetgebruiker de meest geschikte advertenties te tonen |
| **CTR** of **Click-through Rate** | Percentage van het totaal aantal getoonde advertenties waarop een gebruiker klikt |
| **Cookie** | Klein tekstbestand die bij het bezoek van een website op de computer van de bezoeker wordt geplaats waarin informatie opgeslagen kan worden |
| **First party cookie** | Cookie die geplaatst wordt door de website waarop de gebruiker zich bevindt. Als een gebruiker op nieuws.nl komt, dan is een cookie geplaatst door nieuws.nl een first party cookie |
| **Third party cookie** | Cookie die geplaatst wordt door de website waarop de gebruiker zich bevindt. Als een gebruiker op nieuws.nl komt, dan is een cookie geplaatst door een ander domein dan nieuws.nl een third party cookie |
| **Cookie ID** | Unieke identificator, opgeslagen in een cookie, waarmee de bezoeker steeds herkend kan worden bij opeenvolgende bezoeken |
| **Cookie syncing** | Het uitwisselen van Cookie IDs tussen verschillende partijen in de ad tech markt, zodat al deze partijen gemakkelijk over een persoon kunnen communiceren |
| **First party data** | Eigen gegevens van een Publisher of Advertiser |
| **Second party data** | Benaming van Oracle voor gegevens van een andere dienst van Oracle zelf. Bijvoorbeeld gegevens die verzameld zijn met Oracle's dienst AddThis |
| **Third party data** | Gegevens van (andere) partijen dan de DMP of Publisher zelf, zoals ingekochte gegevens van data partners en andere datahandelaren |

| | |
|---|---|
| **Profilering** | Het evalueren van persoonlijke aspecten van consumenten met het doel persoonlijke voorkeuren, interesses, gedrag en andere kenmerken van consumenten te analyseren of te voorspellen. Profilering wordt vaak gedaan op basis van een combinatie van First en Third party data |
| **DNT** of **Do Not Track** | Browserinstelling waarmee internetgebruikers een geautomatiseerd verzoek sturen naar derden om niet gevolgd te worden. Het verzoek wordt niet technisch afgedwongen |
| **Partner Cookie Policy** | Een cookie policy of cookiebeleid is een informatiepagina van een website over de cookies die via de website worden geplaatst. Ten opzichte van de DMP wordt dit een Partner Cookie Policy genoemd |
| **Landing page** | Voorpagina van een website |

**Afkortingen**

| Afkorting | Definitie |
|---|---|
| **ACM** | Autoriteit Consument & Markt |
| **Afdeling** | Afdeling Bestuursrechtspraak van de Raad van State |
| **AP** | Autoriteit Persoonsgegevens |
| **AVG** | Algemene Verordening Gegevensbescherming |
| **DMP** | Data Management Platform |
| **EDPB** | European Data Protection Board |
| **EDPS** | European Data Protection Supervisor |
| **EHRM** | Europees Hof voor de Rechten van de Mens |
| **EER** | Europese Economische Ruimte |
| **EU** | Europese Unie |
| **EVRM** | Europees Verdrag voor de Rechten van de Mens |
| **FTC** | Federal Trade Commission |
| **Handvest** | Handvest van de grondrechten van de Europese Unie |
| **HvJEU** | Hof van Justitie van de Europese Unie |
| **ICO** | Information Commissioner's Office |
| **Nauw Omschreven Groep** | Benadeelde personen voor wier belangen in de procedure wordt opgekomen |
| **Privacyshieldbesluit** | EU-VS Privacy Shield |
| **Tw** | Telecommunicatiewet |
| **UAVG** | Uitvoeringswet Algemene Verordening Gegevensbescherming |
| **VEU** | Verdrag betreffende de Europese Unie |
| **VWEU** | Verdrag betreffende de werking van de Europese Unie |
| **WAMCA** | Wet afwikkeling massaschade in collectieve actie |
| **Wbp** | Wet bescherming persoonsgegevens |
| **WG29** | Artikel 29-werkgroep (opgevolgd door EDPB) |

# 1 INLEIDING

## 1.1 Kern van de zaak

1. Deze zaak heeft betrekking op een van de grootste onrechtmatige gegevensverwerkingen in de geschiedenis van het internet. Het gaat om de verwerking van persoonsgegevens van praktisch alle Nederlanders[1] die informatie op het internet lezen of bekijken. Het gaat om een verwerking die onbeperkt is in tijd en dagelijks op grote schaal plaatsvindt. De verwerking geschiedt louter om commerciële doeleinden, zonder rechtvaardigingsgrond. Het heeft tot gevolg dat de persoonlijke eigenschappen van iedereen die online is, voortdurend op onrechtmatige wijze worden verzameld en uitgewisseld, zonder dat internetgebruikers daar kennis van hebben.

2. Oracle en Salesforce verzamelen in het kader van een dienst, die ook wel Data Management Platform ("**DMP**") wordt genoemd, op ongekende schaal persoonsgegevens van internetgebruikers, verwerken deze in gedetailleerde profielen, en verkopen deze informatie aan derden om hen onder meer in staat te stellen gepersonaliseerde advertenties aan te bieden op websites. De gegevensverzameling begint met het door Oracle en Salesforce plaatsen van een cookie[2] op de randapparatuur van de internetgebruiker. Die cookie is uitgerust met een unieke identificator waarmee internetgebruikers van elkaar worden onderscheiden. Met behulp van de cookie worden persoonsgegevens verzameld, zoals het IP-adres van de internetgebruiker. Oracle en Salesforce volgen de internetgebruiker over diverse apparaten die hij gebruikt en verzamelen daarbij andere unieke identificatoren zoals die van een mobiele telefoon of gepseudonimiseerde e-mailadressen. Zo ontstaat een vingerafdruk van de gebruiker waaraan een uniek profiel wordt gekoppeld.

3. Oracle en Salesforce verrijken de gegevens vergaard via de cookie en andere unieke identificatoren met informatie uit alternatieve bronnen. Het gaat daarbij niet alleen om online aankoop- en klikgedrag, maar ook om informatie uit offline bronnen, zoals van een loyaltyprogramma van een supermarkt. Op die manieren bouwen Oracle en Salesforce op dagelijkse basis aan een profiel zodat een zo volledig mogelijk overzicht ontstaat van de karaktereigenschappen en interesses van de betreffende persoon. Oracle en Salesforce bieden adverteerders de middelen om internetgebruikers te segmenteren en een unieke "audience" te creëren.

4. Het doel van de gegevensverwerkingen is onder meer om het profiel van de internetgebruiker te delen in een proces dat Real Time Bidding ("**RTB**") wordt genoemd. Wie een website bezoekt, wordt ongemerkt object in een veilingproces. In een fractie van een seconde, nog voordat de website is geladen, wordt het profiel van de internetgebruiker, met daarin zijn voorkeuren en interesses, aangeboden aan potentieel honderden partijen. Die partijen gebruiken de gegevens om te bieden op de ruimte om een advertentie te tonen aan de internetgebruiker. De hoogste bieder toont op basis hiervan een advertentie die zoveel

[1] In deze dagvaarding zal voor de leesbaarheid gesproken worden over 'Nederlanders' en 'Nederlandse internetgebruikers' – bedoeld wordt al die personen, die sinds de toepasselijkheid van de AVG in of vanuit Nederland gebruik hebben gemaakt van het internet.
[2] Een cookie is tekstbestand die een websitehouder of derde partij bij een bezoek aan een website of andere online handeling op het apparaat van de internetgebruiker kan plaatsen om informatie te verzamelen die later gebruikt wordt. Cookies kunnen een voor de internetgebruiker nuttige toepassing hebben, zoals het opslaan van wachtwoorden zodat de internetgebruiker deze niet steeds opnieuw hoeft in te voeren, maar bijvoorbeeld ook gebruikt worden om gegevens te verzamelen om een profiel van een internetgebruiker te creëren.

mogelijk aansluit bij de karaktereigenschappen en interesses van de internetgebruiker. Gedurende dit proces worden de unieke identificatoren uitgewisseld met andere commerciële partijen en aan elkaar gekoppeld. Dit proces wordt "cookie syncing" genoemd, waarover later in deze dagvaarding meer.

5. Dit alles gebeurt op geautomatiseerde wijze en zonder dat de internetgebruiker ervan op de hoogte is.

6. Oracle en Salesforce spelen met hun DMP dienst een cruciale rol in het RTB-proces. Oracle en Salesforce plaatsen in dit kader de cookies op de randapparatuur van de internetgebruiker. Oracle en Salesforce verrijken de gegevens en zijn verantwoordelijk voor het uitwisselen van de unieke identificatoren en daaraan gekoppelde informatie, zodat een zo volledig mogelijk beeld ontstaat van de internet. Het verrijkte profiel wordt zo object in het veilingproces.

7. Met deze zaak beoogt Stichting The Privacy Collective (hierna ook wel de "**Stichting**") deze handelwijze een halt toe te roepen en de schade die de personen lijden wier belangen zij behartigt, vergoed te krijgen.

### 1.2 Leeswijzer

8. In deze dagvaarding zal in het navolgende eerst het belang van de zaak worden geschetst (randnummer 1.3). Daarbij zal onder meer worden gewezen op het grote aantal klachten dat is ingediend bij toezichthouders, die echter tot op heden niet tot het opleggen van een sanctie aan Oracle en Salesforce of andere partijen hebben geleid. De Stichting ziet in deze zaak de enig resterende mogelijkheid tot effectieve handhaving: het in een collectieve actie vorderen van schadevergoeding die recht doet aan de schendingen van het recht op privacy en gegevensbescherming die zich in de onderhavige zaak stelselmatig voordoen.

9. Vervolgens zal de positie en rol van de Stichting worden toegelicht (hoofdstuk 2). Aansluitend zal ingegaan worden op de technische handelwijze van Oracle en Salesforce (hoofdstuk 3). Dit vereist een omschrijving van het proces RTB en de partijen die op deze markt actief zijn. Het betreft technisch complexe materie. In dit hoofdstuk zal ook uiteen worden gezet op welke wijze de Stichting onderzoek heeft laten doen naar de handelwijze van Oracle en Salesforce door een technische deskundige.

10. Vervolgens wordt het juridisch kader behandeld (hoofdstuk 4). Daarin zal uiteen worden gezet hoe Oracle en Salesforce dagelijks fundamentele rechten schenden en inbreuk plegen op een groot aantal bepalingen uit de Algemene Verordening Gegevensbescherming ("**AVG**")[3] en de Telecommunicatiewet ("**Tw**"). Hiertoe zullen allereerst de relevante fundamentele rechten worden besproken, mede in het licht van het grote belang dat het Hof van Justitie van de Europese Unie ("**HvJEU**") in zijn jurisprudentie hecht aan strikte naleving van de grondrechten uit het Handvest van de grondrechten van de Europese Unie ("**Handvest**").

11. Aangetoond zal worden dat Oracle en Salesforce op enorme schaal persoonsgegevens verwerken in de zin van de AVG en voor die verwerking (gezamenlijk)

[3] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 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.

verwerkingsverantwoordelijke zijn. Ook zal de territoriale toepasselijkheid worden onderbouwd.

12. Hierop volgt een behandeling van de beginselen en bepalingen uit de AVG en de Tw waarop Oracle en Salesforce inbreuk maken. De Stichting zal laten zien dat Oracle en Salesforce stelselmatig de AVG schenden, onder meer door:

    i. gedetailleerde profielen op te stellen en te onderhouden van internetgebruikers ("profilering") en deze in te zetten voor geautomatiseerde verwerkingen die hen in aanmerkelijke mate treffen ("geautomatiseerde besluitvorming")

    ii. zonder rechtmatige grondslag de gegevens van internetgebruikers te verzamelen en verwerken, onder meer door zonder geldige toestemming cookies te plaatsen op de randapparatuur van internetgebruikers;

    iii. onvoldoende transparantie in acht te nemen over hun handelwijze, bijvoorbeeld ten aanzien van de uitwisseling van unieke identificatoren van cookies met andere partijen ("cookie syncing");

    iv. in strijd te handelen met het vereiste van dataminimalisatie door onbeperkt en bovenmatig persoonsgegevens te verzamelen, combineren en delen;

    v. persoonsgegevens te verwerken in strijd met de doeleinden waarvoor deze oorspronkelijk zijn verzameld, onvoldoende passende beveiliging in acht te nemen, in strijd te handelen met hun verantwoordingsplicht en persoonsgegevens door te geven aan landen zonder passend beschermingsregime.

13. In het volgende hoofdstuk zal de aansprakelijkheid van Oracle en Salesforce worden besproken en hun verplichting om de schade die internetgebruikers lijden en hebben geleden te vergoeden (hoofdstuk 5). De primaire grondslag voor vergoeding van de schade is de schending van de relevante fundamentele rechten alsmede de inbreuk op de AVG en Tw. Mede gelet op de aard, de ernst, de duur en het opzettelijke karakter van de inbreuk wordt deze schade per partij begroot op € 500 per persoon per gedaagde (wat Oracle betreft te vermeerderen met € 100 per persoon vanwege een nog te bespreken datalek).

14. De Stichting beroept zich subsidiair en meer subsidiair op aansprakelijkheid van Oracle en Salesforce uit hoofde van onrechtmatige daad en ongerechtvaardigde verrijking. Voorzover meerdere verwerkingsverantwoordelijken of verwerkers betrokken zijn bij de activiteiten van Oracle en Salesforce wordt toegelicht dat zij hoofdelijk aansprakelijk zijn voor de schade die door de verwerking is veroorzaakt. Aansluitend volgt een toelichting op het petitum (hoofdstuk 6), een uiteenzetting van de bewijsrechtelijke aspecten van de zaak (hoofdstuk 7), een hoofdstuk over de ontvankelijkheid van de stichting (hoofdstuk 8), een toelichting op de rechtsmacht en het toepasselijke recht (hoofdstuk 9) en een weerlegging van de verweren van Oracle en Salesforce (hoofdstuk 10).

### 1.3 Belang van de zaak

15. Het systeem dat Oracle en Salesforce in stand houden en faciliteren ligt internationaal sterk onder vuur, zowel vanuit de politiek als de maatschappij. De kritiek op de ongebreidelde gegevensverwerkingen ten behoeve van onder meer RTB klinkt zowel in de VS als in de Europese Unie. Toezichthouders worden wereldwijd opgeroepen deze praktijken een halt toe te roepen.

16. Op 31 juli 2020 verzoeken senatoren en congresleden van zowel de Republikeinse als de Democratische partij de Amerikaanse toezichthouder Federal Trade Commission ("**FTC**") in te grijpen om de ongeëvenaarde privacyschending te stoppen die via RTB dagelijks wordt gepleegd.[4] "This outrageous privacy violation must be stopped and the companies that are trafficking in Americans' illicitly obtained private data should be shut down," schrijven ze in een brief aan de FTC, ondertekend door tien senatoren en congresleden, onder wie Elizabeth Warren. In de brief verwijzen ze naar onderzoeken van toezichthouders in de Europese Unie.

17. Privacy- en mensenrechtenorganisaties hebben klachten ingediend bij ten minste 14 Europese toezichthoudende autoriteiten op het gebied van de bescherming van privacy en persoonsgegevens. Dat is gebeurd in Polen,[5] België, Spanje, Luxemburg,[6] Duitsland, Frankrijk, Italië, Hongarije, Bulgarije, Tsjechië, Estland, Slovenië,[7] Nederland en Ierland.[8] In Nederland heeft de stichting Bits of Freedom in mei 2019 een klacht bij de Autoriteit Persoonsgegevens ("**AP**") ingediend met betrekking tot inbreuken op de rechten van Nederlanders in de RTB markt.[9]

18. Op 8 november 2018 dient Privacy International klachten in bij de Britse toezichthouder Information Commissioner's Office ("**ICO**")over de verwerking van persoonsgegevens door datahandelaren. De klacht is onder meer gericht tegen Oracle, omdat Oracle door aggregatie en tracking betrokkenen in duizenden categorieën indeelt. Uit analyse van de Britse markt blijkt dat Oracle 180,7 miljoen unieke IDs heeft en betrokkenen indeelt in 58,8 duizend interessesegmenten.[10] De klachten zien ook op zes andere datahandelaren en zijn gedaan in Frankrijk, Ierland en het Verenigd Koninkrijk.[11]

19. Op 6 april 2020 publiceert de Ierse privacytoezichthouder[12] een rapport over tracking technologieën.[13] De toezichthouder gaat met name in op de wijze waarop informatie wordt verstrekt aan en toestemming wordt verkregen van internetgebruikers die websites bezoeken.

---

[4] Brief van senatoren en congresleden aan FTC, 31 juli 2020, onder meer beschikbaar via: https://www.adexchanger.com/privacy/lawmakers-call-rtb-an-unfair-and-deceptive-business-practice-in-letter-to-the-ftc/
[5] https://techcrunch.com/2019/01/27/google-and-iab-ad-category-lists-show-massive-leakage-of-highly-intimate-data-gdpr-complaint-claims/.
[6] https://techcrunch.com/2019/05/20/gdpr-adtech-complaints-keep-stacking-up-in-europe/.
[7] https://www.tijd.be/tech-media/media-marketing/privacyklachten-tegen-hoe-google-advertenties-verdeelt/10140271.html.
[8] https://www.dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and.
[9] https://www.bitsoffreedom.nl/wp-content/uploads/2019/05/20190520-handhavingsverzoek-iab-google-openbaar.pdf.
[10] https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf, p. 6.
[11] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
[12] Data Protection Commission of DPC.
[13] https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Report%20by%20the%20DPC%20on%20the%20use%20of%20cookies%20and%20other%20tracking%20technologies.pdf.

De toezichthouder concludeert onder meer dat van de 38 onderzochte websites slechts twee materieel in overeenstemming met de AVG handelden.

20. Volgens de toezichthouder ontbreekt de meest basale informatie om rechtmatig toestemming te geven voor het plaatsen van cookies. Internetgebruikers hebben geen idee van de omvang van het tracken van hun apparaten, thuis en op werk:

> *"Lacking even basic information or the ability to give unambiguous consent for the placement of tracking technologies or cookies on their devices, most ordinary users will not be aware of the extent to which they may be tracked across their devices at home and at work, and across their browsing, reading and social habits."*[14]

> *"The fact that bad practices were widespread even among companies and controllers that are household names suggests a more systemic issue that must be tackled firstly with the publication of new guidance, followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance."*[15]

21. Een onderzoek van de Ierse privacytoezichthouder naar de *ad-tech* industrie en RTB is nog gaande.[16]

22. Ook de Britse ICO is zeer kritisch. De ICO publiceert op 20 juni 2019 een rapport over de *ad-tech* en RTB markt (**Productie 1**).[17] De toezichthouder concludeert onder meer dat in de *ad-tech* markt het recht op gegevensbescherming wordt genegeerd. De ICO geeft aan dat de informatieverstrekking aan betrokkenen onvoldoende is. De toezichthouder concludeert verder dat zeer gedetailleerde profielen worden gecreëerd en uitgewisseld tussen honderden partijen; dit alles zonder dat de betrokkenen hier kennis van hebben.

> *"profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individual's knowledge."*[18]

23. In januari 2020 publiceert de Noorse consumentenbond een uitgebreid onderzoek, inclusief technische analyse, naar het gebruik van persoonsgegevens in veelgebruikte apps.[19] De Noorse consumentenbond geeft aan dat het volgen en profileren van internetgebruikers voortdurend plaatsvindt:

> *"As we move around on the internet and in the real world, we are being continually tracked and profiled for the purpose of showing targeted advertising. In this report, we demonstrate how every time we use our phones, a large number of*

[14] Pagina 18.
[15] Pagina 19.
[16] https://www.dataprotection.ie/en/data-protection-commission-launches-statutory-inquiry-googles-processing-location-data-and.
[17] Information Commisioner's Office, *Update report into adtech and real time bidding*, 20 juni 2019 (**Productie 1**) te raadplegen via: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.
[18] Pagina 23.
[19] https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/.

*shadowy entities that are virtually unknown to consumers are receiving personal data about our interests, habits, and behaviour."*[20]

24. De Noorse consumentenbond beschrijft de rol van DMPs in de *ad-tech* markt als de dienst waarmee websitehouders en adverteerders hun eigen gegevens kunnen combineren met die van derde partijen. DMPs worden beschreven als gegevenshandelaren die gigantische identiteitsdatabases beheren waarmee profielen tussen verschillende partijen gekoppeld worden:

*"Data management platforms are used by publishers and marketers to combine data on their existing customers, including behavioural data collected from their websites and apps, with data from third party providers. They provide mechanisms to further analyse and refine data on consumers, and then analyse and utilize it across the web, mobile apps and other services. As a part of the RTB process, DMPs also provide instructions to DSPs about which consumers to target based on the profiles that they compile.*

*As data management platforms often resell large amounts of third party data to many clients, in addition to compiling and combining the data, they can also be categorized as a type of data broker. Most of them maintain massive identity databases that help other companies to link digital profiles across contexts and vendors."*[21]

25. De Noorse consumentenbond geeft daarbij aan dat onder meer Oracle en Salesforce tot de "major DMP vendors" behoren:

*"Major DMP vendors include Oracle, Adobe, Salesforce, Nielsen, Neustar, Lotame, The ADEX, KBM Group (owned by the major advertising agency group WPP). Several adtech companies also provide DMP functionality, including MediaMath, AdForm, and Google."*[22]

26. Het rapport leidt in Nederland tot een campagne van de Consumentenbond onder de naam "Datadelers: illegale datahandel"[23] en kamervragen aan Minister Dekker.[24]

27. Bij de evaluatie van de AVG in juni 2020 concludeert de Europese Commissie onder meer dat sterke handhaving jegens bedrijven in de advertentiesector noodzakelijk is om individuen te beschermen, vooral op het gebied van online reclame en "behavourial targeting":

*"Krachtige en doeltreffende handhaving van de AVG ten aanzien van grote digitale platforms en geïntegreerde ondernemingen, onder meer op gebieden als*

[20] Pagina 5.
[21] Pagina 37.
[22] Pagina 37, voetnoot 89.
[23] https://www.consumentenbond.nl/acties/datadealers, geraadpleegd op 30 april 2020.
[24] https://www.tweedekamer.nl/downloads/document?id=8e05af88-94d8-4f86-9998-68aecebd4779&title=Het%20bericht%20dat%20de%20Consumentenbond%20de%20noodklok%20luidt%20om%20illegale%20datahandel%20.pdf, geraadpleegd op 30 april 2020.

*onlinereclame en microtargeting, is bovendien essentieel om personen te kunnen beschermen."*[25]

28. Niettemin kondigt de Britse toezichthouder ICO op 7 mei 2020 aan het onderzoek naar RTB en de *ad-tech* industrie voorlopig op te schorten. De ICO geeft aan tijdens de Covid-19 crisis geen "undue pressure" te willen leggen op de industrie, ondanks haar zorgen over *ad-tech*. Ook het onderzoek van de Nederlandse AP naar aanleiding van de klacht van de stichting Bits of Freedom lijkt stil te liggen.

29. Belangenorganisaties geven aan dat de werkelijke reden dat opvolging van hun klachten uitblijft, schuilt in een gebrek aan middelen en de chronische onderbezetting van de toezichthouders.[26] Het gaat om een complexe markt waarbij een veelheid van spelers grotendeels achter de schermen opereren.

30. Het is in dit speelveld dat de Stichting uw rechtbank verzoekt om Oracle en Salesforce verantwoordelijk te houden voor de wijze waarop zij de dagelijks de fundamentele rechten van internetgebruikers alsmede de AVG en Tw schenden. De Stichting vraagt uw rechtbank dat te doen op een wijze die recht doet aan de schade die internetgebruikers hierdoor dagelijks lijden en die voldoende effectief en afschrikwekkend is.

31. Het HvJEU bevestigt keer op keer het belang van een hoog beschermingsniveau van het recht op bescherming van de persoonlijke levenssfeer en het gegevensbeschermingsrecht. Uit de jurisprudentie van het HvJEU volgt dat voorkomen moet worden dat er een gebrek aan verantwoordelijkheid bestaat. Gewaarborgd moet worden dat betrokkenen de garantie hebben van effectieve en volledige bescherming van hun rechten.[27]

32. Opmerkelijk is dat veel van de belangwekkende jurisprudentie van het HvJEU wordt geïnitieerd door belangenorganisaties of privacy-activisten. In de zaak *Breyer* bevestigt het HvJEU de ruime reikwijdte van het begrip persoonsgegeven en dat IP-adressen daaronder moeten worden geschaard.[28] De procedure is aangespannen door Patrick Breyer, Europarlementariër en activist op het gebied van digitale rechten, tegen de Duitse Staat. De Oostenrijker Max Schrems, advocaat en privacy-activist, geniet inmiddels wereldfaam door tot twee keer toe de gegevensuitwisseling tussen partijen in de Europese Unie en de VS een halt toe te roepen.[29] De belangenorganisatie Digital Rights Ireland zorgde ervoor dat het HvJEU de zogenoemde Dataretentierichtlijn ongeldig verklaarde, een richtlijn die telecomaanbieders verplichtte locatiegegevens op te slaan.[30] In de zaak *Fashion ID* is het de Duitse consumentenorganisatie Verbraucherzentrale NRW die het HvJEU ertoe beweegt de reikwijdte van het begrip (verwerkings)verantwoordelijke uit te leggen.[31] In de zaak *Planet49* is het de Duitse consumentenorganisatie Verbraucherzentrale Bundesverband die ervoor zorgt

[25] Europese Commissie, Mededeling van de Commissie aan het Europees Parlement en de Raad, "Gegevensbescherming als pijler van zeggenschap van de burger en de EU-aanpak van de digitale transformatie — twee jaar toepassing van de algemene verordening gegevensbescherming.", 24 juni 2020 (COM(2020) 264 final), te raadplegen via: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52020DC0264.
[26] Zie https://www.itpro.co.uk/policy-legislation/data-protection/356423/ico-lambasted-for-falling-asleep-at-the-wheel
[27] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13.
[28] HvJEU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*).
[29] HvJEU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*) en HvJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*).
[30] HvJEU 8 april 2014, zaak c-293/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
[31] HvJEU 29 juli 2019, , C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*).

dat het HvJEU vragen van uitleg beantwoordt over, onder meer, de uitleg van het toestemmingsvereiste bij het plaatsen van cookies.[32]

33. Het waarborgen van een hoog beschermingsniveau alsmede een doeltreffende en volledige bescherming van de fundamentele rechten op bescherming van de persoonlijke levenssfeer en gegevensbescherming leidt ertoe dat lidstaten alle passende maatregelen moeten nemen om onverkorte nakoming van de AVG te garanderen.[33] De AVG hecht dan ook aan private handhaving en biedt veel ruimte aan collectieve belangenbehartiging. Artikel 79 AVG garandeert het recht op een doeltreffende voorziening in rechte, onverminderd de mogelijkheid een klacht in te dienen bij de toezichthouder. Artikel 80 AVG geeft betrokkenen het recht zich te laten vertegenwoordigen door een organisatie zonder winstoogmerk. Dit ziet nadrukkelijk ook op de mogelijkheid om het recht op schadevergoeding op grond van artikel 82 AVG uit te oefenen. Het Nederlandse systeem van artikel 3:305a BW is hier bij uitstek geschikt voor.

34. Wat de onderhavige zaak uniek maakt en onderscheidt van de hierboven genoemde voorbeelden is dat dit, voorzover bekend, de eerste keer is dat onder de AVG door middel van een collectieve actie schadevergoeding wordt gevorderd.

## 2 PARTIJEN

### 2.1 Stichting The Privacy Collective

35. De Stichting is op 29 mei 2020 opgericht om een einde te maken aan de grootschalige, onrechtmatige verwerkingen van persoonsgegevens van internetgebruikers en de daarmee gepaard gaande schending van hun privacyrechten en om genoegdoening voor de achterban te verkrijgen (**Productie 2**).

36. De Stichting heeft een bestuur en een Raad van Toezicht.[34] De leden van het bestuur en de Raad van Toezicht beschikken over de specifieke deskundigheid die noodzakelijk is voor een adequate behartiging van de belangen zoals omschreven in de doelstelling van de Stichting.[35]

37. De Stichting heeft geen winstoogmerk en heeft als statutair doel, kort gezegd, de privacybelangen en persoonsgegevens van internetgebruikers te beschermen:[36]

> *"De Stichting heeft ten doel het behartigen van belangen van natuurlijke personen die gebruikmaken van het internet door te surfen op het internet en/of door gebruik te maken van producten en/of diensten die persoonsgegevens in digitale vorm kunnen opslaan, overdragen of verwerken, waardoor jegens die internetgebruikers op enig moment een schending van hun recht op bescherming van hun privacy of hun recht op bescherming van hun persoonsgegevens plaatsvindt of heeft plaatsgevonden, een en ander in de ruimste zin van het woord."*

[32] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[33] Vgl. HvJEU 29 juli 2019, , C-40/17 (*Fashion ID*), ECLI:EU:C:2018:1039, r.o. 50 en 59.
[34] In hoofdstuk 8 wordt de inrichting en de ontvankelijkheid van de Stichting nader toegelicht. In dat hoofdstuk worden de leden van het bestuur en de Raad van Toezicht en hun deskundigheid uitvoerig besproken.
[35] Zie artikel 3 van de statuten van de Stichting (**Productie 2**) voor een omschrijving van de belangen die door de Stichting worden behartigd.
[36] Zie artikel 3 van de statuten van de Stichting (**Productie 2**).

38. De Stichting streeft dit doel onder meer na door campagne te voeren, (technisch) onderzoek te (laten) doen naar de privacyaspecten bij de grootschalige verzameling en verwerking van persoonsgegevens van internetgebruikers en naar de partijen die daarin een rol spelen, zoals Oracle en Salesforce, en onderzoek te doen naar samenwerkingsverbanden met andere organisaties. Doel van dat alles is de schade vergoed te krijgen van al diegenen op wiens rechten door de onrechtmatige, grootschalige verzameling en verwerking van persoonsgegevens inbreuk is gemaakt.

39. De Stichting treedt op voor Nederlandse internetgebruikers (hierna ook wel "**Gedupeerden**"). Zoals hierna zal blijken, moet aangenomen worden dat alle ca. 10 miljoen Nederlandse internetgebruikers, benadeeld zijn door Oracle en Salesforce. Hierna, onder hoofdstuk 3.3, zal worden toegelicht dat bij bezoek aan bijna alle in Nederland populaire commerciële websites, persoonsgegevens worden verzameld van Nederlandse internetgebruikers met behulp van cookies en andere tracking technologieën van Oracle en Salesforce.

40. De groep personen die wordt vertegenwoordigd door de Stichting valt uiteen in (voor wat betreft dit geschil) twee categorieën, te weten de groep die benadeeld is door Oracle, en de groep die is benadeeld door Salesforce. Gezamenlijk vormen zij een 'nauw omschreven groep' ("**Nauw Omschreven Groep**") als bedoeld in de nieuwe Wet afwikkeling Massaschade ("**WAMCA**").

41. De Stichting staat niet alleen. Zij wordt in Nederland gesteund door toonaangevende (belangen)organisaties op het gebied van het behoud en de bevordering van het recht op privacy, zoals Bits of Freedom[37], Privacy First[38], Freedom Internet[39] en Qiy Foundation[40]. Daarnaast werkt de Stichting samen met personen en organisaties in andere landen, waar mogelijk vergelijkbare stappen (zullen) worden ondernomen. In het licht van haar statutaire doelstelling onderneemt de Stichting ook juridische stappen. Deze procedure is daarvan een voorbeeld.

42. In deze procedure stelt de Stichting een collectieve schadevergoedingsactie in jegens Oracle en Salesforce. De Stichting procedeert daarbij op basis van artikel 3:305a BW. De vorderingen strekken tot bescherming van de belangen van Nederlandse internetgebruikers die door Oracle en Salesforce in hun recht op bescherming van privacy of persoonsgegevens zijn en worden geschaad.

43. Per aangetekende brief van 3 juni 2020 heeft de Stichting zowel Oracle (**Productie 3**) als Salesforce (**Productie 4**) aansprakelijk gesteld voor de door haar achterban geleden schade als gevolg van de inbreuken op het recht op bescherming van privacy en het recht op bescherming van persoonsgegevens. De Stichting heeft Oracle en Salesforce daarbij uitgenodigd om in onderhandeling te treden met de Stichting over het toekennen van een redelijke vergoeding voor de door haar achterban geleden schade.

[37] https://www.bitsoffreedom.nl.
[38] https://www.privacyfirst.nl.
[39] https://www.freedom.nl/.
[40] https://www.qiyfoundation.org/nl/.

44. Oracle en Salesforce hebben de uitnodiging van de Stichting geaccepteerd bij brieven van 18 juni 2020 (**Productie 5**) en 17 juni 2020 (**Productie 6**). Op 3 juli 2020 heeft overleg plaatsgevonden tussen de Stichting enerzijds en Salesforce anderzijds. Op 7 juli 2020 heeft eenzelfde overleg plaatsgevonden tussen de Stichting en Oracle. De gevoerde overleggen met Oracle en Salesforce hebben niet tot het gewenste resultaat geleid. Beide partijen hebben aangegeven geen behoefte te hebben aan vervolgoverleg.

45. De Stichting ziet zich dan ook genoodzaakt om deze collectieve actie procedure aanhangig te maken om namens haar achterban schadevergoeding te vorderen.

## 2.2 Oracle en Salesforce

46. Oracle Corporation, Oracle America, Inc. en Oracle Nederland B.V. (hierna "**Oracle**") maken onderdeel uit van een internationaal opererend technologieconcern op het gebied van onder meer bedrijfssoftware voor datamanagement. In het afgelopen decennium is Oracle zich steeds meer gaan richten op het verzamelen, verrijken en verkopen van persoonsgegevens van internetgebruikers.

47. Salesforce.com, Inc. en SFDC Netherlands B.V. (hierna "**Salesforce**") maken eveneens onderdeel uit van een internationaal opererend technologieconcern maar dan op het gebied van onder meer bedrijfssoftware voor klantrelatiebeheer. Ook Salesforce heeft zich in de afgelopen jaren ontwikkeld tot een van de voornaamste handelaren in persoonsgegevens.

48. De online advertentiemarkt is enorm lucratief. In 2019 was deze goed voor een omzet van meer dan 300 miljard dollar.[41] Aanbieders van DMPs zoals Oracle en Salesforce hebben hier een groot aandeel in. Met de Marketing & Commerce Cloud, diensten die draaien om het personaliseren van advertenties en websites, had Salesforce in 2019 een omzet van bijna 1,9 miljard dollar.[42] In 2017 was dit nog "slechts" 947 miljoen dollar. Het gaat om een markt met een veelheid van partijen. Voor alle betrokkenen is de handel in persoonsgegevens enorm winstgevend.

49. Oracle en Salesforce zijn onmisbaar op deze markt. Beide partijen hebben enorm geïnvesteerd in hun positie op de markt onder meer door een groot aantal partijen over te nemen.

50. Oracle nam de afgelopen jaren de volgende ondernemingen en diensten over:

- Bluekai (circa 400 miljoen dollar), een big data platform, gericht op het personaliseren van reclame op basis van big data, met zoveel mogelijk gekoppelde gegevens en profielen;
- AddThis (circa 200 miljoen dollar), software waarmee websites knoppen kunnen plaatsen om artikelen te delen via sociale media. Door middel van deze "share" knoppen worden ook gegevens verzameld;

[41] Magna, *Magna advertising forecasts – winter 2019 update*, 9 december 2019, te raadplegen via: https://magnaglobal.com/magna-advertising-forecasts-winter-2019-update/.
[42] https://s23.q4cdn.com/574569502/files/doc_financials/2019/Salesforce-FY-2019-Annual-Report.pdf, p. 4 en 44, geraadpleegd op 4 mei 2020.

- Moat (circa 850 miljoen dollar), gespecialiseerd in het analyseren en beïnvloeden van de "aandacht" van de internetgebruiker op basis van meer dan 33 miljard aandachtsanalyses per dag;[43]
- Crosswise (circa 50 miljoen dollar), gespecialiseerd in het in kaart brengen welke apparaten (laptops, smartphones, tablets, televisies) bij dezelfde persoon behoren;
- Eloqua (circa 871 miljoen dollar), gespecialiseerd in het automatiseren van digitale marketing;
- Grapeshot (circa 325 miljoen dollar), gespecialiseerd in contextueel adverteren;
- Datalogix (circa 1,2 miljard dollar), gespecialiseerd in het verzamelen van offline informatie van consumenten ten behoeve van online marketing; en
- Responsys (circa 1,5 miljard dollar), gespecialiseerd in het versturen van gepersonaliseerde e-mails.

51. Oracle's DMP is gebaseerd op wat voorheen Bluekai was. Het draait dus om big data.[44] Oracle combineert haar DMP met andere diensten, zoals AddThis, Datalogix, Eloqua, Responsys en Crosswise. Hiermee heeft Oracle in-house de mogelijkheid om gegevens uit veel verschillende bronnen te verkrijgen, over verschillende apparaten, online en offline en om marketing te personaliseren over een breed scala aan kanalen. Volgens Oracle verkrijgen haar klanten (websitehouders, marketeers en adverteerders) met haar DMP "*more data to drive deeper insights and better personalization*"[45] en een "*truly holistic view of customers*".[46] **Productie 7** bevat een selectie pagina's van Oracle's website waarop zij uitlegt wat haar DMP inhoudt.

52. Ook Salesforce heeft door middel van overnames een positie in de gegevensindustrie veroverd. In 2013 nam Salesforce ExactTarget voor 2,5 miljard dollar over, en in 2016 nam Salesforce Krux over voor 700 miljoen dollar. Krux is een dienst voor optimalisatie van marketing met gebruik van persoonlijke informatie, vergelijkbaar met Bluekai. Krux is inmiddels onderdeel van de Salesforce DMP genaamd "Salesforce Audience Studio and Data Studio", ook wel "Salesforce Marketing Cloud".

53. Over haar DMP meldt Salesforce in 2016 dat Krux iedere maand met drie miljard browsers communiceert, 200 miljard "data collection events" ondersteunt en 5 miljard profielen verwerkt. Salesforce omschrijft haar handelwijze als "orkestreren". Zodoende orkestreert zij 200 miljard "personalized consumer experiences":

> *"Salesforce Marketing Cloud empowers marketers in all industries to leverage meaningful customer and prospect data, build personalized customer journeys at scale and drive business performance. And with Einstein, marketers can predict the best audience, content, channel, and send-time for every customer interaction — and recommend the best offer — all automatically. On a monthly basis, Krux interacts with more than three billion browsers and devices, supports more than*

[43] https://moat.com/.
[44] Een introductiefilmpje van Bluekai (2:24) is te vinden op: https://www.youtube.com/watch?v=UBmgkZdWGLw, geraadpleegd op 29 juli 2020.
[45] https://www.oracle.com/de/data-cloud/products/data-management-platform/, geraadpleegd op 14 juli 2020.
[46] https://www.oracle.com/nl/data-cloud/products/data-management-platform/cross-device.html, geraadpleegd op 14 juli 2020.

*200 billion data collection events, processes more than five billion CRM records, and orchestrates more than 200 billion personalized consumer experiences. Salesforce Marketing Cloud's scalable infrastructure, paired with these new artificial intelligence and cross-device identity management capabilities make it uniquely positioned to empower companies to deliver a consistent brand experience throughout the customer journey."*

54. Salesforce prijst de Audience Studio en Data Studio diensten aan als een manier om "deep insights" in internetgebruikers te verkrijgen "across every touchpoint":

*"**Meet Audience Studio.***

*Formerly Salesforce DMP, Audience Studio can help you gain deep insights by unifying and capturing your data to strengthen customer relationships across every touchpoint with a powerful data management platform."*[47]

*"**Meet Data Studio.***

*Get to know Salesforce's #1 solution for audience discovery, data acquisition, and data provisioning — featuring the world's most-trusted premium data ecosystem."*[48]

55. Salesforce doet in wezen hetzelfde als Oracle en andere DMPs: grootschalige datahandel. **Productie 8** bevat een selectie pagina's van de website van Salesforce waarop zij uitlegt wat haar DMP inhoudt. Ook bij Salesforce staat het koppelen van veel verschillende datasets centraal: koppel een unieke code aan iedere internetgebruiker, bouw een profiel op en maak iedere interactie met een internetgebruiker "persoonlijk".

*"**Create a single, consistent customer ID**.*

*Unify customer data across multiple teams, devices, and systems, such as email, online behavior, ecommerce, and CRM data."*

*"**Build effective customer segmentation**.*

*Easily stitch together first-, second-, and third-party data to create and analyze specialized audience segments."*

*"**Personalize every interaction**.*

*Advertise to the right segments and personas with content tailored across social platforms, online ads, and beyond."*[49]

56. In het navolgende zal de handelwijze van een DMP binnen het *ad-tech* ecosysteem worden besproken, en die van Oracle en Salesforce in het bijzonder.

[47] https://www.salesforce.com/products/marketing-cloud/data-management/, geraadpleegd op 28 april 2020.
[48] https://www.salesforce.com/products/marketing-cloud/data-sharing/, geraadpleegd op 28 april 2020.
[49] https://www.salesforce.com/products/marketing-cloud/customer-data-platform/, geraadpleegd op 6 mei 2020.

## 3 DE HANDELWIJZE VAN ORACLE EN SALESFORCE

### 3.1 Wat is een DMP?

57. Oracle en Salesforce bieden ieder een Data Management Platform ("**DMP**") aan. Een DMP is een dienst gericht op het verzamelen en combineren van persoonsgegevens van internetgebruikers teneinde bezoekers van websites specifieke, op het individu gerichte advertenties voor te schotelen. De DMP dienst wordt gebruikt door websitehouders, adverteerders, marketeers en andere datahandelaren, zoals hierna zal worden toegelicht.

58. Waar in de offline wereld advertenties worden geplaatst op basis van een vermoeden van de interesses en voorkeuren van de gezamenlijke lezers van een krant of tijdschrift, stellen nieuwe technologieën adverteerders in staat om zeer precies de interesses en voorkeuren van specifieke internetgebruikers te bepalen. In 2012 berichtte *The New York Times* al over een boze vader die verhaal kwam halen bij warenhuisketen Target. Hij wilde weten waarom zijn tienerdochter kortingsbonnen voor babykleren toegestuurd kreeg. Daarnaast verweet hij Target zwangerschap aan te moedigen. Wat bleek? Zijn dochter was inderdaad zwanger, zonder dat vader het wist. Target had dat vastgesteld op basis van haar koopgedrag.[50]

59. Sindsdien zijn de mogelijkheden om met precisie te weten wie een website bezoekt geëxplodeerd. Dankzij de ontwikkelingen op het gebied van big data en kunstmatige intelligentie weet een adverteerder vaak meer over een websitebezoeker dan hijzelf. In de hierboven aangehaalde brief van 31 juli 2020 aan de FTC geven de senatoren en congresleden aan hoe onlangs big data werd gebruikt om de deelnemers van een Black Lives Matter protest te analyseren. Hiervoor worden locatiegegevens van de mobiele telefoon gebruikt.[51]

60. Aan de basis van dergelijke gepersonaliseerde advertenties, ligt een verzameling van gegevens over de desbetreffende websitebezoeker. Het betreft onder meer demografische eigenschappen (leeftijd, geslacht, etc.), bezochte websites, gebruikte apps, locatiegegevens, zoekopdrachten, interesses en voorkeuren. Het doel van de gegevensverzameling en verwerking is om internetgebruikers te bewegen een bepaalde handeling te verrichten, bijvoorbeeld de aankoop van een product.

### 3.2 De handelingen die Oracle en Salesforce verrichten

61. Oracle en Salesforce spelen een onmisbare rol bij deze gegevensverzameling en -verwerking. Oracle omschrijft de DMP als de "enabler of the digital marketing ecosystem".

> *"**A DMP Functions as an Enabler of the Digital Marketing Ecosystem***
>
> *Oracle's complete mapping of IDs for consumers, along with mapping to downstream media and app partners, positively influences the addressability and deliverability of marketing campaigns across all digital and mobile, and the overall success rate for marketers to use the data. Thanks to the media integrations the*

[50] New York Times, *How companies learn your secrets*, 16 februari 2012, te raadplegen via: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp
[51] Zie ook https://www.wsj.com/articles/lawmakers-urge-ftc-probe-of-mobile-ad-industrys-tracking-of-consumers-11596214541

*Oracle DMP "just works" on day one. The integrations are already in place so clients can leverage the scale of our networks on day one."*[52]

62. Volgens de *Cambridge Dictionary* is een "enabler" een persoon die het mogelijk maakt dat iets gebeurt of plaatsvindt. In het Nederlands zouden we die persoon een "arrangeur" noemen. Met andere woorden, de DMP is de partij die de zaken in het ecosysteem van online reclame zo schikt dat "behavourial targeting" kan plaatsvinden.

63. Als DMPs verrichten Oracle en Salesforce, onder meer, de volgende handelingen:

1. het plaatsen van cookies uitgerust met een unieke identificator op de randapparatuur van de internetgebruiker;

2. het met behulp van deze cookies en andere unieke identificatoren verzamelen van persoonlijke informatie over de internetgebruiker;

3. het evalueren van persoonlijke aspecten van internetgebruikers met het doel persoonlijke voorkeuren, interesses, gedrag en andere kenmerken van hen te analyseren of te voorspellen ("profilering");

4. het verrijken van deze profielen en persoonsgegevens met informatie uit andere bronnen;

5. het creëren en aanbieden van profielen zodat derden deze kunnen gebruiken om in een veiling te beoordelen of en, zo ja, hoeveel zij willen bieden voor advertentieruimte ("real-time bidding");

6. het koppelen van de unieke identificator van de cookies aan de unieke identificatoren van de cookies van andere adtech partijen om gegevensuitwisseling mogelijk te maken ("cookie syncing").

64. Deze handelingen verrichten zij geautomatiseerd door middel van software. Een DMP biedt haar klanten en/of partners onder meer de volgende middelen aan:

– een softwareplatform dat voortdurend ontwikkeld en onderhouden wordt ten behoeve van het verzamelen, bewaren en verrijken van gegevens;

– een softwaresysteem waarmee websitehouders een koppeling kunnen maken met het platform van Oracle en Salesforce ten behoeve van het plaatsen en uitlezen van cookies;

– het onderhouden en toegankelijk maken van gigantische databases voor gegevensopslag waarin gegevens uit diverse bronnen aan elkaar worden gekoppeld;

– het creëren van koppelingen met databases van derde partijen aan het platform ten behoeve van het verrijken van gegevens;

– het ontwikkelen en onderhouden van algoritmes om één betrokkene te identificeren en zijn activiteiten te volgen over meerdere apparaten;

[52] https://www.oracle.com/nl/data-cloud/products/data-management-platform/ecosystem.html, geraadpleegd op 4 augustus 2020.

- het ontwikkelen en onderhouden van cookies met unieke identificatoren en het creëren van technische koppelingen tussen de eigen cookie identificatoren en die van derde partijen met als doel dat zij elkaars gebruikers kunnen identificeren en gegevens kunnen uitwisselen;

- het ontwikkelen en onderhouden van software waarmee grote hoeveelheden gegevens met "big data" technieken gestructureerd, georganiseerd en inzichtelijk kunnen worden gemaakt;

- het ontwikkelen en onderhouden algoritmes met als doel om van de verschillende gegevenssets profielen en interessesegmenten te maken;

- het aanbieden van een interface / dashboard waarmee de klanten van Oracle en Salesforce specifieke doelgroepen of interessesegmenten kunnen vinden.

65. Door de grote hoeveelheid gegevens die zij over internetgebruikers verzamelen en de (geautomatiseerde) analyses die zij daaraan toevoegen, creëren Oracle en Salesforce een indringend beeld van het online leven van individuele personen. Internetgebruikers krijgen kenmerken toebedeeld en worden ingedeeld is aparte segmenten of "audiences". Oracle en Salesforce koppelen verschillende unieke identificatoren aan elkaar, zodat één vingerafdruk of "ID Graph" ontstaat. Oracle en Salesforce zijn bovendien gespecialiseerd in het verrijken van deze gegevens met gegevens uit andere bronnen. Denk hierbij aan gegevens over offline aankopen, locatiegegevens, credit card gegevens, financiële gegevens en gegevens van sociale media. Oracle en Salesforce bieden hun klanten ook de mogelijkheid om hun eigen gegevens toe te voegen. Zo ontstaat een indringend beeld van iemands gehele leven, zowel online als offline.

66. Dit profiel wordt onder meer gebruikt bij real-time bidding (ook wel "RTB"). Bij RTB wordt de advertentieruimte op bijvoorbeeld een website "real time", dus op het moment dat een persoon een website bezoekt, in een veiling verkocht. Dit proces verloopt volledig geautomatiseerd en DMPs zijn hierbij onmisbaar. Oracle en Salesforce stellen adverteerders in staat om op basis van informatie te bieden op advertentieruimte. Het zijn Oracle en Salesforce die de informatie in dit kader samenbrengen en delen met derden.

67. Steeds wanneer een internetgebruiker een website bezoekt waarop advertenties of andere gepersonaliseerde inhoud kan worden getoond, vindt op de achtergrond een veiling plaats. Door het gebruik van een grote set gegevens die over de internetgebruiker beschikbaar is, kan de adverteerder beoordelen of hij wil bieden op de advertentieruimte en hoeveel. De veiling vindt plaats in de tijd die het kost om de webpagina te laden, een fractie van een seconde.

68. Om de gerichte advertentie op een website te kunnen tonen, worden persoonsgegevens over internetgebruikers verzameld, gecombineerd, verrijkt en gedeeld. Dat verzamelen, combineren, verrijken en delen gebeurt door middel van een DMP.

69. Wanneer de advertentieruimte aangeboden wordt, worden de gegevens over de bezoeker tegelijkertijd gedeeld met honderden potentiële adverteerders, marketeers en de advertentie-exchanges (veilinghuizen) waarvan zij gebruik maken. De identiteit van die partijen is niet bekend bij de andere deelnemers aan het RTB-proces of bij de bezoeker. Het is evenmin

bekend wat die honderden partijen doen met de gegevens nadat zij hebben deelgenomen aan de veiling. De DMP maakt het mogelijk om advertenties te serveren aan de juiste persoon en is daarom cruciaal voor het doel van het RTB-proces: het verkopen van advertentieruimte aan de hoogste bieder op basis van het profiel van de internetgebruiker.

70. Oracle en Salesforce stellen op deze wijze heel specifieke doelgroepen samen voor adverteerders. Dit doet een DMP onder meer door de gegevens over de eigen klanten van de adverteerders te analyseren en op basis daarvan een precies profiel van de gemiddelde klant te creëren. Dat profiel wordt vervolgens vergeleken met de profielen die een DMP heeft van internetgebruikers om juist de personen met datzelfde profiel de advertentie te tonen.

*3.2.1 Het plaatsen van cookies*

71. Oracle en Salesforce verzamelen de gegevens die gebruikt worden om het profiel van een internetgebruiker te creëren met behulp van cookies en vergelijkbare technieken. Cookies kunnen een voor de internetgebruiker nuttige toepassing hebben. Het zijn tekstbestanden die een websitehouder of derde partij op de computer van de gebruiker kan plaatsen om informatie te verzamelen die later gebruikt wordt. Cookies kunnen bijvoorbeeld internetgebruikers herkennen zodat zij niet steeds opnieuw een wachtwoord hoeven in te voeren of zodat de inhoud van het winkelwagentje van een webshop onthouden wordt.

72. Op de advertentiemarkt worden cookies echter niet voor deze doeleinden gebruikt. Op de advertentiemarkt worden cookies met name gebruikt om de ene internetgebruiker van de andere te onderscheiden en om hun gegevens te verzamelen. Dit gebeurt door in de cookie een unieke code ("**Cookie ID**") toe te kennen aan de gebruiker van een apparaat (zoals een computer of smartphone). Door telkens wanneer een persoon een website bezoekt het Cookie ID uit te lezen, wordt de persoon herkend en wordt zijn internetgebruik over verschillende websites en applicaties gedurende een periode bijgehouden en opgeslagen. Ook worden bepaalde handelingen op de website, zoals het aanklikken van een bepaald nieuwsitem of het kopen van een product, met cookies gevolgd en gekoppeld aan hetzelfde Cookie ID. Cookies kunnen worden geplaatst door zowel de websitehouder zelf (bijvoorbeeld als nu.nl een cookie plaatst bij een bezoek aan www.nu.nl, dit wordt een "**first party cookie**" genoemd), of een derde (bijvoorbeeld als oracle.com een cookie plaatst bij een bezoek aan nu.nl, een "**third party cookie**").

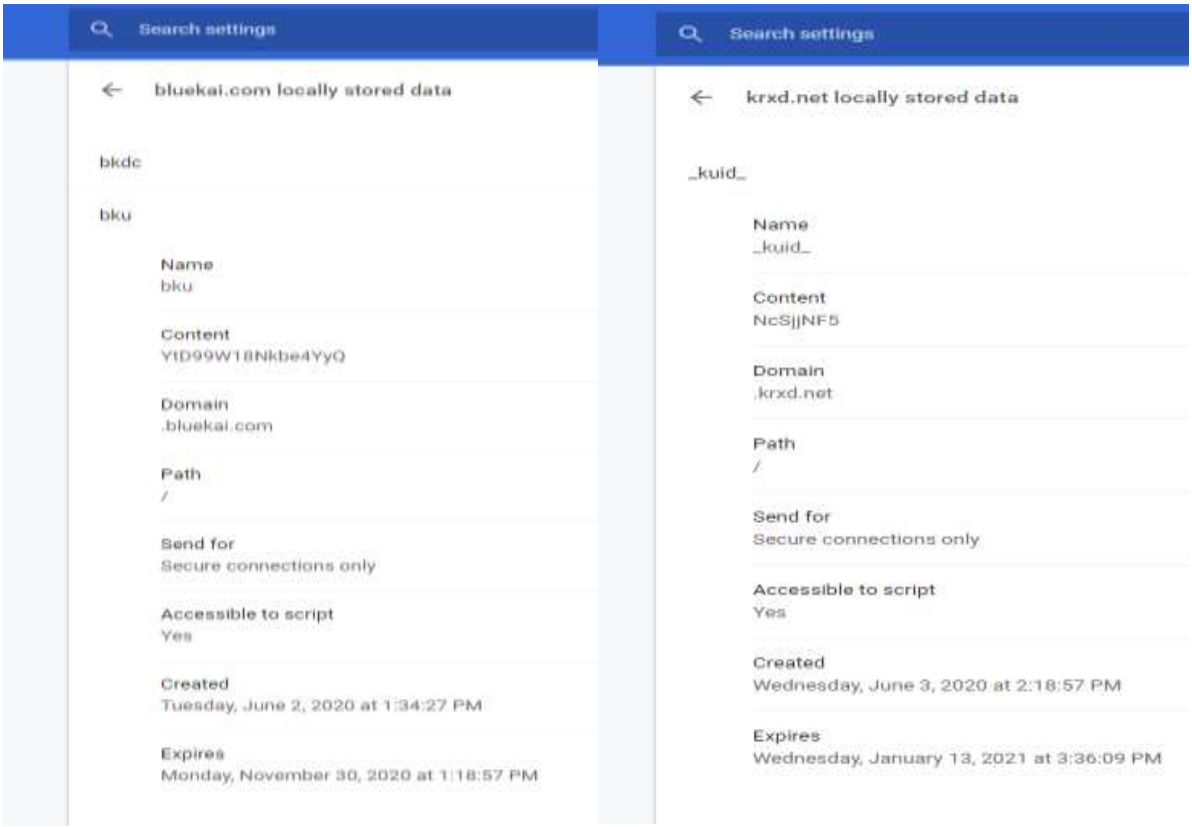
73. Oracle en Salesforce plaatsen cookies via websites van derden. Het gaat om duizenden websites, waardoor het kijk-, luister- en koopgedrag en ook de interacties, zoals het klik- en zoekgedrag van personen, over een lange periode wordt gevolgd.

74. De cookie die Oracle plaatst via de websites van haar klanten heeft de naam "bku", die verwijst naar het bedrijf BlueKai. In **Productie 9** is een voorbeeld te vinden van een bku cookie. De cookie is geplaatst bij een bezoek aan www.voetbalzone.nl. In de cookie is een Cookie ID terug te vinden waarmee Oracle de gebruiker herkent, in dit geval "k9L99B9y3a8aHMQA". Hetzelfde Cookie ID is nogmaals zichtbaar bij een later bezoek aan www.touretappe.nl. Oracle volgt op deze manier de gebruiker over het internet.

75. Ook Salesforce plaatst voor haar DMP "third party" cookies. Deze cookie heeft de naam _kuid_. In **Productie 10** is een voorbeeld te vinden van een _kuid_ cookie. De cookie is

geplaatst bij een bezoek aan www.nu.nl. In de cookie is een Cookie ID terug te vinden waarmee Salesforce de gebruiker herkent, in dit geval "Ne6nmAjL". Hetzelfde Cookie ID is nogmaals zichtbaar bij een later bezoek aan www.buienradar.nl en www.mediamarkt.nl. Ook Salesforce volgt op deze manier de gebruiker over het internet.

76. In de Chrome browser kan een internetgebruiker gemakkelijk zien welke cookies op zijn apparaat aanwezig zijn (door te gaan naar: chrome://settings/siteData). Wanneer een gebruiker op een website komt waarmee door Oracle (BlueKai) of Salesforce (Krux) cookies worden geplaatst, verschijnt bijvoorbeeld de volgende informatie in de Chrome lijst van cookies:




77. De Oracle cookie heeft als naam "*bku*". Het domein dat de cookie uit kan lezen is bluekai.com. De cookie is geplaatst op 2 juni 2020 en zal verlopen op 30 november 2020. Daarmee heeft de cookie een levensduur van 150 dagen. Aan de hand van het Cookie ID "YtD99W18Nkbe4YyQ" kan Oracle de gebruiker steeds herkennen.

78. De Salesforce cookie heeft als naam "*_kuid_*". Het domein dat de cookie kan uitlezen is krxd.net. De cookie is geplaatst op 3 juni 2020, en zal verlopen op 12 januari 2021. Daarmee heeft de cookie een levensduur van ruim 7 maanden. Aan de hand van het Cookie ID, in dit geval "NcSjjNF5" kan Salesforce de gebruiker steeds herkennen.

79. Cookies worden op zeer grote schaal ingezet op de advertentiemarkt. Uit vrij recent onderzoek blijkt dat bij het laden van een gemiddelde voorpagina van een website 55 cookies worden geplaatst. Bezoekt een persoon meer pagina's binnen een zelfde website (bijvoorbeeld door op

een kop van een artikel op een nieuwswebsite te klikken) dan stijgt dit aantal naar 78 cookies.[53] In 2010 bleek uit onderzoek naar de top 50 meest bezochte websites dat de gemiddelde webpagina 64 onafhankelijke tracking technieken, waaronder cookies, gebruikt.[54]

80. **Productie 11** bevat een overzicht van wat er in enkele seconden op de achtergrond gebeurt wanneer de voorpagina van www.nu.nl wordt geladen. In het 35 pagina's tellende overzicht is te zien hoe niet alleen allerlei gegevens worden verzameld, maar ook hoe advertentiepartijen identificatienummers aan de gebruiker toekennen en uitlezen om het gebruik van de website te koppelen aan de gebruiker.

81. Cookies worden geplaatst op bijvoorbeeld de smartphone of computer van een internetgebruiker en kunnen alleen op datzelfde apparaat weer uitgelezen worden. Iedere cookie maakt het mogelijk om de gebruiker steeds weer ter herkennen als die hetzelfde apparaat en dezelfde browser gebruikt. Nadeel in het kader van "behavourial targeting" is dat hierdoor een gefragmenteerd beeld van een internetgebruiker ontstaat. Immers, internetgebruikers maken gebruik van verschillende apparaten en op al deze apparaten worden duizenden cookies en vergelijkbare technieken geplaatst met allen eigen identificatoren.

82. *Ad-tech* bedrijven, onder wie Oracle en Salesforce, hebben hier oplossingen voor gevonden. Oracle en Salesforce geven beiden verschillende apparaten die aan één persoon toebehoren een identificator om "cross-device" te kunnen koppelen.[55] Dit kan bijvoorbeeld met behulp van IP-adressen, locatiegegevens, inloggegevens of patroonherkenning.[56] *Ad-tech* bedrijven wisselen ook informatie die verzameld wordt onderling uit, door het koppelen van cookies: cookie syncing. Op deze manier krijgen *ad-tech* bedrijven een zo compleet mogelijk beeld van een gebruiker. Salesforce legt bijvoorbeeld uit dat het locatiegegevens gebruikt om apparaten te koppelen:

> *"The core of the model is designed to uncover the devices that stay together in various places over long periods of time. To do this effectively there are three important considerations - scale, training, and validation.*
>
> *Scale - Because the success of the model is predicated on seeing lots of devices and how they move over time, it is essential to have massive reach into the device world. With one of the largest device footprints on the planet, Audience Studio has an advantageous position from which to deliver accurate results."*[57]

---

[53] Cookiebot, *How do website track users?,* 10 juli 2020, te raadplegen via: https://www.cookiebot.com/en/website-tracking/ en T. Urban, T. Holz, M. Degeling & N. Poholman, '*Beyond the Front Page:* Measuring Third Party Dynamics in the Field', te raadplegen via: https://arxiv.org/pdf/2001.10248.pdf.
[54] A. Narayanan & D. Reisman, 'The Princeton Web Transparency and Accountability Project', *Springer* 2017, te raadplegen via https://lonlon.io/webtap_book_chapter.pdf, p. 5.
[55] https://www.oracle.com/data-cloud/products/data-management-platform/cross-device.html, Oracle heeft het bedrijf Crosswise opgekocht om zich verder te specialiseren in dit "cross-device" koppelen; https://konsole.zendesk.com/hc/en-us/articles/215234358-Cross-Device-User-Matching, geraadpleegd 11 augustus 2020.
[56] Mozilla, *This is Your Digital Fingerprint,* 26 juli 2018, te raadplegen via: https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/.
[57] https://konsole.zendesk.com/hc/en-us/articles/115009397188-Cross-Device-Identity-Management-CDIM-FAQ-, geraadpleegd 11 augustus 2020.

83. Oracle gebruikt hiervoor onder meer Crosswise, een van haar acquisities (zie randnummer 50). Zoals Oracle bij de acquisitie beschreef:

> *"Crosswise's innovative technology processes over one petabyte of user and device activity data from billions of unique devices every month. By applying advanced data science and proprietary machine-learning techniques to this data, Crosswise constructs a new probabilistic Device Map™ matching multiple devices to individual users in an accurate, scalable and high quality manner."*[58]

84. Oracle en Salesforce gebruiken niet alleen Cookie IDs om gebruikers te volgen. Ook andere IDs worden gebruikt om persoonsgegevens aan een persoon te koppelen. Het kan gaan om IDs gekoppeld aan login gegevens, e-mail IDs, device IDs, mobile advertising IDs,[59] maar ook om IDs die aangeleverd worden door data partners en klanten. Dit is waar DMPs zich in specialiseren. Het koppelen en organiseren en analyseren van gegevens uit allerlei bronnen.

*3.2.2 Het verzamelen van gegevens*

85. Oracle geeft onder meer in een van haar privacydocumenten (zie daarover hierna hoofdstuk 4.3.1.1) aan dat zij de volgende informatie verzamelt:

- *unieke id's zoals de id van uw mobiele apparaat of een cookie-id in uw browser;*
- *een id van een aangesloten apparaat, zoals een id van een smart-tv of streaming-apparaat (wordt alleen gebruikt voor overeenkomende doeleinden in de VS);*
- *IP-adressen en gegevens die kunnen worden afgeleid van IP-adressen, zoals de geografische locatie;*
- *gegevens over uw apparaat, zoals browser, apparaattype, besturingssysteem, de aanwezigheid of het gebruik van "apps", schermresolutie of de voorkeurstaal;*
- *persoonlijke informatie die onidentificeerbaar is gemaakt, zoals e-mailadressen waarop een hash-bewerking is uitgevoerd (directe id's zijn verwijderd);*
- *demografische informatie, zoals geslacht, leeftijd en inkomensschaal, wanneer deze informatie niet is gekoppeld aan informatie waarmee u direct identificeerbaar bent;*
- *gedragsgegevens van een met internet verbonden computer of apparaat dat u gebruikt tijdens interactie met websites, toepassingen of andere verbonden apparaten, zoals advertenties waarop u hebt geklikt of die u*

[58] https://www.oracle.com/corporate/acquisitions/crosswise/, geraadpleegd op 23 april 2020.
[59] Een Mobile Advertising ID is een ID die gekoppeld is aan een mobiel apparaat. Het ID fungeert in wezen als Cookie ID voor mobiele applicaties.

> *hebt bekeken, websites en inhoudsgebieden, datum en tijd van deze activiteiten of de webzoekactie die u hebt gebruikt om een website te zoeken en hiernaar te navigeren.*[60]

86. Het gaat dus om allerhande gegevens die de internetgebruiker kan onderscheiden van anderen, variërend van een IP-adres, demografische gegevens tot het unieke device ID van het apparaat dat door de internetgebruiker wordt gebruikt.

87. Door Salesforce worden vergelijke gegevens verzameld. In een van haar privacy documenten (zie daarover hierna hoofdstuk 4.3.1.2) valt onder meer te lezen dat Salesforce "*pseudonymized personal data related to that user's visits to the website or mobile app (our Customer's "Session Data")*" verzamelt. Session data wordt toegelicht als volgt:

> *"This Session Data may include information about how the user came to the Customer Site and App, which search engines they use, the search terms used to find the Customer Site, their experience on the Customer Site and App, information about how they interact with the Customer Site and App, demographic information that the Customer has collected from that user and other visitors, data from third-party data providers, and information regarding how users interact with advertisements on the Customer Site and App. Additionally, browsers automatically send certain standard information to every website a user visits, such as an IP address, browser type and language settings, access times, and referring website addresses."*[61]

88. Een recent datalek bij Oracle geeft een indruk van de ruwe data die gebruikt wordt om profielen te bouwen (**Productie 12**).[62] TechCrunch geeft aan dat het bedrijfsonderdeel BlueKai van Oracle voortdurend achter de schermen informatie over internetgebruikers verzamelt om profielen op te bouwen en deze profielen voortdurend verrijkt. De ruwe data die met het datalek naar buiten kwam, bevat onder meer gegevens van een Duitse man, inclusief zijn naam, adres, telefoonnummer en e-mailadres, die een debetcard gebruikt om € 10 te besteden aan online gokweddenschappen. Dit is bijzonder gevoelige informatie, omdat het gegevens bevat over mogelijke kansspelverslaving. Het gaat dus om gegevens over gezondheid.

> *"Behind the scenes, BlueKai continuously ingests and matches as much raw personal data as it can against each person's profile, constantly enriching that profile data to make sure it's up to date and relevant.*
>
> *But it was that raw data spilling out of the exposed database.*
>
> *TechCrunch found records containing details of private purchases. One record detailed how a German man, whose name we're withholding, used a prepaid debit card to place a €10 bet on an esports betting site on April 19. The record also contained the man's address, phone number and email address.*

[60] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder 4, geraadpleegd op 23 april 2020 (tevens **Productie 22.a**).
[61] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/ (tevens **Productie 23.d**).
[62] Techcrunch, *Oracle's BlueKai tracks you across the web. The data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).

> *Another record revealed how one of the largest investment holding companies in Turkey used BlueKai to track users on its website. The record detailed how one person, who lives in Istanbul, ordered $899 worth of furniture online from a homeware store. We know because the record contained all of these details, including the buyer's name, email address and the direct web address for the buyer's order, no login needed."*

89. Op deze aspecten van de DMP diensten van Oracle en Salesforce zal hieronder ingegaan worden. Eerst zal echter worden aangegeven hoe Oracle en Salesforce profielen maken van de informatie die zij verzamelen.

*3.2.3 Het creëren van profielen*

90. Aanbieders van DMPs zoals Oracle en Salesforce verzamelen zodoende persoonsgegevens via vele websites, apps en apparaten door middel van cookies en vergelijkbare technieken en verrijken deze informatie met informatie uit andere bronnen. Zij verwerken de verzamelde informatie geautomatiseerd. Daarbij evalueren zij bepaalde persoonlijke aspecten van internetgebruikers. Het voornaamste doel daarvan is het analyseren en voorspellen van persoonlijke voorkeuren, interesses, gedrag en andere kenmerken van internetgebruikers. Dit wordt profilering genoemd.

91. Profielen bevatten informatie, zoals geslacht, woonplaats, leeftijd, aantal apparaten in gebruik, etc., maar ook gevoeligere informatie zoals de informatie over zoekopdrachten, de websites die iemand bezoekt, de artikelen die iemand leest en koopgedrag. Uit die informatie kunnen vervolgens door het combineren en evalueren persoonlijke aspecten, voorkeuren, interesses en andere kenmerken worden afgeleid. Op die wijze ontstaat een gedetailleerd en indringend beeld van iemand.

92. Toezichthouders zijn hierover terecht bezorgd. De ICO uit haar zorgen dat privacyregels worden veronachtzaamd bij de wijze waarop deze data-aggregatie plaatsvindt. De Britse toezichthouder benadrukt dat het gaat om zeer gedetailleerde profielen die met oneindig veel bedrijven worden gedeeld. In haar rapport over dit onderwerp verwoordt zij het als volgt:

> *"We list our concerns - that the creation and sharing of personal data profiles about people, to the scale we've seen, feels disproportionate, intrusive and unfair, particularly when people are often unaware it is happening.*
>
> *We outline that one visit to a website, prompting one auction among advertisers, can result in a person's personal data being seen by hundreds of organisations, in ways that suggest data protection rules have not been sufficiently considered."*[63]
>
> *"The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bidrequest, all without the individuals' knowledge."*[64]

[63] Information Commisioner's Office, *Update report into adtech and real time bidding*, 20 juni 2019 (**Productie 1**), p. 4.
[64] Information Commisioner's Office, *Update report into adtech and real time bidding*, 20 juni 2019 (**Productie 1**), p. 23.

93. Om tot dergelijke profielen te komen, worden de gegevens die Oracle en Salesforce verzamelen zoveel mogelijk aan elkaar gekoppeld via één centraal ID, de ID die alle andere IDs verbindt. Oracle noemt dit haar Oracle ID Graph. Oracle beschrijft haar ID Graph als een fundamentele technologie die de Oracle DMP aandrijft. Alle koppelingen die Oracle maakt worden continu gevalideerd en gescoord. Het gaat hierbij niet alleen om de Cookie ID maar ook om andere identifiers, "massive amounts of IDs" volgens Oracle. Oracle noemt naast Cookie IDs ook "login, HH, email, and mobile ad IDs on a weekly or sometimes daily basis from ID data partners". Met het Oracle ID Graph kan 90% van de mensen online bereiken in de VS en andere markten internationaal:

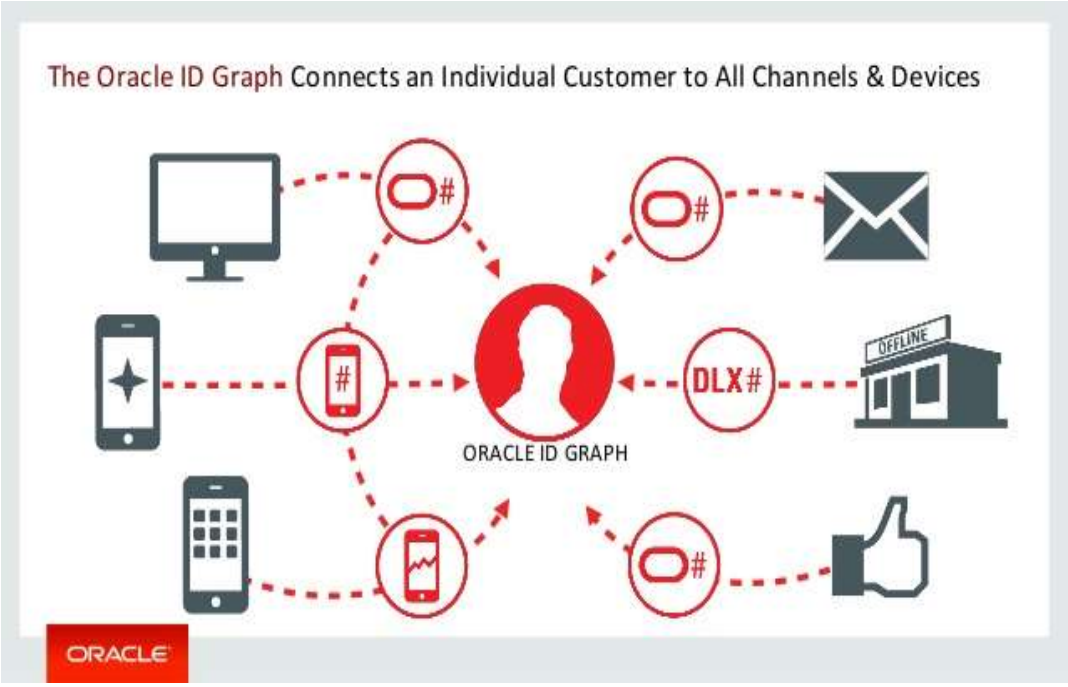
> *"**The Oracle ID Graph, a Foundational Technology That Powers the Oracle DMP**: The Oracle ID Graph establishes and validates connections between IDs that enable the transport of data from one ID space to another, for the purposes of targeting or measurement applications. The Oracle ID Graph is not a product but it is a foundational capability or technology that power the Oracle DMP. All linkages in Oracle ID Graph are continuously validated and scored, which changes dynamically based on a proprietary algorithm to the input. Only the linkages deemed accurate are accepted. Oracle ingests massive amounts of IDs across cookies, login, HH, email, and mobile ad IDs on a weekly or sometimes daily basis from ID data partners. The Oracle ID Graph can reach over 90% of people online in the US and in markets that matter internationally so users can deliver audiences, at scale, and across channels"*

94. Op haar website geeft ze aan dat Oracle de macht van de ID Graph in handen geeft van de marketeers. Dankzij dit unieke profiel hebben marketeers nog meer mogelijkheden om hun doelgroep exact te targeten en te analyseren.

> *"The Oracle Data Management Platform's Audience Builder puts the power of the Oracle ID Graph in the hands of marketers. The Audience Builder allows marketers to visualize linkages and build audiences across devices. With enhanced audience segmentation and delivery, Oracle DMP users now have even more options to define exactly who they want to analyze and target by selecting the device ID from the environment from which the data was collected."*[65]

95. Oracle promoot haar ID Graph met onder meer de volgende afbeelding:

[65] https://www.oracle.com/data-cloud/products/data-management-platform/cross-device.html, geraadpleegd op 23 april 2020.




https://www.slideshare.net/BobLewis15/oracle-marketing-cloud-49482488, geraadpleegd op 24 april 2020.

96. Salesforce heeft een vergelijkbaar ID Graph. Salesforce zelf geeft aan dat deze slechts beschikbaar is voor de Amerikaanse markt.[66] Niettemin koppelt ook Salesforce op grote schaal gegevens. Als hiervoor aangegeven, profileert Salesforce zichzelf onder meer als specialist in het koppelen van verschillende apparaten aan één persoon, op basis van "one of the largest device footprints on the planet" (zie randnummer 82).

97. Oracle en Salesforce verzamelen aldus gegevens over het gedrag van gebruikers van een computer, tablet, smartphone, van e-mail en sociale media en offline data (waaronder winkelaankopen). Oracle koppelt al deze gegevens aan elkaar om een groot gegevensprofiel te maken van de internetgebruiker, onafhankelijk van welk apparaat of welke applicatie hij gebruikt .

98. Daarbij gebruiken adverteerders de DMPs om doelgroepen of "audiences" te creëren. Audiences zijn in wezen lijsten van personen met bepaalde eigenschappen. Dit doen zij op basis van gegevens van de DMP, hun eigen gegevens en gegevens van derde partijen, die zij ook via een DMP kunnen verkrijgen,. Een adverteerder kan bijvoorbeeld op zoek gaan naar personen die waarschijnlijk een bepaald type product kopen, omdat zij lijken op bestaande klanten. Die personen vormen de "doelgroep".

99. Uit documentatie op de websites van Oracle en Salesforce blijkt dat beide partijen als onderdeel van hun DMP doelgroepen creëren.

[66] https://help.salesforce.com/articleView?id=mc_rn_october_2019_dmp_act_seg_ID_graph.htm&type=5, geraadpleegd op 11 augustus 2020

100. Uit documentatie van Oracle blijkt dat klanten gebruik kunnen maken van eigen gegevens ("first party"), gegevens van andere Oracle diensten ("second-party") en gegevens van Oracle's data partners[67] ("third party") om doelgroepen te creëren (**Productie 13**):

> *"Digging a little deeper, note that a segment may contain one or more first-party, second-party, and third-party categories. For example, a segment may include users interested in purchasing one or more products or services, users with a specific geographic location or demographics, or any other data category available in the Oracle BlueKai DMP."*[68]

101. Vervolgens toont Oracle een afbeelding waaruit blijkt dat met enkele klikken "third party data" van onder meer "Oracle's data partners" kan worden gebruikt voor het creëren van doelgroepen. Daarna toont Oracle hoeveel personen binnen de doelgroep vallen, zodat deze personen getarget kunnen worden met advertenties.[69]

102. Uit documentatie van Salesforce ontstaat een vergelijkbaar beeld. Salesforce promoot de "third party" bronnen van haar dienst als volgt (**Productie 14**):

> *"Salesforce Audience Studio has many third-party data options – use the search field or expand the third-party data provider folders to find an appropriate segment."* [70]

103. Als voorbeelden geeft Salesforce een doelgroep van mannen met een inkomen van meer dan 60 duizend dollar of vrouwen die in Boston wonen. Salesforce geeft ook voorbeelden van eigenschappen die gebruikt kunnen worden om doelgroepen te bepalen, zoals leeftijd, opleidingsniveau, etniciteit, gezondheid en fitness, hobby's, huwelijkse staat, vermogen, politiek, religie en spiritualiteit, reizen. Als met de DMP dienst een doelgroep is gecreëerd gaat Salesforce, op basis van de geselecteerde bronnen, op zoek naar personen die in deze doelgroep vallen, zodat de adverteerder deze doelgroep kan targeten. [71]

*3.2.4 Het verrijken van profielen met informatie uit andere bronnen*

104. Oracle en Salesforce verrijken de informatie die zij online hebben verkregen via hun cookies met informatie uit andere bronnen. Zij erkennen ook offline bronnen te raadplegen, bijvoorbeeld loyaltyprogramma's of enquêtes, om de door hen gecreëerde profielen zo volledig mogelijk te maken. Daarnaast werken zij met een enorme hoeveelheid "gegevenspartners" samen om profielen te verrijken.

105. Oracle stelt verder in een van haar privacy documenten (zie daarover hierna paragraaf 4.3.1.1) dat zij zowel uit offline als uit online bronnen informatie verzamelt.

---

[67] Data partners of gegevenspartners zijn de partijen waarvan Oracle en Salesforce gegevens aanbieden in hun respectievelijke data marktplaatsen. Een Advertiser kan bijvoorbeeld via Oracle's DMP gegevens gebruiken van data partner "ShareThis".
[68] Oracle Create Audience Segments, **Productie 13**, tevens beschikbaar via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, geraadpleegd op 22 juli 2020.
[69] Oracle Create Audience Segments, **Productie 13**, tevens beschikbaar via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, geraadpleegd op 22 juli 2020.
[70] Salesforce Segment Builder Guide, **Productie 14**, tevens beschikbaar op https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, geraadpleegd op 22 juli 2020.
[71] Salesforce Segment Builder Guide, **Productie 14**, tevens beschikbaar op https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, geraadpleegd op 22 juli 2020.

*"Oracle verwerkt mogelijk zowel offline als online informatie over u, met inbegrip van informatie die afkomstig is van openbaar beschikbare bronnen of externe gegevensleveranciers.*

- ***Offline informatie** over u verkrijgt Oracle van zijn offline partners zoals fysieke winkels, supermarkten en hun loyaliteitsprogramma's, betaalkaartmerken, catalogusorders en consumentenenquêtes, alsmede derde partijen die mogelijk geen relatie met u hebben en die offline informatie verzamelen van hun offline partners.*

- ***Online informatie** over u komt voort uit uw activiteiten op sites van onze online partners, zoals reclamebureaus en websitebeheerders (bijvoorbeeld online winkels of reiswebsites). Oracle verkrijgt ook online informatie van derde partijen die mogelijk geen relatie met u hebben en die online informatie verzamelen met behulp van cookies of soortgelijke technologieën, zoals pixeltags en apparaat-id's, terwijl u op internet navigeert en interactie voert met websites. Voor meer informatie over cookies en vergelijkbare technologieën die worden gebruikt in verband met Oracle Data Cloud raadpleegt u onderstaande Sectie 11.*

  *Onze online Oracle Marketing & Data Cloud-gegevenspartners staan vermeld in onze catalogus, met een uitgebreide lijst van onze huidige gegevensleveranciers in de EU/EER. Sommige van deze partners verstrekken alleen informatie over personen in specifieke regio's."*

106. Deze offline en online informatie over betrokkenen, kan Oracle zelf verzamelen of opkopen van derden, zelfs als deze geen relatie hebben met de betrokkene.

107. Onder de offline informatie valt onder meer telefoonnummers en online aankoopgedrag:

- *naam en woonadres, e-mailadressen en telefoonnummers;*
- *demografische kenmerken, indien gerelateerd aan andere informatie waarmee u kunt worden geïdentificeerd;*
- *transactiegegevens op basis van uw aankopen, wanneer deze zijn gekoppeld aan andere informatie waarmee u kunt worden geïdentificeerd;*
- *bedrijfsgegevens zoals de naam, grootte en locatie van het bedrijf waar u werkt en uw functie binnen het bedrijf;*
- *gegevens van aanmeldingslijsten voor marketing, consumentenenquêtes of openbare informatie;*
- *alleen voor de Verenigde Staten: breedtegraad en lengtegraad die zijn afgeleid van een fysiek adres.*[72]

[72] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, par. 4, geraadpleegd op 23 april 2020 (tevens **Productie 22.a**).

108. Daarnaast verrijkt Oracle de data met gegevens die zij van derden ontvangt. Deze derden worden veelal "datapartners" of "gegevenspartners" genoemd. De catalogus van gegevenspartners van wie Oracle gegevens verkrijgt, bevat circa 75 bedrijven.[73] Een aantal van de 75 bedrijven is ook zelf datahandelaar die gegevens verkrijgt uit een grote hoeveelheid bronnen. Of deze aantallen juist zijn, is de vraag. In 2017 sprak Oracle nog over meer dan 1500 gegevenspartners (**Productie 15**).

109. Verder biedt Oracle de mogelijkheid van "partner integrations" of "media integrations". Oracle heeft volledig in kaart welke identificatoren bij welke internetgebruikers behoren, zelfs tot aan de media en applicaties waarop advertenties getoond worden.

110. Zoals gezegd, benadrukt Oracle dat de DMP fungeert als "enabler" van het digitale marketing ecosysteem. Door het systeem van media integraties kan met Oracle op dag één gewerkt worden met allerlei media partners. Op haar website noemt zij in het kader van DMP "200 partner integrations":

> *"With the Oracle ID Graph as the foundation, the Oracle DMP can stitch all these different ID sources together to provide better match and scale at bringing data in and delivering data out to the over 200 partner integrations."*[74]

111. De lijst van integraties bevat onder meer exchangers, ad networks, DSPs, (andere) DMPs en ad tech partijen. De lijst bevat "every major media company", aldus Oracle, inclusief Google, Facebook, Twitter, TikTok, YouTube, Twitter alsook andere datahandelaren zoals Lotame, Salesforce, Adobe en AppNexus.[75]

112. Oracle verkrijgt daarnaast gegevens via Oracle en Bluekai cookies en wisselt met cookies verkregen informatie uit met andere datahandelaren via cookie syncing. Oracle geeft onder meer aan:

> *"Oracle en onze advertentietechnologiepartners gebruiken cookies en soortgelijke technologieën (bijvoorbeeld pixeltags en apparaat-id's) om u en/of uw apparaten te herkennen op en buiten verschillende services en apparaten voor de doeleinden die zijn gedefinieerd in bovenstaande Paragraaf 5."*[76]

113. Onder door Oracle verzamelde en ingekochte gegevens vallen onder meer:

a. Cookies die Oracle plaatst op vele duizenden websites van Publishers die klant zijn van Oracle, met name via de "bku" cookie. Publishers kunnen deze gegevens niet alleen koppelen aan de database van Oracle, maar kunnen de data ook verkopen met gebruik van Oracle's DMP.[77] Onderzoek laat zien dat uit een geselecteerde lijst van 100 populaire websites die door Nederlandse internet gebruikers veel bezocht worden, 28 websites Oracle's cookies plaatsen (**Productie 16**, zie hierover tevens paragraaf 3.3). Hieronder

[73] https://www.oracle.com/nl/data-cloud/solutions/data-as-a-service/data-providers.html, geraadpleegd op 21 juli 2020.
[74] https://www.oracle.com/data-cloud/products/data-management-platform/, geraadpleegd op 17 juli 2020.
[75] https://www.oracle.com/data-cloud/solutions/data-as-a-service/media-integrations.html, geraadpleegt op 4 augustus 2020.
[76] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder 11, geraadpleegd op 23 april 2020 (tevens **Productie 22.a**).
[77] https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/index.html#UsingBlueKaiIntegrations/becoming_a_data_provider.html%3FTocPath%3DIntegrator%2520Guide%7C6, geraadpleegd op 26 april 2020: "*The Oracle Data Cloud enables data providers to activate and monetize their data assets in the Oracle Data Marketplace. To become an Oracle Data Cloud data provider, follow these steps.*"

vallen onder meer nieuwswebsites nu.nl, ad.nl, trouw.nl, parool.nl, volkskrant.nl, een aantal lokale nieuwswebsites, sportwebsite voetbalzone.nl, marktplaats.nl en booking.com. Op 10 van deze 28 websites werden cookies geplaatst voordat de internetgebruiker enige interactie met de website had (zoals het klikken op "ik accepteer cookies"). Het onderzoek laat ook zien dat het plaatsend domein van deze cookies "bluekai.com" is (**Productie 16**, zie hierover tevens paragraaf 3.3). Het zijn daarmee "third party" cookies die uitsluitend door Oracle worden uitgelezen. In **Productie 9** is een voorbeeld te vinden van een dergelijke cookie. In de cookie met de naam "bku", die geplaatst is bij een bezoek aan www.voetbalzone.nl, is een Cookie ID terug te vinden waarmee Oracle de gebruiker kan herkennen. Hetzelfde Cookie ID is nogmaals zichtbaar bij een later bezoek aan www.touretappe.nl. Oracle volgt op deze manier de gebruiker over het internet.

b. Gegevens die Oracle verzamelt via sociale media knoppen zoals knoppen waarmee artikelen of andere inhoud op websites gedeeld worden via Facebook of WhatsApp. Oracle's DMP verkrijgt onder meer gegevens via AddThis (een Oracle dienst) en ShareThis (een dienst van een derde). Dit zijn twee van de grootste leveranciers van sociale media knoppen. ShareThis[78] verzamelt gegevens via meer dan 3 miljoen partijen zoals websites en apps wereldwijd, via meer dan 1,8 miljard cookies en over 18 miljard interacties. De gegevens gaan over onder meer reizen, farma, retail en financiën (**Productie 17**).[79] Oracle promoot ShareThis als een van de partijen die ook gegevens uit de EU verkrijgt en licht als volgt toe:

> *"ShareThis is the leading source of online behavioral data across the open web. With a global network of 3M publisher domains, the ShareThis network captures shares, searches, clicks, and pageviews, providing a dynamic and comprehensive picture of consumer interest and intent. Marketers can leverage this proprietary, real-time data to better understand their audiences and connect with them in the moments that matter most."*[80]

Oracle's eigen AddThis knoppen worden op meer dan 15 miljoen websites gebruikt.[81] Daarmee worden gegevens verwerkt van meer dan 900 miljoen websitegebruikers en 1 miljard mobiele gebruikers. Per webpagina waarop AddThis sociale media knoppen staan, verzamelt Oracle tot 30 datapunten.[82] Zowel ShareThis als AddThis diensten bieden de knoppen gratis aan, en vermelden daarbij vrijwel niets over de verzameling van gegevens met gebruik van de knoppen.[83]

[78] https://sharethis.com/, geraadpleegd op 23 april 2020.
[79] Oracle Data Directory 2019 (**Productie 17)**, p. 131-132.
[80] Oracle Data Directory 2019 (**Productie 17)**, p. 131-132.
[81] https://www.addthis.com/, geraadpleegd op 23 april 2020.
[82] Oracle Audience Playbook. raadpleegbaar via: https://fliphtml5.com/atnl/kjmi/basic. Het Oracle Audience Playbook bevat een overzicht van de interessesegmenten die met Oracle AddThis kunnen worden bereikt. Het gaat onder meer om interesse in politieke partijen, homoseksuele films en financiële situatie. Oracle geeft verder aan dat via AddThis gegevens verzameld worden van meer dan 15 miljoen websites wereldwijd.
[83] https://sharethis.com/ en https://www.addthis.com/, geraadpleegd op 26 juni 2020.

c. Gegevens via sociale media. De omvang van deze gegevensverzameling is niet duidelijk, maar Oracle geeft zelf aan dat zij gegevens via sociale media verkrijgt:

> *"Access to more than 700 million social messages daily via feeds from more than 40 million social media and news data sales."*[84]

Oracle verkrijgt ook gegevens van Affinity Answers (een derde partij). In 2019 gaf zij daarover nog aan dat zij van Affinity Answers ook gegevens over personen in de EU verkreeg.[85] Affinity Answers gebruikt data van sociale media om profielen te verrijken en nieuwe klanten te vinden. Het gaat om gegevens van meer dan 400 miljoen sociale media gebruikers. [86]

d. Gegevens die zij verkrijgt door uitwisseling met andere databedrijven via cookie syncing. Uit het hierna te bespreken onderzoek van Dr Ahmad Bashir blijkt dat Oracle via cookie syncing gegevens verkrijgt van onder meer de hierna volgende datapartijen, terwijl deze niet partijen niet worden genoemd in de lijst met "data partners" van Oracle met wie Oracle in de Europese Unie gegevens uitwisselt.

i. "crwdcntrl", dit is het domein van Lotame, eveneens een DMP en grootschalige datahandelaar en "krxd", het domein van Krux, Salesforce;

ii. "id5-sync", het domein van ID5, een partij die gespecialiseerd is in efficiënte en grootschalige cookie syncing. Door middel van ID5 kunnen met één cookie syncing actie talloze onzichtbare partijen hun cookies aan elkaar koppelen.

114. De onderstaande afbeelding toont hoe al deze informatie samenkomt in de Oracle ID Graph. Oracle combineert het gedrag van gebruikers van computer, tablet, smartphone, e-mail, offline data (waaronder winkelaankopen) en sociale media.

https://www.oracle.com/us/assets/general-presentation-2395307.pdf, p. 8, geraadpleegd op 24 april 2020.

[84] Zie de beschrijving van Oracle's Data as a Service dienst in Oracle Cloud – Oracle Data as a Service for Business, raadpleegbaar via: http://www.audentia-gestion.fr/oracle/daas-for-business-2245611.pdf.
[85] Oracle Data Directory 2019 (**Productie 17**), p. 17-18.
[86] Oracle Data Directory 2019 (**Productie 17**), p. 17-18.

115. Salesforce verrijkt haar profielen op vergelijkbare wijze. Ook Salesforce vergaart data uit offline bronnen en werkt samen met "data partners" van wie zij informatie krijgt.

116. Ook Salesforce exploiteert een Third-Party Data Marketplace als onderdeel van de DMP met gegevens van een grote hoeveelheid gegevenspartners:

> *"**Third-Party Platforms***
>
> *The Audience Studio Services integrate with and allow users to interact with third-party advertising technology partners, products, services and platforms, including Non-SFDC Applications, websites, products, services and platforms operated by or on behalf of a customer of the Audience Studio Services, whether through a partner of Salesforce or otherwise (collectively "Third-Party Platforms").*
>
> *● Customers must enable the Audience Studio Services to access customers' Third-Party Platform accounts if needed to perform the services for the integration selected by customer.*
>
> *● The Audience Studio Services may access, collect, process, and/or store information or Content from Third-Party Platform accounts (including information otherwise classified as Customer Data under customer's agreement with Salesforce).*
>
> *● Customers are solely responsible for any content their users or consumers provide to any Third-Party Platform.*
>
> *[…]*
>
> *● Available integrations are listed here."*[87]

117. De knop "here" verwijst naar lijsten van gegevenspartners waar klanten gebruik van kunnen maken. Hier worden onder meer alle grote datahandelaren (Google, DoubleClick, Facebook Custom Audiences, Adobe Analytics en Adobe Audience Manager, Oracle Data Cloud, Rubicon, Amazon Advertising, Criteo, Lotame) genoemd en nog honderden andere partijen.[88] De lijst bevat ook partners die gegevens verzamelen over het offline leven van gebruikers. Denk hierbij aan gegevens over winkelaankopen, credit card gebruik en locatiegegevens. Ook bevat de lijst partners die gegevens van sociale media gebruiken en partners gespecialiseerd in het combineren van gegevens. Dit is vergelijkbaar met Oracle.

118. Op de website van Salesforce is overigens ook een andere lijst gegevenspartners te vinden.[89] Hoe de twee lijsten zich tot elkaar verhouden is onduidelijk.

119. Onder de gegevenspartners van Salesforce vallen onder meer:

[87] https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/audience-studio-notices-and-license-information.pdf, p. 4, geraadpleegd op 24 juli 2020.
[88] https://konsole.zendesk.com/hc/en-us/sections/206625468-Salesforce-DMP-Ecosystem-Partners, geraadpleegd op 29 april 2020.
[89] https://www.salesforce.com/products/commerce-cloud/partner-marketplace/, geraadpleegd op 29 april 2020.

a. De voornaamste andere DMPs Oracle Data Cloud, Adobe Audience Manager, Lotame, Neustar en Nielsen.

Over Lotame geeft Salesforce aan:

*"Lotame Data Exchange (LDX) data comes from an extensive, global, network of publisher partners and offline data partners. The data consists of self-declared and demonstrated behavioral data from unique publishers, yielding accurate and scalable demographic, behavioral interest, and social influencer audience segments.Lotame Data bundles 100% declared and demonstrated - NOT panel-based - data into over 6,000 audience segments across all major verticals (Auto, Travel, Finance, Retail, CPG). Lotame's global reach covers North America, South America, Europe, and Asia."*[90]

b. Een aantal voorname andere datahandelaren waarnaar in de Verenigde Staten onderzoek is gedaan door een senaatscommissie en de mededingingsautoriteit: Acxiom, Experian, Epsilon, Datalogix (thans onderdeel van Oracle) en CoreLogic.

*Van Acxiom wordt expliciet aangegeven dat de dienst ook Nederland dekt en wordt verder vermeld dat Acxiom elke week bijdraagt aan meer dan 3 biljoen transacties.*[91] *Als onderwerpen waarover Acxiom gegevens verstrekt noemt Salesforce onder meer leeftijd, gezinssamenstelling, interesses, politiek, sport, gezondheidsverzekering, financiële situatie, goede doelen, gezondheid en fitnes, etniciteit en sociale media.* [92]

c. Betaalprovider Mastercard Advisors, die gegevens levert van Mastercard over meer dan 160 miljoen transacties per uur:

*"MasterCard Advisors is the professional services, data & analytics arm of MasterCard Worldwide, the global payment processor.*

*Leveraging insights drawn from 160,000,000+ transactions an hour generated by over 2.2 billion MasterCard payment cards. MasterCard Audiences allows advertisers the ability to target more effectively by leveraging aggregated past purchase behavior within specific categories (ie-fine dining, retail, etc.) to identify heavy, frequent and consumers highly likely to spend."*[93]

d. Leverancier van sociale media deelknoppen ShareThis (zie hiervoor randnummer 113.b).[94]

[90] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder Lotame, geraadpleegd op 29 april 2020.
[91] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder Acxiom, geraadpleegd op 29 april 2020.
[92] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder Acxiom, geraadpleegd op 29 april 2020.
[93] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder MaxterCard Advisors, geraadpleegd op 29 april 2020.
[94] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder ShareThis, geraadpleegd op 29 april 2020.

e. Partijen die gebruik maken van "publieke informatie", zoals Mobilewalla (die ook aangeeft gegevens over "politics" te verzamelen:

*"Mobilewalla provides device-ID based segments for targeting mobile in-app audiences on Android and iOS. Mobilewalla has the IP to make sense of billions of data points daily, which allows hundreds of millions of devices to be classified with high confidence. By associating every device ID with installed apps, lat/long and points of interest, the user is classified into hundreds of demographic and behavioral segments. The company's footprint extends throughout North America, Europe and Asia, covering 20 countries."*[95]

f. Partijen die gespecialiseerd zijn in het verzamelen van locatiegegevens zoals Placed, Inc. en Factual.

Over Factual geeft Salesforce onder meer aan:

*"Factual is the neutral data company making high quality location data accessible to everyone. Factual's Global Places data is the leading independent data set covering over 85 million local businesses and points of interest in 50 countries and used by 1000s of developers/companies including Apple Maps, Facebook Places, and Microsoft Bing. Factual maps anonymous location data from mobile devices to these places to generate mobile-first location-based audiences to enhance publishers' advertising products.*

*Factuals Global Places data is built from billions of inputs from millions of sources including user contributions from its network of app clients, relationships with listings management companies and with retail brands, and data from the web. Factual partners with mobile publishers, networks, and ad exchanges to gather anonymous location data from mobile devices, cleans the data using its Location Validation Stack, and then builds location-based audiences tied to mobile IDs."*[96]

Uit documentatie van Factual blijkt dat Nederland een van deze 50 landen is.[97]

120. Ook Salesforce maakt op grote schaal gebruik van cookie syncing technologie om haar cookies en de daaraan gekoppelde gegevens te kunnen koppelen met die van andere partijen, onder meer met Oracle, Google, ad exchanges en andere data handelaren.

121. Dit alles resulteert in een gigantische databerg, verkregen bij honderden partijen, gecombineerd met gegevens via duizenden websites en apps en met gegevens verkregen via synchronisatie met de cookies van andere datehandelaren. De gegevens zien op het gebruik van smartphone, laptop, tablet en televisie en betreffen niet alleen het online maar ook het offline leven van personen. Oracle gaf al tijdens de overname van BlueKai in 2014 aan meer

[95] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder MobileWalla, geraadpleegd op 29 april 2020.
[96] https://konsole.zendesk.com/hc/en-us/articles/217592967-Third-Party-Data-Marketplace, onder Factual, geraadpleegd op 29 april 2020.
[97] Factual, *Knowledge Base; Places; Supported Countries,* te raadplegen via: https://developer.factual.com/docs/places-supported-countries.

dan 30.000 datapunten over individuen te verzamelen in meer dan 700 miljoen profielen.[98] In 2017 sprak zij over meer dan 2 miljard profielen[99] en eerder dit jaar zelfs over 3 miljard profielen, verzameld via 15 miljoen websites.[100] Welke gegevens deze 30.000 datapunten kunnen zijn, is voor de personen over wie de profielen gaan volstrekt onduidelijk.

122. Omdat DMPs grote hoeveelheden gegevens verhandelen via hun data marktplaatsen, en gegevens aggregeren en samenvoegen, worden ze vaak ook aangemerkt als datahandelaar.[101]

*3.2.5 Het gebruik van profielen voor RTB*

123. Zoals hiervoor toegelicht is RTB een systeem waarbij adverteerders bieden op (advertentie)ruimte op een website. Op hoofdlijnen werkt het als volgt:[102]

a. De houder van een website[103] ("**Publisher**") beschikt over vensters waarin hij specifieke boodschappen kan tonen. De inhoud van deze vensters, bijvoorbeeld reclamebanners, kan variëren naar gelang de websitebezoeker. De Publisher kan zo een andere boodschap laten tonen afhankelijk van het profiel van de websitebezoeker. De Publisher biedt deze vensters voor gepersonaliseerde inhoud aan ter verkoop. Publishers maken hiervoor gebruik van de diensten van een derde partij die de advertentieruimte namens hen verkoopt. Deze derde partij wordt een Supply Side Platform of SSP genoemd. Daarnaast maken Publishers gebruik van de diensten van een DMP om gegevens over hun bezoekers te verzamelen en daardoor meer inkomsten uit de advertentieruimte te genereren.

b. Een adverteerder ("**Advertiser**"), zoals de verkoper van een product of dienst, wil de meest interessante plek op een website benutten door er klikbare advertenties of andere content te tonen. De Advertiser beoogt daarom de ruimte, bijvoorbeeld een reclamebalk, te kopen die de grootste kans heeft op een aankoop. Advertisers maken hiervoor gebruik van de diensten van een derde partij die de advertentieruimte namens hen inkoopt. Deze derde partij wordt een Demand Side Platform of DSP genoemd. Daarnaast maken Advertisers gebruik van een DMP om op basis van gegevens over websitebezoekers te beoordelen wie het meest geneigd is zijn product te kopen, zodat aan die personen de advertentie wordt getoond.

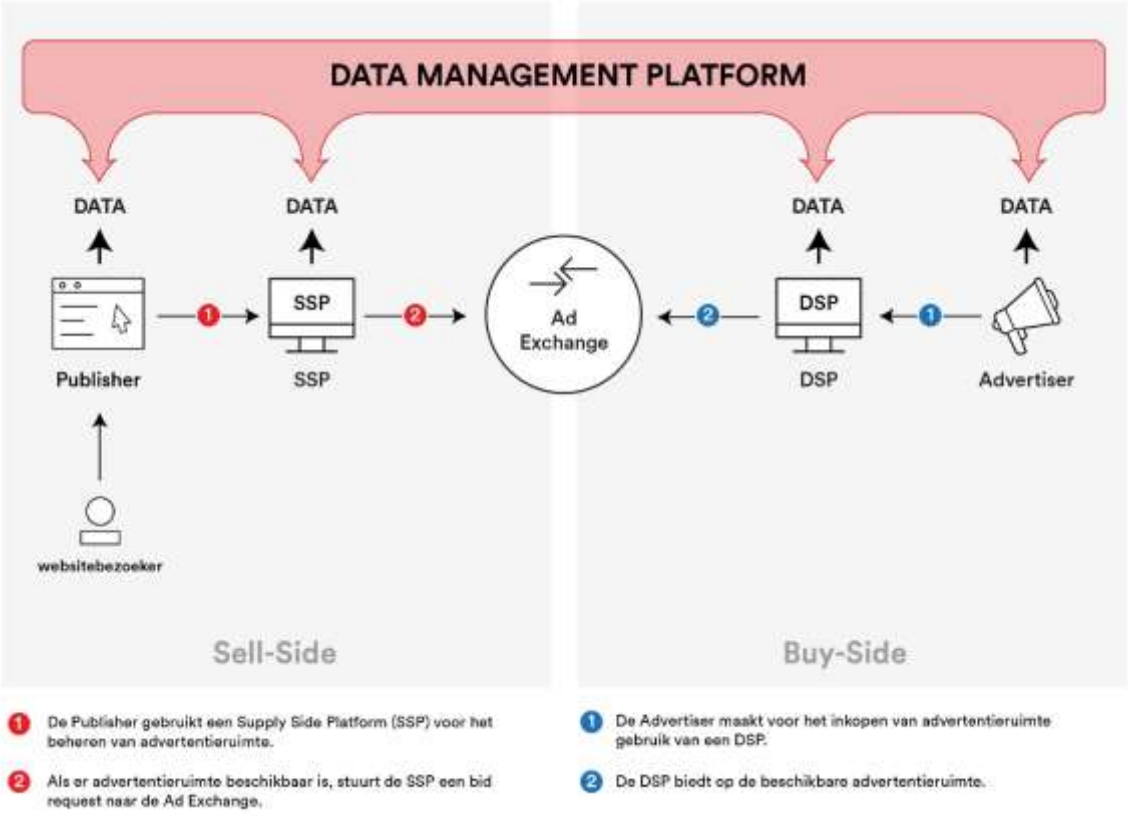
c. Wanneer iemand een website bezoekt waarop ruimte beschikbaar is, stuurt de Publisher een verzoek inclusief gegevens van de bezoeker ("bid request") naar één of meerdere veilinghuizen ("ad exchanges"). De ad exchanges sturen de zogenoemde bid requests naar alle potentieel geïnteresseerde Advertisers. Daarna wordt de beschikbare ruimte geveild. Aan één veiling voor een reclamebalk kunnen tientallen of zelfs honderden

[98] https://www.oracle.com/us/assets/general-presentation-2150582.pdf, geraadpleegd op 23 april 2020.
[99] **Productie 15**, nieuwsbericht Oracle Marketing Cloud Teams with Eyeota to Enhance Global Data Offering.
[100] https://www.oracle.com/corporate/acquisitions/crosswise/, geraadpleegd op 6 mei 2020.
[101] Zie onder het rapport van de Noorse consumentenbond "Out of Contro", beschikbaar op https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf, p. 37. Zie ook de klacht van Privacy International, beschikbaar op https://privacyinternational.org/sites/default/files/2018-11/08.11.18%20Final%20Complaint%20Acxiom%20%26%20Oracle.pdf.
[102] Zie tevens een video van een presentatie die privacy activist Johnny Ryan in februari 2019 hield bij de European Data Protection Supervisor over de werking van het RTB systeem, te raadplegen via: https://vimeo.com/317245633./.
[103] RTB wordt ook gebruikt voor het tonen van gepersonaliseerde inhoud in apps of e-mails.

Advertisers meedoen. De hoogste bieder krijgt de ruimte en betaalt de Publisher. De Publisher plaatst de advertentie.

124. Het doel van dit alles is de websitebezoeker te bewegen op de advertentie te klikken. De ratio van dit klikgedrag wordt “click-through rate” of “CTR” genoemd. Een hogere CTR is voor alle partijen gunstig. Voor de Publisher omdat die een hogere prijs zal ontvangen voor advertentieruimte en voor de Advertiser omdat meer personen het product kopen.

125. Schematisch kan dit als volgt worden weergegeven:




126. Om de websitebezoeker te bewegen op een advertentie te klikken, wordt de inhoud toegespitst op de persoon die de inhoud te zien krijgt. Hiervoor gebruiken de verschillende partijen uiteenlopende gegevens van die persoon.

127. De Britse privacytoezichthouder ICO geeft in een rapport een overzicht van de gegevens die met bid requests meegestuurd worden:

*“The information in a bid request can vary but most include the following:*

- *a unique identifier for the bid request;*
- *the user's IP address (possibly with the final set of numbers removed, eg in Google’s Authorized Buyers framework);*
- *Cookie IDs;*
- *user IDs;*

- *a user-agent string identifying the user's browser and device type;*
- *the user's location;*
- *the user's time zone;*
- *the detected language of the user's system;*
- *the device type (desktop/mobile, brand, model, operating system);*
- *other information relating to the user (this can vary); and*
- *information relating to the audience segmentation of the user.*

*The above information is personal data where it enables a natural person to be identified, directly or indirectly, from the information itself (alone or in combination) as well as additional information that controllers may possess.*

*Other information about the user can include:*

- *referring sites (where the user came from);*
- *user journey on the site (including mouse cursor movement);*
- *events (scrolling, clicking, highlights, media views);*
- *location;*
- *search queries;*
- *session time;*
- *site behaviour (contextual and thematic preferences to certain topics and pages, interactions such as downloads, transitions to other pages through clicking on advertisements and links); and*
- *demographic data."*[104]

128. Alle potentiële bieders ontvangen dus dergelijke gegevens met betrekking tot de websitebezoeker. Zij kunnen deze combineren met andere (eerder verzamelde, ingekochte of op andere manier verkregen) gegevens om op basis van een uitgebreid profiel te bieden op (advertentie)ruimte. Verder kunnen deze bieders met de gegevens doen wat zij willen. De Publisher, ad exchange of enige andere betrokken partij heeft geen controle meer over wat er met de gegevens gebeurt nadat deze aan Advertisers zijn verstrekt.

129. Om een beeld te geven van de omvang van de RTB-markt: Index Exchange, een ad exchange (veilinghuis die advertentieruimte verhandelt), behandelt circa 50 miljard bid requests per dag.[105] Dat betekent dat 50 miljard keer per dag ruimte op een website, in een applicatie of in een bericht wordt aangeboden, dat dit aanbod inclusief gegevens van de websitebezoeker (het "bid request") wordt verstuurd naar het veilinghuis Index Exchange en wordt verspreid onder tientallen of honderden potentiële bieders die de ruimte kunnen gebruiken om een advertentie of andere content aan een websitebezoeker te tonen. Index Exchange ontvangt dagelijks maar liefst 600 miljard biedingen als reactie op de bid requests. Index Exchange is de kleinste van de acht grote ad exchanges.[106]

[104] Information Commisioner's Office, *Update report into adtech and real time bidding*, 20 juni 2019 (**Productie 1**).
[105] Index Exchange, *Tour IX's Amsterdam & Frankfurt Data Centers,* 2 juli 2019, te raadplegen via: https://www.indexexchange.com/tour-ix-amsterdam-frankfurt-data-centers/.
[106] Brave, *Scale billions of bid requests per day,* 2019, te raadplegen via: https://brave.com/wp-content/uploads/2019/07/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf.

*3.2.6 Cookie syncing: het koppelen van cookies om internetgebruikers nog beter te volgen*

130. Met behulp van cookie syncing of cookie matching kunnen *ad-tech* bedrijven onderling Cookie IDs kunnen uitwisselen. De uitwisseling van unieke identificatoren is cruciaal voor RTB. Zonder cookie syncing is RTB niet mogelijk. Een internetgebruiker krijgt op een gemiddelde website al 78 cookies op zijn randapparatuur geplaatst, allemaal uitgerust met en unieke Cookie ID.[107] Cookie syncing zorgt ervoor dat verschillende partijen in de ad-tech industrie die cookies plaatsen die IDs onderling met elkaar kunnen vergeleken. Het doel hiervan is onderling informatie uit te wisselen, zodat voor iedereen duidelijk is wie internetgebruiker "abc" of "xyz" is.

131. Wanneer Oracle en Salesforce bijvoorbeeld met elkaar cookies syncen, dan leggen ze vast dat een bepaalde internetgebruiker voor Oracle de persoon is met Cookie ID "abc" en voor Salesforce de persoon met Cookie ID "xyz". Als Oracle dan gegevens over persoon "abc" verstrekt, weet Salesforce dat het om "xyz" gaat. Dit proces maakt het voor adtech bedrijven mogelijk om gemakkelijk te kunnen communiceren over een persoon en gegevens over die persoon uit te wisselen. Op deze manier worden op grote schaal Cookie IDs uitgewisseld tussen de websitehouder, adverteerders, data management platforms en andere betrokken partijen, zodat al deze partijen steeds eenvoudig kunnen communiceren over dezelfde persoon.[108] Op die manier kunnen ook profielen aan elkaar gekoppeld worden.

132. Een groot deel van het overzicht van het laden van de voorpagina van www.nu.nl (**Productie 11**) bestaat uit cookie syncing. Op pagina's 5 en 10 staan bijvoorbeeld de volgende door het domein "acdn.adnxs.com" verzonden links:

> *https://stags.bluekai.com/site/3085?id=4671557832191386248*
>
> *https://beacon.krxd.net/usermatch.gif?adnxs_uid=4671557832191386248*[109]

133. De code "4671557832191386248" is de code die de plaatser (in dit geval AppNexus, ook een grote speler in de adtech markt) aan verschillende bedrijven meegeeft zodat zij hun eigen cookies, kunnen koppelen aan de cookies van AppNexus. Zodra de cookies gekoppeld zijn, kan alle achterliggende informatie van de personen worden uitgewisseld. Voornoemde links zijn gericht aan bluekai.com en krxd.net. bluekai.com is een domein van Oracle. Krxd is een domein van Salesforce. Met deze links worden dus de cookies die AppNexus enerzijds en Oracle en Salesforce anderzijds gekoppeld. Met deze koppeling wordt het mogelijk om alle achterliggende informatie te koppelen.[110]

---

[107] Cookiebot, *How do website track users?,* 10 juli 2020, te raadplegen via: https://www.cookiebot.com/en/website-tracking/ en T. Urban, T. Holz, M. Degeling & N. Poholman, '*Beyond the Front Page:* Measuring Third Party Dynamics in the Field', te raadplegen via: https://arxiv.org/pdf/2001.10248.pdf.
[108] Een technische uitleg is te vinden op Clearcode, *What is Cookie Syncing and How Does it Work?,* 15 december 2015, te raadplegen via: https://clearcode.cc/blog/cookie-syncing/.
[109] Deze links zijn verzonden door het bedrijf AppNexus, eveneens een grote speler in de adtech markt. De links zijn te vinden op pag. 5 en 10 van het overzicht van het laden van de voorpagina van www.nu.nl (**Productie 11**).
[110] In veel gevallen zijn de datapartners niet bij naam genoemd, maar bij nummer. Zie bijv. p. 4 van het overzicht van het laden van de voorpagina van www.nu.nl (**Productie 11**):
https://image4.pubmatic.com/AdServer/SPug?**partnerID=27**&partnerUID=42a75ea7-e1e4-4300-ac31-a6b76c529cb3

## 3.3 Onderzoek naar de handelingen van Oracle en Salesforce

### *3.3.1 Onderzoek Dr. Bashir*

134. De Stichting heeft onderzoek laten doen naar de activiteiten van Oracle en Salesforce door Dr. Muhammad Ahmad Bashir (**Productie 16**). Dr. Bashir is gepromoveerd op de privacy implicaties van het RTB systeem en is op dit moment werkzaam bij de gerenommeerde universiteit van Berkeley, gespecialiseerd in technisch onderzoek naar privacy aspecten bij het gebruik van onder meer cookies.[111] Met gebruik van een virtuele computer met een Nederlands IP adres heeft hij geautomatiseerd websites bezocht en gemonitord welke verbindingen deze websites maken en welke cookies deze websites plaatsen. Hij heeft hiervoor gebruik gemaakt van een selectie van 100 veelgebruikte Nederlandse websites en van elk van deze websites 6 willekeurige pagina's bezocht. Met het onderzoek heeft Dr. Bashir in kaart gebracht welke veelgebruikte Nederlandse websites gebruik maken van de trackingtechnologieën van Oracle en Salesforce.

135. Dr. Bashir heeft in kaart gebracht via welke van de 100 websites de cookies van Oracle en Salesforce worden geplaatst. Voor Oracle gaat het om de cookie met de naam "bku" die geplaatst worden door het domein bluekai.com. Bij Salesforce gaat het om de cookies met de naam "_kuid_" die geplaatst worden door krxd.net. Hij heeft verder in kaart gebracht met welke partijen cookies gesynchroniseerd worden met gebruik van cookie syncing technologieën, via deze websites.

136. Uit het onderzoek blijkt dat Oracle en/of Salesforce cookies plaatsen via 41 van de 100 websites. Oracle plaatst cookies op 28 websites,[112] Salesforce plaatst cookies via 31 websites; via 18 websites worden beide cookies geplaatst. Het gaat onder meer om de volgende websites, waarbij is aangegeven van welke van deze twee partijen cookies geplaatst worden. Ook is aangegeven hoeveel *unieke bezoekers* de website trok in de maand juni 2020.[113]

- Bol.com – Salesforce – 9,97 miljoen
- Buienradar.nl – Salesforce – 8,36 miljoen
- Marktplaats.nl – Oracle en Salesforce – 7,88 miljoen
- Booking.com – Oracle en Salesforce – 2,49 miljoen
- Startpagina.nl – Oracle en Salesforce – 3,12 miljoen
- Mediamarkt.nl – Salesforce – 2,93 miljoen
- Libelle.nl – Oracle en Salesforce – 2,37 miljoen
- Nieuwswebsites:
  - Nu.nl – Oracle en Salesforce – 7,22 miljoen
  - Ad.nl – Oracle en Salesforce – 7,39 miljoen
  - Rtlnieuws.nl – Salesforce – 5,53 miljoen
  - Trouw.nl – Oracle en Salesforce – 2,66 miljoen
  - Volkskrant.nl – Oracle en Salesforce – 3,85 miljoen
  - Parool.nl – Oracle – 2,62 miljoen

[111] Zie onder meer https://cltc.berkeley.edu/about-us/researchers/ahmad-bashir/ en https://www.ahmadbashir.com/
[112] Hier zijn zowel de websites opgenomen die voordat toestemming is gegeven cookies plaatsen als nadat toestemming is gegeven cookies plaatsen, zie annexen 6 en 7 van **Productie 16**.
[113] Gebaseerd op de statistieken van NOBO, beschikbaar op http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.

- Indebuurt.nl – Salesforce – 2,45 miljoen
- gelderlander.nl – Oracle en Salesforce – 2,06 miljoen

137. Dr. Bashir heeft eveneens onderzocht op hoeveel websites cookies al geplaatst worden voordat er toestemming is gegeven. Bij Oracle zijn dat 10 websites, bij Salesforce 12.

138. In het onderzoek zijn verder de partijen geïdentificeerd waarmee Oracle en Salesforce koppelingen maken door middel van cookie syncing (toegelicht in paragraaf 3.2.6). Uit het onderzoek blijkt dat Oracle op de 28 websites waarop Oracle cookies zijn aangetroffen, gebruik maakt van cookie syncing met 12 andere partijen. Vermoedelijk gaat het echter om veel meer partijen omdat een van de partijen waarmee Oracle cookies synchroniseert het bedrijf ID5 (id5-sync) is. ID5 is gespecialiseerd in efficiënte en grootschalige cookie syncing. Via ID5 kan Oracle met talloze bedrijven cookies synchoniseren met slechts één cookie syncing actie. Het is voor de gebruiker, en zelfs voor Dr. Bashir, onmogelijk om te zien om welke partijen het gaat. Oracle synchroniseert cookies verder met onder andere:

a. “rubiconproject”, het domein van Rubicon Project, een van de grootste ad exchanges die naar eigen zeggen advertenties verwerkt voor meer dan een miljoen websites en 60 duizend mobiele applicaties;[114]

b. “crwdcntrl”, dit is het domein van Lotame, eveneens een DMP en grootschalige datahandelaar;

c. “krxd”, het domein van Krux, Salesforce;

d. “spotxchange”; het domein van SpotX, en “tidaltv”, domein van TidalTV, beide gespecialiseerd in advertenties in videos.

139. Met 5 partijen worden al cookies gesynchroniseerd voordat de internetgebruiker toestemming heeft gegeven. Het gaat onder meer om ID5, Salesforce en Lotame.

140. Salesforce synchroniseert met 23 andere partijen cookies op de 31 populaire websites waarop Salesforce cookies zijn aangetroffen. Het gaat om onder meer:

a. “adnxs”, dit is het domein van AppNexus, een datahandelaar gespecialiseerd in het laten uitwisselen van gegevens;

b. “bluekai”, het domein van Oracle;

c. “doubleclick”, een domein van Google, de grootste partij in de advertentiemarkt;

d. “everesttech” en “demdex”, beide domeinen van Adobe die eveneens een DMP service aanbiedt en daarbij fungeert als datahandelaar;

e. “openx”, “pubmatic”, domeinen van gelijknamige partijen die gespecialiseerd zijn in gepersonaliseerde advertenties;

f. “rubiconproject” en “casalemedia”, beide ad exchanges;

[114] https://rubiconproject.com/.

g. “spotxchange”, “tidaltv”, en “fwmrm”, allen gespecialiseerd in advertenties in video’s (**Productie 16**).

Met 15 van deze 23 partijen worden cookies gesynchroniseerd voordat de gebruiker daar überhaupt enige vorm van toestemming voor heeft gegeven. Het gaat onder meer om Oracle, AppNexus en Google.

141. Het onderzoek van Dr. Bashir toont aan dat de technologieën van Oracle en Salesforce gebruikt worden op veel “household names” websites die vrijwel elke Nederlander bezoekt. Vrijwel elke Nederlander zal dan ook in aanraking gekomen zijn gekomen met de DMPs van Oracle en Salesforce. Het onderzoek toont verder aan dat niet alleen cookies geplaatst worden via deze websites, maar dat Oracle en Salesforce deze cookies tegelijkertijd koppelen met tientallen andere partijen, waaronder ad exchanges, andere DMPs en datahandelaren.

142. **Productie 18** laat een overzicht zien van de websites die, blijkens het onderzoek van dr. Bashir (**Productie 16**), gebruik maken van de cookies van Oracle en/of Salesforce. Het overzicht laat zien dat een groot deel van de websites niet op juiste wijze toestemming vraagt en/of informatie verstrekt over de verwerking van persoonsgegevens door Oracle en Salesforce (zie daarover paragraaf 4.6.2 en 4.6.3).

143. Uit kolom C van het overzicht blijkt het bereik van deze websites in de maand juni 2020 in Nederland, voor zover bekend. Hiervoor is gebruik gemaakt van het Nederlands Online Bereik Onderzoek (“NOBO”)[115] en SimilarWeb. Het aantal unieke bezoekers in deze maand varieert van ruim 2 miljoen bezoekers aan degelderlander.nl tot bijna 10 miljoen aan bol.com.[116] Ook websites als buienradar.nl (ruim 8 miljoen), nu.nl (ruim 7 miljoen), marktplaats.nl (bijna 7 miljoen) en rtlnieuws.nl (ruim 5 miljoen) hebben veel unieke bezoekers.

144. Dr. Bashir heeft slechts onderzocht of op bepaalde websites Oracle en Salesforce cookies zijn aangetroffen. De verwerking van partijen zijn daartoe echter niet beperkt tot deze websites. Nog vele andere websites geven in hun cookiebeleid aan dat Oracle en Salesforce partners zijn die gebruik kunnen maken van de cookies die via hun websites worden geplaatst of dat zij op andere wijze gebruik maken van de diensten van Oracle en Salesforce. Beide DMPs staan bijvoorbeeld genoemd in de lijst van circa 550 data partners van telegraaf.nl.[117] Funda.nl noemt eveneens zowel Oracle als Salesforce in een lijst van circa 600 ad tech partners. De websites hadden respectievelijk 5.862.000 en 4.797.000 unieke bezoekers in de maand juni 2020.[118] De omvang van de relevante gegevensverzameling door Oracle en Salesforce is daarom nog vele male groter dan het gebruik van hun cookies doet vermoeden. Al met al kan geconcludeerd worden dat Oracle en Salesforce van vrijwel iedere Nederlandse internetgebruiker gegevens verzamelen en verwerken.

145. Oracle en Salesforce richten hun diensten ook specifiek op de Nederlandse markt. Voor Oracle geldt dat onderdelen van de website van Oracle die zien op de promotie van de DMP dienst in het Nederlands beschikbaar zijn. Op die pagina zijn de Nederlandse contactgegevens van

[115] Het NOBO is een onderzoek dat uitgevoerd wordt door de Verenigde Internet Exploitanten en Stichting KijkOnderzoek. Het NOBO brengt maandelijks het aantal *unieke bezoekers* in kaart van de top 50 meest bezochte mediaplatforms. 16 van de 41 websites waren beschikbaar in de NOBO statistieken.
[116] http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.
[117] Te zien door in de cookiebanner van https://www.telegraaf.nl/ te klikken op “derden”.
[118] http://vinex.nl/wp-content/uploads/2020/07/NOBO-Top-50-juni-2020.xlsx.

Oracle te vinden. Ook is de lijst van media integraties van Oracle te vinden op een Nederlandse pagina (**Productie 19**).

146. Voor Salesforce geldt dit eveneens. Hoewel het Audience Studio and Data Studio Privacy Policy geen Nederlandse versie heeft, zijn alle promotionele webpagina's voor de verkoop van de DMP dienst wel in het Nederlands te vinden. Salesforce verstrekt ook Nederlandse contactgegevens en promoot de dienst door te verwijzen naar voorbeelden van Nederlandse klanten. In 2018 geven grote mediabedrijven de Persgroep, Sanoma en Telegraaf Media Groep aan met gebruik van de Salesforce DMP te gaan samenwerken op het gebied van "programmatic advertising" (**Productie 20**). Daarnaast zijn er verschillende wederverkopers die de Salesforce DMP aanbieden in Nederland actief.[119]

*3.3.2 Inzage in segmenten van Oracle*

147. Oracle biedt internetgebruikers de mogelijkheid om een deel van de persoonsgegevens die over hen zijn verwerkt in te zien via datacloudoptout.oracle.com. **Productie 21** laat een dergelijk overzicht zien van een Nederlandse internetgebruiker. Het overzicht bevat 11 pagina's aan interessesegmenten en andere informatie. Onder meer is te zien hoe koppelingen gemaakt zijn met Google en andere *ad-tech* bedrijven zoals DataXu, AppNexus, Beeswax en Mediamath. Genoemde interessesegmenten zijn onder meer "job search", "fitness", "fitbit", "Men's health magazine", huidverzorgingsproduct "Neutrogena", betaalproviders en interesse in computerspellen, films, elektronica en auto's. Verder lijkt Oracle met "Oracle Modelling 360" inschattingen te maken van de emotionele staat van de persoon. Er staat bijvoorbeeld "shocked_EU > 20-30%".

148. In de brief van 18 juni 2020 geeft Oracle aan dat zij slechts gebruikt maakt van vier "data providers", die bovendien moeten voldoen aan stringente voorbeelden. Uit het overzicht dat Oracle zelf verstrekt blijkt echter dat Oracle met veel meer "data providers" samenwerkt. Het overzicht laat verder een grote hoeveelheid "branded data" zien van ad tech partner Affinity Answers. Affinity Answers analyseert sociaal media gebruik. Het bedrijf werd in 2019 nog aangemerkt als een partner die ook data verschaft van Europese internetgebruikers.[120] Inmiddels geeft Oracle echter aan geen EU data meer te verzamelen met gebruik van Affinity Answers.[121] Uit het overzicht blijkt echter dat Oracle nog steeds persoonsgegevens verwerkt van Affinity Answers van Europese internetgebruikers.

## 3.4 Datalekken bij Oracle en Salesforce

149. Zoals hiervoor toegelicht verzamelen, verwerken en delen Oracle en Salesforce in het kader van hun DMPs grote hoeveelheden gegevens over grote hoeveelheden personen. De risico's van het op grote schaal verzamelen, verwerken en delen, worden pijnlijk zichtbaar door verschillende beveiligingsproblemen en datalekken waar Oracle en Salesforce mee te maken hebben gehad. Bij beide partijen hebben verschillende datalekken plaatsgevonden waarbij grote hoeveelheden gegevens zijn gelekt. Hieronder volgen enkele voorbeelden:

[119] Zie bijvoorbeeld: https://emark.com/nl/landing/salesforce-dmp/.
[120] Zie http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf, p. 17
[121] Zie https://www.oracle.com/data-cloud/solutions/data-as-a-service/data-providers.html.

a. Op 19 juni 2020 publiceerde technologie website TechCrunch een artikel over een datalek in verband met de DMP dienst van Oracle (**Productie 12**).[122] Een onderzoeker had toegang verkregen tot een server en gegevens gedeeld met TechCrunch. De onderzoeker en TechCrunch hebben op deze wijze toegang verkregen tot miljarden gegevens van een enorme groep betrokkenen. Het betrof onder meer namen, adressen, emailadressen, maar bijvoorbeeld ook gegevens over deelname aan online kansspelen voor e-sports en betaalgegevens.

   De onderzoeker en TechCrunch konden toegang verkrijgen tot de gegevens omdat de server waarop de gegevens waren opgeslagen niet adequaat beveiligd was en er onder meer geen login met een wachtwoord was vereist.

   Uit de publicatie blijkt verder dat Oracle de onrechtmatige toegang wijt aan onjuiste instellingen van een tweetal klanten. Voorts stelt zij zich op het standpunt dat zij aanvullende maatregelen heeft genomen om een dergelijk incident in de toekomst te voorkomen.

   Volgens TechCrunch is het incident enkel vanwege de omvang van de toegankelijke database één van de grootste veiligheidsinbreuken van het jaar. [123]

b. In februari 2020 startte een Amerikaanse burger een class action op grond van nieuwe Californische privacyregelgeving naar aanleiding van een datalek bij Salesforce. Klantgegevens van een winkel voor kinderkleding waren bijna twee maanden onbeschermd beschikbaar geweest. Het ging om onder meer namen, adressen en credit card gegevens. De gegevens zijn te koop aangeboden op het “dark web”. Het datalek werd veroorzaakt door malware, geïnstalleerd op het platform van Salesforce.[124]

c. In 2018 waarschuwde Salesforce een aantal van haar klanten dat door hen opgeslagen gegevens meer dan een maand toegankelijk waren voor derden. Dit kwam door een Salesforce veroorzaakte softwarefout. Salesforce controleerde het verkeer naar haar servers niet, en kon niet ontdekken of en in welke mate gebruik was gemaakt van het lek.[125]

d. In mei 2018 vond een datalek plaats bij een start-up genaamd Apollo. Het datalek betrof meer dan 200 miljoen contacten (personen en ondernemingen), met totaal meer dan 9 miljard datapunten. Veel klanten van Apollo hadden hun account gekoppeld aan Salesforce, waardoor de gegevens van Salesforce en Apollo uitgewisseld waren. Het Apollo datalek bevat om die reden ook een grote hoeveelheid Salesforce gegevens.[126]

---

[122] Techcrunch, *Oracle’s BlueKai tracks you across the web. The data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).
[123] Techcrunch, *Oracle’s BlueKai tracks you across the web. The data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).
[124] Law Street, *Salesforce Cloud Data Breach Leaked Thousands of Customers’ Information,* 5 februari 2020, te raadplegen via: https://lawstreetmedia.com/tech/salesforce-cloud-data-breach-leaked-thousands-of-customers-information/.
[125] Bank Info Security, *Salesforce Security Alert: API Error Exposed Marketing Data,* 3 augustus 2019, te raadplegen via: https://www.bankinfosecurity.com/salesforce-security-alert-api-error-exposed-marketing-data-a-11278.
[126] Wired, *A Recent Startup Breach Exposed Billions of Data Points,* 10 mei 2018, te raadplegen via: https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/.

# 4 JURIDISCH KADER

## 4.1 Inleiding

150. Bij de hiervoor omschreven handelingen verwerken Oracle en Salesforce op grote schaal persoonsgegevens en handelen zij in strijd met het recht op privacy van internetgebruikers. Het recht op bescherming van persoonsgegevens en het recht op bescherming van de persoonlijke levenssfeer worden erkend als fundamentele rechten.

151. Artikel 7 van het Handvest van de grondrechten van de Europese Unie ("**Handvest**") bevat het algemene recht op bescherming van het privéleven. Artikel 8 Handvest omschrijft een apart en autonoom grondrecht op bescherming van persoonsgegevens. [127] Artikel 8 lid 1 Handvest luidt:

> *"Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens."*

152. In het tweede lid worden vijf voorwaarden aan de verwerking gesteld (nummering toegevoegd door advocaat): *"[De] gegevens moeten (1) eerlijk worden verwerkt, (2) voor bepaalde doeleinden en (3) met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. (4) Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en (5) op rectificatie daarvan.*" Het derde lid vereist dat een onafhankelijke autoriteit wordt ingesteld die toeziet op de naleving van deze regels.

153. Als gevolg van de invoering van het Handvest in 2009 heeft de bescherming van persoonsgegevens een zeer prominente plaats gekregen in de jurisprudentie van het Hof van Justitie van de Europese Unie ("**HvJEU**"). Het HvJEU heeft meermaals bevestigd dat het niet mogelijk is (lagere) privacyregelgeving te interpreteren zonder te kijken naar de grondrechtelijke achtergrond.[128]

154. Binnen de Europese Unie is het recht op gegevensbescherming voor het eerst verankerd in de Privacyrichtlijn[129] van 1995, die in Nederland werd geïmplementeerd in de Wet bescherming persoonsgegevens ("**Wbp**").[130] Voor het digitale domein werd bovendien de e-Privacyrichtlijn[131] aangenomen, met de doelstelling om de Privacyrichtlijn aan te vullen. De e-Privacyrichtlijn tracht een hoge mate van privacy te garanderen bij de communicatie via openbare netwerken, ongeacht welke technologie daarbij ook gebruikt wordt.

155. Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming ("**AVG**") van toepassing, die in de plaats is getreden van de Privacyrichtlijn en de Nederlandse Wbp Nu de

[127] Net als (de gewijzigde versie van het) Verdrag betreffende de werking van de Europese Unie (*PbEU* 2010, C 83/47),) ("**VWEU**"), waarin het recht op bescherming van persoonsgegevens is opgenomen in artikel 16.
[128] Zie b.v. HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain t. Costeja*), r.o. 38
[129] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PbEG* 1995, L 281-31) ("Privacyrichtlijn").
[130] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens, *Stb.* 2000, 302.
[131] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie (*PbEG* 2002, L 201/37), als gewijzigd in Richtlijn 2006/24/EG en Richtlijn 2009/136/EG (*PbEG 2002, L 201/37).*

Uniewetgever heeft gekozen voor een verordening, niet voor een richtlijn, heeft dit tot gevolg dat de bepalingen uit de AVG rechtstreekse werking hebben. De AVG heeft het grondrecht op gegevensbescherming verder versterkt en geharmoniseerd.

156. In de onderhavige zaak wordt de handelwijze van Oracle en Salesforce zowel getoetst aan het grondrechtelijke kader als aan de AVG en de bijzondere bepalingen in de Telecommunicatiewet ("**Tw**"). Het betreft een separate, cumulatieve toetsing.[132] De AVG staat niettemin in nauw verband met de grondrechtelijke context en vormt daarvan een uitwerking, hetgeen ook wordt bevestigd door overweging 1 in de preambule van de AVG:

> *"De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie (het „Handvest") en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van zijn persoonsgegevens."*

157. Omdat de Privacyrichtlijn en de AVG voor een belangrijk deel van dezelfde begrippen uitgaan, is de interpretatie van de Privacyrichtlijn door het HvJEU of supranationale organen ook relevant voor de interpretatie van de AVG.

158. In deze zaak is bovendien voorts artikel 11.7a Tw van belang voor de beoordeling van de handelwijze van Oracle en Salesforce. Artikel 11.7a Tw bevat de zogenaamde Cookiewet en vormt de implementatie van artikel 5 lid 3 van de ePrivacyrichtlijn.[133]

159. De Autoriteit Persoonsgegevens ("**AP**") houdt toezicht op naleving van de AVG in Nederland. De Autoriteit Consument & Markt ("**ACM**") houdt toezicht op naleving van o.a. artikel 11.7a Tw. Daarnaast houdt de AP toezicht op naleving van artikel 11.7a Tw voor zover het de verwerking van persoonsgegevens betreft. De European Data Protection Board ("**EDPB**") is een orgaan waarin alle nationale privacytoezichthouders uit de Europese Unie samenwerken bij hun toezicht op de AVG. De EDPB heeft de Artikel 29-werkgroep ("**WG29**") opgevolgd.

160. Uit het feitelijk kader volgt dat Oracle en Salesforce op uiteenlopende manieren persoonsgegevens verwerken en gebruikmaken van cookies, onder meer door de volgende handelingen:

i. Oracle en Salesforce plaatsen cookies uitgerust met een unieke identificator op de randapparatuur van de internetgebruiker;

ii. Oracle en Salesforce verzamelen met behulp van deze cookies en andere unieke identificatoren persoonlijke informatie over de internetgebruiker;

[132] Zie ook conclusie AG Saugmandsgaarde van 19 juli 2016 in gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:572, (*Tele2*), punt 131.
[133] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), als gewijzigd in Richtlijn 2006/24/EG en Richtlijn 2009/136/EG (*PbEG 2002, L 201/37).*

iii. Oracle en Salesforce evalueren de persoonlijke aspecten van internetgebruikers met het doel persoonlijke voorkeuren, interesses, gedrag en andere kenmerken van hen te analyseren of te voorspellen ("profilering");

iv. Oracle en Salesforce verrijken deze profielen en persoonsgegevens met informatie uit andere bronnen;

v. Oracle en Salesforce verschaffen deze profielen aan derden, zodat deze gebruikt kunnen worden om in een veiling te beoordelen of en, zo ja, hoeveel zij willen bieden voor advertentieruimte ("real-time bidding");

vi. Oracle en Salesforce koppelen de unieke identificator van de cookies aan de unieke identificatoren van de cookies van andere adtech partijen om gegevensuitwisseling mogelijk te maken ("cookie syncing").

161. In het navolgende zal worden uiteengezet dat Oracle en Salesforce op meerdere manieren in strijd handelen met de relevante grondrechten, AVG en artikel 11.7a Tw. Met name is sprake van schending van het verbod op profilering en de onder meer de beginselen van rechtmatigheid, transparantie en dataminimalisatie worden geschonden.

162. De conclusie is dan ook dat Oracle en Salesforce op ernstige wijze het relevante regelgevend kader schenden en onrechtmatig handelen jegens de personen wier belangen de Stichting behartigt. Gelet op de aard, de ernst en de duur van de inbreuk zijn Oracle en Salesforce schadeplichtig jegens de betrokkenen.

163. In het navolgende zal eerst de schending van de fundamentele rechten worden uiteengezet. Aansluitend zal de schending van de AVG en Tw worden behandeld.

### 4.2 Schending artikelen 7, 8 en 11 van het Handvest

164. De artikelen 7 en 8 van het Handvest zijn nauw met elkaar verbonden. Het recht op bescherming van persoonsgegevens berust mede op de eerbieding van het privéleven. Het HvJEU heeft bevestigd dat de gegevensbescherming op grond van artikel 8 Handvest van bijzonder belang is voor het in artikel 7 verankerde recht op eerbiediging van het privéleven.[134] Met de introductie van artikel 8 in het Handvest heeft de Uniewetgever niettemin een autonoom fundamenteel recht gecreëerd met een specifieke en verstrekkende reikwijdte. Het Handvest bevat met artikel 8 een grondrecht *sui generis* ten behoeve van gegevensbescherming, anders dan het Europees Verdrag van de Rechten voor de Mens ("**EVRM**"), waarbinnen persoonsgegevens bescherming vinden op grond van het algemene recht op bescherming van het privéleven (artikel 8 EVRM). [135]

165. Afhankelijk van de aard van de gegevens en de aard van de activiteiten, kan een gegevensverzameling en -verwerking een inmenging vormen van zowel artikel 7 als artikel 8 Handvest. Zoals AG Cruz Villalon uitlegt in zijn conclusie bij de zaak de zaak *Digital Rights Ireland* kan een onderscheid gemaakt worden tussen "gewone persoonsgegevens" en informatie die meer verband houdt met het privéleven, met intimiteit, met andere woorden

[134] HvJEU 8 april 2014, zaak c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), r.o. 53.
[135] Zie onder meer EHRM 16 februari 2000, no. 27798/95, (*Amann t. Zwitserland*), r.o. 65.

die bijzondere kenmerken van het persoonlijk leven blootlegt. Een inmenging in de eerste categorie zal vooral artikel 8 Handvest raken, terwijl inmenging in de tweede categorie ook strijdig is met artikel 7 Handvest. [136]

166. In de onderhavige zaak betreft de handelwijze van Oracle en Salesforce zowel een bijzonder ernstige inmenging in het recht op eerbiediging van het privéleven (artikel 7 Handvest) als het recht op bescherming van persoonsgegevens (artikel 8 Handvest).

167. Het creëren van een gigantische database gegevens over internetgebruikers, de koppeling van databases van derden daaraan, het verrijken van de informatie, het creëren van profielen, het gedurende lange tijd bewaren van de gegevensverzameling, dat alles raakt in bijzondere mate de bescherming van het privéleven. De enkele aanwezigheid van zo'n enorme gegevensverzameling die alleen met moderne technieken voor big data, algoritmes en kunstmatige intelligentie kan ontstaan vormt al een constante bedreiging voor het privéleven.

168. In de zaak *Digital Rights Ireland* gaat het om de bewaring van een beperkt aantal specifieke gegevens op grond van een specifieke richtlijn die voorschrijft dat, kort gezegd, telecomaanbieders gegevens bewaren ten behoeve van het onderzoeken en vervolgen van ernstige criminaliteit door de bevoegde autoriteiten. Het gaat onder meer om gegevens die nodig zijn om de bron en de bestemming van de telecommunicatie te traceren en identificeren, zogenaamde verkeersgegevens. Het HvJEU oordeelde dat uit deze gegevens "zeer precieze conclusies" worden getrokken over het privéleven van de personen.

> *"Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren."* [137]

169. AG Cruz Villalon geeft in zijn conclusie aan dat het loutere bewaren van verkeersgegevens in de zaak *Digital Rights Ireland* resulteert in een "permanente bedreiging" van het recht op bescherming van de persoonlijke levenssfeer en een "gevoel van gecontroleerd worden".[138] Dit vormt bij uitstek een inmenging in het fundamentele recht dat artikel 7 Handvest beschermt. Het HvJEU voegt daaraan toe dat ook de toegang van de bevoegde nationale autoriteiten een aanvullende inmenging in dat recht vormt.[139] Het feit dat gegevens worden bewaard en later gebruikt, leidt ertoe dat bij de betrokken personen het gevoel wordt opgewekt "dat hun privéleven constant in de gaten wordt gehouden", aldus het HvJEU.[140] De mededeling van persoonsgegevens aan een derde vormt ook een inmenging in artikel 7 Handvest.[141]

170. In de onderhavige zaak gaat het niet alleen om de bewaring of mededeling van persoonsgegevens, maar ook om de uitwisseling, verrijking en voortdurende en dagelijkse verzameling van een schier oneindige hoeveelheid gegevens, die bijzondere en gevoelige

[136] Conclusie AG Cruz Villalon van 12 december 2013, zaak c-293/12, (*Digital Rights Ireland*).
[137] HvJEU 8 april 2014, zaak c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), r.o. 27.
[138] Conclusie AG Cruz Villalon van 12 december 2013, zaak c-293/12, (*Digital Rights Ireland*), punt 72.
[139] HvJEU 8 april 2014, zaak c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), r.o. 35. Zie ook HvJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*), r.o. 170.
[140] HvJEU 8 april 2014, zaak c-293/12, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), r.o. 37.
[141] Zie HvJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*), r.o. 171.

kenmerken over het persoonlijk leven van individuen blootleggen. Het gaat bovendien om een gegevensverwerking die niet ten dienste staat van het gerechtvaardigde belang van de overheid, in het bijzonder de bevoegde opsporingsautoriteiten, maar van de louter commerciële belangen van duizenden partijen die actief zijn in de *ad-tech* industrie.

171. Dat alles vormt vanzelfsprekend een inmenging in artikel 7 Handvest.

172. Aangezien het in de onderhavige zaak gaat om de grootschalige verwerking van persoonsgegevens wordt ook artikel 8 van het Handvest in de kern aangetast. Artikel 8 van het Handvest wordt onder meer in het bijzonder geraakt door het plaatsen van cookies uitgerust met unieke identificatoren, de uitwisseling van Cookie IDs in het kader van cookie syncing en de verspreiding van profielen onder talloos veel commerciële partijen in het kader van RTB. Dat geldt te meer nu de betrokkenen er geen weet van hebben dat hun profiel aan de hoogste bieder wordt verkocht, laat staan wat al die honderden partijen die niet het winnende bod hebben uitgebracht maar wel het profiel hebben ontvangen tijdens een veiling met hun profiel doen.

173. In de zaak *Tele2* oordeelt het HvJEU dat de bewaring van verkeergegevens ook invloed heeft op de wijze waarop gebruikers van elektronische communicatiemiddelen gebruik maken van hun communicatiemiddelen. Het HvJEU beklemtoont dat daarom de aan de orde zijnde nationale regeling die de verplichting oplegt verkeersgegevens te bewaren niet alleen getoetst moet worden aan de artikelen 7 en 8 Handvest, die in de prejudiciële vragen van de Zweedse en Engelse rechter waren genoemd, maar ook aan het fundamentele recht van vrijheid van meningsuiting dat door artikel 11 Handvest wordt beschermd.[142] Het HvJEU noemt dit grondrecht "een van de wezenlijke grondslagen van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie (…) is gebaseerd".[143]

174. Dit recht wordt in de onderhavige zaak ook in de kern geraakt. De gegevensverwerking die onderwerp is van deze zaak kan er immers toe leiden dat men afkerig wordt van het gebruik van het belangrijkste communicatiemiddel van deze tijd, het internet. Het gebruik hiervan is op dit moment immers alleen mogelijk in het geval de internetgebruiker accepteert dat hij voortdurend wordt gevolgd en dat een profiel van hem wordt ontwikkeld en onderhouden op basis waarvan hij advertenties krijgt voorgeschoteld, passend bij zijn specifieke karaktereigenschappen. In het bijzonder wordt de vrijheid informatie te garen geraakt, hetgeen onderdeel is van de vrijheid van meningsuiting. Dat geldt helemaal in het geval de internetgebruiker geen toegang tot informatie krijgt als hij niet accepteert dat hij gesegmenteerd en gevolgd wordt, onder meer door middel van "cookiewalls".

175. De activiteiten van Oracle en Salesforce vormen dus een ernstige inmenging in de fundamentele rechten die bescherming vinden in de artikel 7, 8 en 11 van het Handvest. De Stichting kan zich ten behoeve van de Gedupeerden hier rechtstreeks op beroepen. De

[142] HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 92.
[143] HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 93.

grondrechten uit het Handvest werken in horizontale verhoudingen. Het HvJEU heeft dat meerdere malen erkend.[144]

176. Op grond van artikel 52 lid 1 Handvest moeten beperkingen op de in het Handvest erkende rechten bij wet zijn gesteld en de wezenlijke inhoud daarvan eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld wanneer deze noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de bescherming van de rechten van anderen.[145] In de onderhavige zaak betekent dat concreet dat:

- De activiteiten van Oracle en Saleforce een wettelijke grondslag moeten hebben;
- De activiteiten van Oracle en Salesforce de wezenlijke inhoud van de in het Handvest erkende rechten eerbiedigen;
- De activiteiten van Oracle en Salesforce noodzakelijk zijn om een doelstelling van algemeen belang na te streven of noodzakelijk zijn ter bescherming van hun rechten en daadwerkelijk geschikt moeten zijn om die doelstelling na te streven of die rechten te beschermen;
- De activiteiten van Oracle en Salesforce evenredig zijn, in een democratische samenleving, aan het nagestreefde doel.[146]

177. De handelwijze van Oracle en Salesforce voldoet aan geen van deze vereisten.

178. In de eerste plaats geldt dat de handelingen van Oracle en Salesforce niet gebaseerd zijn op een nationale wet, laat staan een Unierichtlijn, zoals het geval was in de zaken *Digital Rights Ireland* en *Tele2*. Zij kunnen zich niet beroepen op een rechtsgrond die inmenging in de rechten toestaat die "zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht bepaalt".[147] Integendeel, Oracle en Salesforce rechtvaardigen hun handelwijze louter met het argument dat deze binnen de stringente voorwaarden van de AVG en Tw valt. In het bijzonder baseren Oracle en Salesforce zich op uitzonderingen of beperkingen in de regelgeving, die volgens vaste rechtspraak van het HvJEU strikt moeten worden uitgelegd.[148] Zoals hieronder bij de toetsing van de activiteiten van Oracle en Salesforce aan de AVG en de Tw zal blijken, schenden zij een veelheid van elementaire beginselen en bepalingen uit de AVG en de Tw. De activiteiten berusten dus niet op een voldoende toegankelijke en voorzienbare wettelijke grondslag die naar behoren tegen willekeur beschermt, zoals het criterium "bij wet gesteld" vereist.[149]

---

[144] Zie onder meer HvJEU 8 april 1976, zaak 43/75 (*Defrenne*), HvJEU 12 juli 2011, zaak C-324/09, ECLI:EU:C:2011:474 (*L'Oréal / eBay*), HvJEU 24 november 2011, zaak C-70/10 , ECLI:EU:C:2011:771 (*Scarlet/SABAM*). Zie ook HvJEU 27 maart 2014, zaak C-314/12, ECLI:EU:C:2014:192 (*UPC Telekabe*l), HvJEU 29 januari 2009, zaak C-275/16, ECLI:EU:C:2008:54 (*Promusicae*) en HvJEU 19 februari 2009, zaak C-557/07 (*LSG / Tele2*).
[145] HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 94.
[146] Vgl. conclusie AG Saugmandsgaardoe van 19 juli 2016 in gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:572, (*Tele2*), punt 132
[147] Zie HvJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*), r.o. 175.
[148] HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 89.
[149] Vgl. conclusie AG Saugmandsgaardoe van 19 juli 2016 in gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:572, (*Tele2*), punten 134-154.

179. In de tweede plaats geldt dat de handelingen van Oracle en Salesforce de wezenlijke inhoud van de relevante fundamentele rechten in de kern raken. Zoals hierboven aangegeven gaat het om een ingreep in de grondrechten die bijzonder groot en ernstig is. Het feit dat internetgebruikers geen of onvoldoende wetenschap hebben van de gewraakte praktijken kan bij hen immers het gevoel opwekken dat hun privéleven "constant in de gaten wordt gehouden", aldus ook het HvJEU in de zaak *Tele2*. [150]

180. In de derde plaats geldt dat Oracle en Salesforce hun handelingen niet verrichten ten behoeve van een algemeen belang. AG Cruz Villalon schrijft in zijn conclusie in de zaak *Digital Rights Ireland* dat de in die zaak aan de orde zijnde "retentie" van gegevens nooit zou mogen bestaan en, waar dat wel zo is, zouden daarvoor zeer dwingende redenen van algemeen belang moeten bestaan.[151] Welnu, in de onderhavige zaak is van enig algemeen belang geen sprake. Oracle en Salesforce verrichten hun handelingen, inclusief de dataopslag, louter ten behoeve van hun eigen commerciële belangen en de commerciële belangen van derden.

181. Oracle en Salesforce kunnen ook niet een bijzonder recht inroepen dat voorziet in de bescherming van hun activiteiten. Voorzover zij zich zouden beroepen op de vrijheid van meningsuiting, geldt dat dit fundamentele recht reclame-uitingen slechts in beperkte mate beschermt. Artikel 7 lid 4 Grondwet sluit handelsreclame zelfs uit van de grondwettelijke bescherming van de uitingsvrijheid. Uit vaste jurisprudentie van het EHRM volgt dat "commercial speech" minder bescherming geniet en de lidstaten een ruime "margin of appreciation" hebben om daaraan beperkingen te stellen.[152] De vrijheid van meningsuiting biedt al helemaal geen bescherming aan de veelheid van handelingen van Oracle en Salesforce, in onderling verband beschouwd, binnen het ecosysteem van online marketing.

182. Hoe dan ook, zullen de grondrechten waar de Stichting zich in deze zaak op beroept bij afweging van deze fundamentele rechten prevaleren.

183. In de vierde en laatste plaats komt het vereiste dat de activiteiten van Oracle en Salesforce evenredig moeten zijn aan het beoogde, legitieme doel in de zin van artikel 52 Handvest. Dit vereiste hoeft uw rechtbank niet te onderzoeken, nu hierboven al is vastgesteld dat de handelingen van Oracle en Salesforce geen legitiem doel nastreven en zij zich ook niet kunnen beroepen op een eigen fundamenteel recht dat bescherming behoeft. Niettemin wordt in het navolgende uiteengezet dat de handelingen van Oracle en Salesforce niet evenredig zijn als bedoeld in artikel 52 Handvest.

184. Opgemerkt zij dat dit evenredigheidsbeginsel verder gaat dan evenredigheid als algemeen beginsel voor het optreden in de Unie (in de zin van artikel 5 lid 4 van het Verdrag betreffende de Europese Unie) en gaat specifiek om evenredigheid als "constitutieve voorwaarde voor enige beperking van grondrechten".[153] Hiertoe is vereist dat de uitzonderingen op de bescherming van persoonsgegevens binnen de grenzen van het "strikt noodzakelijke" blijven. Volgens vaste jurisprudentie van het HvJEU moeten beperkingen duidelijke en nauwkeurige regels bevatten over de reikwijdte en de toepassing van de uitzondering, die minimale eisen

[150] Vgl. HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 100.
[151] Conclusie AG Cruz Villalon van 12 december 2013, zaak C-293/12, (*Digital Rights Ireland*), punt 144.
[152] Zie o.a. EHRM 20 november 1989, zaak 10572-83, (*Markt Intern t. Duitsland*), r.o. 33.
[153] Conclusie AG Cruz Villalon van 12 december 2013, zaak C-293/12, (*Digital Rights Ireland*), punt 133.

opleggen, zodat degenen van wie gegevens worden verzameld, verrijkt, uitgewisseld, bewaard en verkocht over voldoende garanties beschikken dat hun persoonsgegeven doeltreffend worden beschermd tegen het risico van misbruik.[154] Het HvJEU geeft in de recente zaak *Schrems II* aan dat:

> *"De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens automatisch worden verwerkt (...)."*

185. Dergelijke garanties of waarborgen geven Oracle en Salesforce niet. Het is voor de gemiddelde internetgebruiker volstrekt onduidelijk welke informatie betreffende hem wordt verzameld, voor welke doeleinden, voor welke periode. Hij weet niet hoe zijn profiel is opgebouwd, met wie zijn profiel wordt gedeeld en op welke wijze adverteerders op basis van zijn profiel hem aanbiedingen doen. De gegevens worden ook onvoldoende beveiligd zoals blijkt uit de in het feitelijk kader beschreven datalekken.

186. Voorzover "behaviorial targeting" een legitiem doel kan vormen, is de wijze waarop Oracle en Salesforce het proces hebben ingericht volstrekt buitenproportioneel. Het is onnodig dagelijks persoonlijke gegevens van internetgebruikers te verzamelen, verrijken, uit te wisselen, bewaren en verkopen om online reclame te maken. Het gericht adverteren kan ook op andere manieren. Advertenties kunnen ook gericht zijn op de interesses van de lezer, afhankelijk van de inhoud van het artikel. Dit wordt contextueel adverteren genoemd.[155] Onder meer de New York Times is naar aanleiding van de AVG overgestapt op deze vorm van adverteren en haar inkomsten uit advertenties stijgen nog steeds.[156]

187. In januari 2020 is ook Ster Reclame gestopt met het gebruik van cookies voor het aanbieden van advertenties en overgestapt op contextueel adverteren op de websites van de NPO. Ster Reclame publiceerde hierover een uitgebreid onderzoek en concludeerde onder meer dat contextueel adverteren zorgt voor een online omzetstijging van meer dan 50% ten opzichte van adverteren op basis van persoonsgegevens.[157]

188. Ook andere privacyvriendelijke alternatieven zijn beschikbaar zodat websites de mogelijkheid hebben om inkomsten te generen met gebruik van advertenties, zonder de grootschalige datahandel die inherent is aan het RTB systeem.[158]

189. Gelet op het voorgaande schenden Oracle en Salesforce de relevante grondrechten. Zoals opgemerkt in de inleiding van het juridisch kader vormen de AVG en de Tw deels een nadere uitwerking van de hierboven besproken grondrechten. De AVG en Tw zullen daarom mede uitgelegd moeten worden in het licht van de bescherming van de fundamentele rechten die de Uniewetgever met deze regelgeving beoogt te beschermen. Alvorens de specifieke schendingen van de AVG en de Tw te behandelen, zal hieronder eerst uiteen gezet worden dat de AVG en Tw op de onderhavige zaak van toepassing zijn.

---

[154] Zie HvJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559, (*Schrems II*), r.o. 176.
[155] Kobler, *Study of Effects of Contextual Targeting on News,* te raadplegen op: https://kobler.no/contextual-insights/.
[156] Digiday, *After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue,* 16 januari 2019, te raadplegen op: https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.
[157] Ster reclame, *Een toekomst zonder advertentiecookies? Het kan!*, p. 17.
[158] Medium, *Blockchain & Advertising – New Solutions to Old Problems,* 28 juni 2018, te raadplegen op: https://medium.com/trivial-co/blockchain-advertising-new-solutions-to-old-problems-e7fcbbc16b85.

## 4.3 Toepasselijkheid AVG en artikel 11.7a Tw

*4.3.1 Verwerking van persoonsgegevens*

190. De AVG is van toepassing op de *verwerking* van *persoonsgegevens*. Degene op wie persoonsgegevens betrekking hebben wordt de *betrokkene* genoemd. Oracle en Salesforce betwisten niet dat persoonsgegevens worden verwerkt. Dat blijkt uit de privacy documentatie gepubliceerd op hun websites (**Producties 22 en 23**).

4.3.1.1 Privacy documentatie van Oracle

191. Oracle beschrijft haar verwerkingen van persoonsgegevens in een serie van zeven privacy documenten.[159] De DMP dienst valt onder Oracle's "Data Cloud" en wordt, met name, beschreven in het Oracle "Privacybeleid voor Oracle Data Cloud" (**Productie 22.a**) en het "AddThis Privacy Policy"(**Productie 22.b**).

192. Het Privacybeleid voor Oracle Data Cloud lijkt betrekking te hebben op alle Oracle Data Cloud en Marketing Cloud diensten, waaronder de DMP dienst. Het AddThis Privacy Policy ziet op gegevens die verzameld worden via de sociale media knoppen die Oracle aanbiedt onder de naam AddThis. Deze gegevens worden gebruikt in de DMP dienst. Oracle heeft daarnaast een "Algemeen privacybeleid van Oracle". Hierin omschrijft zij onder meer de verwerking van gegevens van haar websitebezoekers en klanten. Het Algemeen privacybeleid van Oracle lijkt niet van toepassing te zijn op de DMP dienst, maar omdat deze erg algemeen is opgesteld, kunnen wij niet uitsluiten dat dat toch het geval is.

4.3.1.2 Privacy documentatie van Salesforce

193. De wijze waarop Salesforce persoonsgegevens verwerkt, moet ontleend worden uit diverse documenten. De Nederlandse website bevat links naar drie "privacyverklaringen" (**Productie 23.a**):

a. De volledige Privacyverklaring (**Productie 23.b**);
b. Een bericht over de Privacy Shield Certification; en
c. Een data processing addendum FAQ.

194. Daarnaast bevat de website een samenvatting van de belangrijkste punten uit de volledige privacyverklaring (**Productie 23.a**).

195. De volledige privacyverklaring (**Productie 23.b**) bevat slechts enkele onderdelen die zien op de DMP activiteiten zoals in deze dagvaarding omschreven, te weten:

a. De opname van "advertentie cookies" in de lijst van typen cookies die Salesforce gebruikt, zonder aanduiding van de websites waarop zij dit doet, met de beschrijving:

*"Advertentiescookies volgen activiteit op websites om inzicht te verwerven in de interesses van een bezoeker en direct marketing op hem af te stemmen.*

[159] https://www.oracle.com/nl/legal/privacy/ en https://www.oracle.com/legal/privacy/, geraadpleegd op 14 juli 2020.

*We gebruiken soms cookies die door ons of door derden zijn verstrekt om u op apparaten die u gebruikt advertenties te tonen voor onze producten waarin u volgens ons mogelijk interesse hebt en om de prestaties van onze advertenties bij te houden. Deze cookies verzamelen bijvoorbeeld informatie zoals welke browser u hebt gebruikt bij het bezoeken van onze websites.*

*Salesforce sluit ook contracten af met advertentienetwerken van derden die IP-adressen en andere informatie verzamelen van webbakens op onze websites, van e-mails en op websites van derden. Advertentienetwerken volgen uw online activiteiten in de loop van de tijd en op verschillende websites of andere online diensten door het verzamelen van apparaat- en gebruiksgegevens via geautomatiseerde middelen, waaronder door het gebruik van cookies. Deze technologieën kunnen u herkennen op de verschillende apparaten die u gebruikt. Wanneer we werken met advertentienetwerken van derden, vereisen we dat ze hun gegevensverwerking beperken tot alleen datgene wat nodig is om ons de gevraagde advertentiediensten te verstrekken."*[160]

b. Een afmeldmogelijkheid voor gerichte advertenties van/via Salesforce Audience Studio:

*"Klik hier om u af te melden voor gerichte advertenties die door Salesforce Audience Studio aan ons en aan derden worden verstrekt."*[161]

c. Een afmeldmogelijkheid voor gerichte advertenties van / via Salesforce DMP:

*"Klik hier om u af te melden voor gerichte advertenties die door Salesforce DMP aan ons en aan derden worden verstrekt. Houd er echter rekening mee dat u mogelijk niet volledig kunt profiteren van de websites door het blokkeren of verwijderen van cookies en soortgelijke technologieën die op onze websites worden gebruikt."*[162]

196. Een Nederlandse internetgebruiker die de website van Salesforce[163] bezoekt, wordt automatisch doorgeleid naar de Nederlandse pagina,[164] en krijgt daarom in beginsel slechts voornoemde informatie te zien wanneer hij daar op "Privacyverklaring" klikt. Op de Engelstalige versie van de website met privacy documentatie[165] wordt echter meer informatie verstrekt (**Productie 23.c**). Op die pagina is onder meer een document genaamd "Salesforce Audience Studio Privacy Policy" (**Productie 23.d**)[166] te vinden onder de kop "Resources in respect of how we protect our customer's data as a processor". Hierin is meer informatie opgenomen over de verwerkingen in verband met de DMP dienst van Salesforce. Het Salesforce Audience Studio Privacy Policy maakt niet duidelijk of het exclusief of in aanvulling van de volledige privacyverklaring van toepassing is.

[160] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder 4.2 (tevens bijgevoegd als **Productie 23.b)**.
[161] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder 4.3 (tevens **Productie 23.b**).
[162] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder 4.4 (tevens **Productie 23.b**).
[163] https://www.salesforce.com, geraadpleegd op 14 juli 2020.
[164] https://www.salesforce.com/nl/?ir=1, geraadpleegd op 14 juli 2020.
[165] https://www.salesforce.com/company/privacy/, geraadpleegd op 14 juli 2020.
[166] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/ (tevens **Productie 23.d**).

197. Overige informatie over de DMP dienst van Salesforce is beschikbaar op Engelstalige websites van Salesforce die gericht zijn op de klanten van Salesforce, zoals de Trust and Compliance Documentation pagina van Salesforce (**Productie 23.e**).[167] Deze documentatie is niet eenvoudig vindbaar voor een gemiddelde internetgebruiker.

4.3.1.3 Oracle en Salesforce erkennen dat zij persoonsgegevens verwerken

198. In de voornoemde documentatie erkennen Oracle en Salesforce dat zij persoonsgegevens verwerken in het kader van de DMP dienst. In haar brief van 18 juli bevestigt Oracle ook dat zij persoonsgegevens verzamelt (**Productie 5**). Zij onderscheidt de gegevens die zij naar eigen zeggen verzamelt van "direct identifiers", maar daarmee wil Oracle niet het standpunt innemen dat zij geen persoonsgegevens verwerkt. Dat blijkt ook niet uit de brief.

199. Oracle en Salesforce betwisten voornamelijk, althans lijken te betwisten, dat zij aangemerkt moeten worden als verwerkingsverantwoordelijke ten aanzien van de gegevensverwerking.

200. Volledigheidshalve zal in het navolgende niettemin worden onderbouwd dat de informatie die Oracle en Salesforce verzamelen kwalificeert als "persoonsgegevens" en dat de handelingen die zij daarmee verrichten moeten worden aangemerkt als "verwerking" waarop de AVG van toepassing is.

4.3.1.4 Persoonsgegevens

201. Artikel 4 lid 1 AVG definieert het begrip *persoonsgegevens* als volgt:

> *"„persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;"*

202. De onderhavige zaak heeft, zoals in het feitelijk kader aangegeven (paragraaf 3.2.2), betrekking op onder meer de volgende informatie en gegevens:

a. Gegevens om de internetgebruiker te identificeren zoals een Cookie ID of een andere online identificator;

b. IP adres(sen);

c. Locatiegegevens;

d. Informatie over de gebruiker zoals andere websites die de gebruiker bezocht heeft, handelingen die hij op websites heeft verricht (zoals het klikken op een artikel) en gegevens die daaruit direct of indirect worden afgeleid zoals het geslacht, de leeftijd, woonplaats, aankoophistorie, inkomen, beroep, interesses en voorkeuren.

[167] https://trust.salesforce.com/en/trust-and-compliance-documentation/audience-studio-and-data-studio/ (tevens **Productie 23.e**).

Voornoemde gegevens worden in het navolgende aangeduid met "**Cookie IDs en daaraan gekoppelde informatie**".

203. Wanneer de verschillende onderdelen van de definitie van persoonsgegevens worden bekeken, blijkt ook dat Cookie IDs en daaraan gekoppelde informatie binnen deze definitie vallen. Het betreft immers:

a. informatie;

b. betreffende;

c. een geïdentificeerde of identificeerbare natuurlijke persoon.[168]

Ad a, het betreft informatie

204. Het HvJEU heeft in de zaak *Nowak* bevestigt dat uit de woorden "alle informatie" in de definitie van het begrip persoonsgegeven moet worden afgeleid dat de Uniewetgever een ruime betekenis aan dit begrip heeft willen geven, dat zich uitstrekt tot elke soort informatie, "zowel objectieve informatie als subjectieve informatie onder de vorm van meningen of beoordelingen".[169] De Cookie IDs en daaraan gekoppelde gegevens zijn informatie. Informatie kan objectief of subjectief zijn. Ook interesses en voorkeuren vallen onder het begrip informatie.

Ad b, betreffende

205. Persoonsgegevens onderscheiden zich van andere gegevens of informatie doordat zij betrekking hebben op een persoon. Cookie IDs en daaraan gekoppelde informatie hebben betrekking op en gaan over een persoon, namelijk een consument. Informatie kan ook over een persoon gaan als deze bijvoorbeeld een voorwerp dat eigendom is van een persoon (bijv. de waarde van een woning) betreft of processen of gebeurtenissen. Er moet gekeken worden naar de inhoud, het doel of het resultaat van de informatie om te beoordelen of de informatie over een persoon gaat.[170] In casu is alle informatie die door Oracle en Salesforce wordt verzameld en verwerkt, bedoeld om een zo breed mogelijk profiel van een internetgebruiker te verkrijgen. Alle informatie heeft dan ook betrekking op een persoon.

Ad c, een geïdentificeerde of identificeerbare natuurlijke persoon

206. De persoon op wie een Cookie ID en daaraan gekoppelde informatie betrekking heeft is niet in alle gevallen een "geïdentificeerde persoon". Deze informatie onthult immers, in de meeste gevallen, niet rechtstreeks en onmiddellijk wie de natuurlijke persoon is die een website bezocht.

207. Er is wel sprake van een persoon die direct of indirect (via een derde) geïdentificeerd kan worden, en dus een "identificeerbare persoon". Volgens artikel 4 lid 1 AVG wordt als identificeerbaar beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator. Als voorbeelden van een

[168] Artikel 29 werkgroep, Advies 4/2007 over het begrip persoonsgegeven, 20 juni 2007, WP136 ('WP136 Begrip persoonsgegeven'), p. 6.
[169] HvJEU 20 december 2017, C/434-16, (*Nowak*), ECLI:EU:C:2017:994, r.o. 34. Deze zaak is gewezen met toepassing van het begrip "persoonsgegeven" uit richtlijn 95-46.
[170] WP136 Begrip persoonsgegeven, p. 10-11.

identificator worden in dat artikel onder meer genoemd een identificatienummer, een online identificator en elementen die kenmerkend zijn voor de identiteit van die persoon.

208. Cookie IDs en de andere identificatoren die door Oracle en Salesforce worden gebruikt (zie onder 3.2.1 zijn dergelijke online identificatoren. Deze identificatoren hebben immers als enig doel internetgebruikers te herkennen op internet zodat aan hen de juiste advertentie kan worden getoond.

209. In de zaak *Planet49* bevestigde het HvJEU dat het plaatsen van een cookie met een uniek nummer, beschouwd moet worden als verwerking van persoonsgegevens, hetgeen overigens door Planet49 werd erkend.[171]

210. Dat Cookie IDs en daaraan gekoppelde informatie gegevens over een identificeerbare persoon betreffen, volgt ook uit de uitleg van de Advocaat-Generaal bij het *Breyer*-arrest van het HvJEU:

> *"56. De persoon op wie deze details betrekking hebben is geen „geïdentificeerde natuurlijke persoon". De datum en het tijdstip van een verbinding of het nummer voor de toegang tot de website onthullen niet rechtstreeks en onmiddellijk wie de natuurlijke persoon is die eigenaar is van het apparaat waarmee de website wordt bezocht, en evenmin de identiteit van degene die dat apparaat gebruikt (dat kan elke willekeurige natuurlijke persoon zijn).*
>
> *57. Aangezien echter een dynamisch IP-adres helpt te bepalen – hetzij alleen, hetzij in combinatie met andere gegevens – wie de eigenaar is van het voor het bezoeken van de website gebruikte apparaat, kan het worden beschouwd als informatie over een „identificeerbare persoon"."*[172]

211. Dat identificatie plaats kan vinden via online identificatoren zoals Cookie IDs, wordt voorts benadrukt in overweging 30 AVG:

> *"Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen."*

212. Ook WG29 overweegt nadrukkelijk dat een Cookie ID een persoonsgegeven is:

> *"When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used[11]. The*

[171] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*), r.o. 45.
[172] Conclusie AG Campos Sánchez-Bordona van 12 mei 2016 in zaak C-582/14, ECLI:EU:C:2016:779 (*Breyer*).

*behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned."*[173]

213. Het HvJEU benadrukt in dit verband dat uit het feit dat de Uniewetgever de uitdrukking "indirect" gebruikt, kan worden afgeleid dat het voor de kwalificatie van een gegeven als persoonsgegeven niet nodig is dat dit gegeven het op zichzelf mogelijk maakt de betrokken persoon te identificeren. Het is bovendien niet vereist dat alle informatie aan de hand waarvan de betrokkene kan worden geïdentificeerd, bij één en dezelfde partij berust. Als gevolg hiervan kunnen bijvoorbeeld dynamische IP-adressen worden aangemerkt als persoonsgegeven.[174] Evenmin is relevant of identificatie daadwerkelijk plaatsvindt.[175]

214. Over "behavioural advertising", een proces waarvan de diensten die Oracle en Salesforce bieden onderdeel uitmaakt, overweegt WG29 dat de verzameling van IP adressen en Cookie IDs tot doel hebben om individuele personen te kunnen onderscheiden van elkaar en informatie is betreffende een persoon, gebruikt om die persoon te beïnvloeden. WG29 verwijst in dat verband ook naar de mogelijkheid om profielen te koppelen aan andere informatie betreffende de betrokkene.

*"The Article 29 Working Party notes that the behavioural advertising methods described in this Opinion often entail the processing of personal data as defined by Article 2 of Directive 95/46/EC and interpreted by Article 29 Working Party[22]. This is due to various reasons: i) behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (through the cookie). The use of such devices with a unique identifier allows the tracking of users of a specific computer even when dynamic IP addresses are used. In other words, such devices enable data subjects to be 'singled out', even if their real names are not known. ii) Furthermore, the information collected in the context of behavioural advertising relates to, (i.e. is about) a person's characteristics or behaviour and it is used to influence that particular person[23]. This view is further confirmed if one takes into account the possibility for profiles to be linked at any moment with directly identifiable information provided by the data subject, such as registration related information. Other scenarios that can lead to identifiability are mergers, data losses and the increasing availability on the Internet of personal data in combination with IP addresses."*[176]

215. Naast Cookie IDs en andere online identificatoren verzamelen en verwerken Oracle en Salesforce allerlei gegevens over de internetgebruiker, waaronder de hiervoor opgesomde gegevens (onder paragraaf 3.2.2). Daaruit worden (direct of indirect) ook allerlei gegevens afgeleid over de betrokkene zoals het geslacht, de leeftijd, woonplaats, aankoophistorie, inkomen, beroep, interesses en voorkeuren. Het totale profiel dat bestaat uit verzamelde en afgeleide gegevens, bevat gegevens die in combinatie met elkaar maar op één persoon van

[173] Artikel 29 werkgroep, Advies 1/2008 over gegevensbescherming en zoekmachines, 4 april 2008, WP148 ('WP148 Zoekmachines'), p. 9.
[174] HvJEU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer*), r.o. 44 en in vergelijkbare zin HvJEU 29 juli 2019, C-40/17 (*Fashion ID*), ECLI:EU:C:2018:1039, r.o. 26-27.
[175] WP136 Begrip persoonsgegeven, p. 15-16.
[176] Artikel 29 werkgroep, Advies 2/2010 over online reclame op basis van surfgedrag ('behavioural advertising'), 22 juni 2010, WP171 ('WP171 Behavioural Advertising'), p. 9.

toepassing kunnen zijn.[177] Dat is ook nodig voor het uiteindelijke doel waarvoor de profielen worden opgesteld; het tonen van een advertentie die past bij de kenmerken en voorkeuren van één persoon.

216. Het doel van Oracle en Salesforce is om internetgebruikers van elkaar te kunnen onderscheiden en om deze internetgebruikers gerichte aanbieden te doen, gebaseerd op hun persoonlijke kenmerken en interesses. Het doel is een beeld te verkrijgen van de hoogstpersoonlijke en individuele kenmerken van de internetgebruikers teneinde deze te bewegen tot het doen van een aankoop of ander gedrag. Informatie die vanwege inhoud, doel of gevolg ertoe strekt een persoon te evalueren en beoordelen, moet bij uitstek als persoonsgegeven(s) worden gekwalificeerd. In de zaak *Nowak* oordeelde het HvJEU bijvoorbeeld dat examenantwoorden gekwalificeerd moeten worden als persoonsgegevens, onder meer, omdat het verzamelen van de antwoorden tot doel heeft een "evaluatie te maken van de beroepsbekwaamheden van de kandidaat".[178]

217. Ten slotte kan een profiel vaak via een of meerdere gegevens daarin direct aan een betrokkene gekoppeld worden. Denk hierbij bijvoorbeeld aan het koppelen van een telefoonnummer of IP-adres (in het profiel) aan een naam via de telefoon- of internetaanbieder.[179]

218. Dat de Cookie IDs en daaraan gekoppelde informatie die Oracle en Salesforce verwerken persoonsgegevens betreffen, is gezien het voorgaande evident.

219. Voor zover Oracle en Salesforce zouden betogen dat door pseudonimisering geen sprake is van persoonsgegevens, geldt het volgende. Van pseudonimisering is sprake wanneer gegevens aan pseudoniem zoals een nummer gekoppeld worden in plaats van bijvoorbeeld aan de naam van betrokkene. Bij pseudonimisering is dat pseudoniem echter nog steeds herleidbaar tot een geïdentificeerde of identificeerbare persoon. Om die reden geldt dat bij het gebruik van pseudonimisering nog steeds sprake is van persoonsgegevens. Wel kan pseudonimisering in het algemeen gezien worden als een noodzakelijke beveiligingsmaatregel omdat gepseudonimiseerde gegevens door derden minder eenvoudig misbruikt kunnen worden (zie tevens randnummers 514 e.v.). Dit doet echter geen afbreuk aan de toepasselijkheid van de AVG.[180]

220. Ten slotte is ook op grond van artikel 11.7a Tw sprake van persoonsgegevens, zoals hieronder nader zal worden besproken (paragraaf 4.3.2.2).

4.3.1.5 <u>Verwerken</u>

221. Artikel 4 lid 2 AVG definieert het begrip "verwerking" als volgt:

> *"verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken,*

[177] Ministerie van Justitie en Veiligheid, Handleiding Algemene verordening gegevensbescherming, januari 2018, 108130, p 25.
[178] HvJEU 20 december 2017, C/434-16, (*Nowak*), ECLI:EU:C:2017:994, r.o. 38.
[179] Ministerie van Justitie en Veiligheid, Handleiding Algemene verordening gegevensbescherming, januari 2018, 108130, p 25.
[180] Zie tevens Artikel 29 werkgroep, Advies 5/2014 over anonimiseringstechnieken, 10 april 2014, WP216 ("WP216 Anonimiseringstechnieken").

*verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;"*

222. Alle handelingen die met betrekking tot een persoonsgegeven kunnen worden verricht, vanaf het eerste moment dat een gegeven verzameld wordt tot en met het verwijderen ervan, vallen onder het begrip verwerken.

223. De handelingen die Oracle en Salesforce uitvoeren ten aanzien van persoonsgegevens, bestaan kort gezegd uit (zie paragraaf 3.2):

a. Het verzamelen van gegevens via cookies, andere online identificatoren en uit andere bronnen;

b. Het aan elkaar koppelen, combineren en verrijken van de gegevens;

c. Het analyseren en evalueren van de gegevens en toevoegen van afgeleide informatie;

d. De opslag in de DMP database;

e. Het beschikbaar maken van de gegevens ten behoeve van het RTB proces.

Deze handelingen moeten worden aangemerkt als verwerkingen in de zin van de AVG.

224. Oracle en Salesforce verwerken de persoonsgegevens voorts geautomatiseerd, waarmee de verwerking onder het materiele toepassingsgebied van artikel 2 AVG valt.

225. Bij de verwerking worden bovendien bepaalde persoonlijke aspecten van internetgebruikers geëvalueerd, met name met het doel persoonlijke voorkeuren, interesses, gedrag en andere kenmerken van internetgebruikers te analyseren of te voorspellen. Deze manier van het verwerken van persoonsgegevens wordt in artikel 4 lid 4 AVG aangemerkt als profilering. In de feiten is al uiteengezet welke uitgebreide profielen op deze manier worden opgesteld, en wat deze profielen kunnen zeggen over personen (zie met name paragraaf 3.2.3 t/m 3.2.5).

226. Dat de verwerking kan worden aangemerkt als profilering, maakt dat de verwerking in zijn algemeenheid als ingrijpender zal moeten worden beschouwd en dat aanvullende verplichtingen gelden om de belangen van betrokkenen te waarborgen. Deze zullen in het navolgende (waar relevant) worden besproken bij de behandeling van de inbreuk op de AVG en Tw (paragraaf 4.6).

*4.3.2 Artikel 11.7a Tw*

4.3.2.1 Toepasselijkheid op Oracle en Salesforce

227. Naast een verwerking van persoonsgegevens kwalificeert de handelwijze van Oracle en Salesforce als het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker in de zin van artikel 11.7a Tw. Oracle en Salesforce plaatsen immers cookies op de randapparatuur van gebruikers.

228. Oracle stelt zich op het standpunt alleen first party cookies te gebruiken, wat zou betekenen dat niet zij maar haar klanten de cookies plaatsen. Uit onderzoek blijkt echter dat bij een bezoek aan een grote hoeveelheid door Nederlanders veel bezochte websites cookies door een Oracle domein worden geplaatst (**Productie 16** en **Productie 9,** zie tevens randnummer 74 en paragraaf 3.3.1). Dat betekent dat die cookies niet door de klanten van Oracle worden geplaatst en uitgelezen maar door Oracle zelf.

229. Salesforce plaatst eveneens third party cookies en ontkent dit ook niet. Dat Salesforce third party cookies plaatst, blijkt ook uit **Productie 16 en Productie 10**, zie tevens randnummer 75 en paragraaf 3.3.1).

230. De handelswijze valt daarmee binnen het bereik van artikel 11.7a Tw, dat, kort gezegd, voor het plaatsen en uitlezen van cookies voorafgaande informatie en toestemming vereist.

4.3.2.2 Bewijsvermoeden tracking cookies

231. Bovendien is in artikel 11.7a lid 4 Tw een bewijsvermoeden opgenomen. Op grond daarvan wordt het gebruik van cookies om gegevens over het gebruik van verschillende online diensten te verzamelen, combineren of analyseren, zodat de betrokken persoon anders behandeld kan worden (zogenaamde tracking cookies), als een verwerking van persoonsgegevens beschouwd.

232. Artikel 11.7a lid 1 en 4 Tw luiden:

> *"1. Onverminderd de Algemene verordening gegevensbescherming is het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de randapparatuur van een gebruiker, alleen toegestaan op voorwaarde dat de betrokken gebruiker:*
>
> *(...)*
>
> *4. Een handeling als bedoeld in het eerste lid, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren zodat de betrokken gebruiker of abonnee anders behandeld kan worden, wordt vermoed een verwerking van persoonsgegevens te zijn."*

233. Het bewijsvermoeden in lid 4 Tw is toegevoegd wegens zorgen over de privacy-implicaties van third-party cookies en cookies waarmee surfgedrag, interesses en andere gegevens van internetgebruikers worden verzameld, gecombineerd en geanalyseerd voor commerciële doeleinden.[181] Dit is precies de kern van de onderhavige activiteiten van Oracle en Salesforce. De cookies van Oracle en Salesforce worden immers via een grote hoeveelheid websites geplaatst en geven bij bezoek aan de website informatie over de gebruikersactiviteit door aan Oracle en Salesforce. Daarmee kunnen Oracle, Salesforce en hun klanten het gedrag van betrokkenen over al die websites volgen. Ze verzamelen, combineren en analyseren gegevens over het gedrag van betrokkenen, en gebruiken die informatie vervolgens om betrokkenen anders te kunnen behandelen. Dat valt bij uitstek onder het bewijsvermoeden van artikel 11.7a

[181] *Kamerstukken II* 2010/11, 32 549, 39.

lid 4 Tw. Ook op grond van de Tw moet het handelen van Oracle en Salesforce dus worden aangemerkt als het verwerken van persoonsgegevens.

### 4.4 Verantwoordelijkheid

234. Zoals hiervoor opgemerkt, lijken Oracle en Salesforce te betwisten dat zij moeten worden aangemerkt als de "verwerkingsverantwoordelijke" ten aanzien van de hierboven omschreven gegevensverwerking, in ieder geval ten aanzien van delen van hun activiteiten.

235. In haar brief van 18 juni 2020 geeft Oracle aan dat zij slechts (zelfstandig) verwerkingsverantwoordelijke is ten aanzien van een gedeelte van haar DMP dienst. Oracle noemt deze dienst in haar brief Audience Data Marketplace ("ADM"). Oracle noemt deze dienst "optional" voor haar klanten. Haar DMP heeft echter geen of nauwelijks zelfstandige waarde zonder de dienst die zij ADM noemt Oracle geeft aan dat bij ADM de door haar via cookies verzamelde gegevens worden gekoppeld met gegevens afkomstig uit andere bronnen. Het zijn deze gegevens die zij vervolgens verkoopt aan adverteerders in het RTB-proces. Het onderscheid dat Oracle hier tracht te maken, bestaat feitelijk niet. De ADM dienst maakt onderdeel uit van de DMP dienst. De DMP dienst van Oracle is zonder ADM dienst commercieel niet of nauwelijks te exploiteren. Dit onderschrijft Oracle zelf ook in haar commerciële documentatie (zie randnummer 966.b).

236. Opmerkelijk genoeg neemt Oracle in haar privacy documentatie zelf ook een ander standpunt in. Daarin omschrijft Oracle zichzelf wel degelijk als verwerkingsverantwoordelijke. [182]

237. In het Privacybeleid voor Oracle Data Cloud dat specifiek ziet op de DMP dienst merkt zij Oracle Corporation en Oracle America, Inc. aan als verantwoordelijke voor de gegevensverwerking:

> *"Oracle Corporation en Oracle America, Inc., met hun geregistreerde adres op 500 Oracle Parkway, Redwood Shores, CA, 94065, Verenigde Staten, zijn verantwoordelijk voor de verwerking van uw persoonlijke gegevens binnen het kader van dit Privacybeleid."* [183]

238. In het AddThis Privacy Policy (dat alleen in het Engels beschikbaar is) staat als verantwoordelijke voor de gegevensverwerking vermeld:

> *"Oracle Corporation and its affiliated entities are responsible for processing AddThis Data described in this Privacy Policy. A list of Oracle entities is available here. Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country."* [184]

239. De lijst van Oracle entiteiten verwijst voor Nederland naar Oracle Nederland B.V. Nu AddThis onderdeel uitmaakt van haar DMP, geeft Oracle hiermee aan dat ook Oracle Nederland B.V.

---

[182] De privacy documentatie is gepubliceerd op: https://www.oracle.com/nl/legal/privacy/, geraadpleegd op 14 juli 2020
[183] Privacybeleid voor Oracle Data Cloud, onder "3. Wie is verantwoordelijk voor uw persoonsgegevens", zie https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 14 juli 2020 (tevens **Productie 22.a**).
[184] Privacybeleid voor AddThis, onder "3. Wie is verantwoordelijk voor uw persoonsgegevens", zie https://www.oracle.com/nl/legal/privacy/addthis-privacy-policy.html, geraadpleegd op 14 juli 2020.

een rol speelt bij het aanbieden van de DMP dienst. Het Algemeen privacybeleid van Oracle bevat overigens een vergelijkbare bepaling (in het Nederlands):

> *"Oracle Corporation en zijn gelieerde entiteiten zijn verantwoordelijk voor de verwerking van uw persoonlijke informatie zoals beschreven in dit Privacybeleid. Zie de lijst met Oracle-entiteiten. Selecteer een regio en land om het geregistreerde adres en de contactgegevens van de Oracle-entiteit of -entiteiten in elk land te bekijken."*[185]

240. Salesforce geeft in haar privacydocumentatie ook niet duidelijk aan hoe zij zelf haar rol kwalificeert. Zij lijkt zichzelf op de Engelstalige privacy pagina[186] van de Audience Studio Privacy Policy enkel als verwerker aan te merken. Dat volgt slechts uit de omstandigheid dat zij deze Privacy Policy heeft opgenomen onder de kop "Resources in respect of how we protect our customer's data as a processor" (onderstreping advocaat).[187]

241. In de Audience Studio Privacy Policy geeft Salesforce echter nergens aan of zij voor de verwerkingen de verwerkingsverantwoordelijke of de verwerker is. Bovendien wordt de Nederlandse internetgebruiker slechts naar een pagina geleid waar dit document niet vindbaar is (zie hiervoor randnummer 196).

242. In de volledige privacyverklaring op de Nederlandse website van Salesforce staat:

> *"1. Verantwoordelijke Salesforce-entiteit*
>
> *Salesforce is de verwerkingsverantwoordelijke van uw Persoonsgegevens zoals beschreven in deze Privacyverklaring, tenzij anders vermeld.*
>
> *Deze Privacyverklaring is niet van toepassing voor zover we Persoonsgegevens verwerken in de rol van verwerker of dienstverlener namens onze klanten, inclusief wanneer we onze klanten verschillende cloudproducten en -diensten aanbieden waarmee onze klanten (of hun gelieerde ondernemingen): (i) hun eigen websites en applicaties maken die op onze platforms draaien; (ii) hun eigen producten en diensten verkopen of aanbieden; (iii) elektronische communicatie naar anderen sturen; of (iv) anderszins Persoonsgegevens verzamelen, gebruiken, delen of verwerken via onze cloudproducten en -diensten.*
>
> *Voor uitgebreide privacy-informatie met betrekking tot een Salesforce-klant die of een gelieerde onderneming van een klant die de Salesforce cloudproducten en -diensten als verwerkingsverantwoordelijke gebruikt, neemt u rechtstreeks contact op met onze klant. Wij zijn niet verantwoordelijk voor de privacy- of gegevensbeveiligingspraktijken van onze klanten, die kunnen verschillen van die uitgelegd in deze Privacyverklaring. Zie ook Sectie 10.3 hieronder voor meer informatie."*

[185] Algemeen privacybeleid van Oracle, onder "3. Wie is verantwoordelijk voor uw persoonsgegevens", zie https://www.oracle.com/nl/legal/privacy/privacy-policy.html, geraadpleegd op 14 juli 2020.
[186] https://www.salesforce.com/eu/company/privacy/, geraadpleegd op 22 juli 2020.
[187] Het verdient opmerking dat de Nederlandse internetgebruiker niet naar deze Engelstalige privacy pagina wordt doorgeleid.

243. In de privacyverklaring wordt verder nergens vermeld dat Salesforce geen verwerkingsverantwoordelijke is voor de verwerkingen in verband met de DMP dienst, noch dat zij in dat kader slechts persoonsgegevens verwerkt in de rol van verwerker of als dienstverlener namens haar klanten. Daarmee wekt zij de indruk de verwerkingsverantwoordelijke te zijn. Die indruk wordt bovendien versterkt door de omstandigheid dat zij in diezelfde verklaring wel op enige punten refereert aan de DMP dienst (zie hiervoor randnummer 195).

244. Voorzover Oracle en Salesforce zich op het standpunt stellen dat zij ten aanzien van bepaalde aspecten van hun dienstverlening geen "verwerkingsverantwoordelijke" zijn, althans die suggestie wekken, willen Oracle en Salesforce daarmee betogen dat zij aan een groot aantal belangrijke verplichtingen uit de AVG niet hoeven te voldoen, onder meer het verkrijgen van toestemming voor de gegevensverwerking (artikel 7 AVG). , transparantieverplichtingen (artikel 12 AVG), dataminimalisatie (artikel 5 lid 1 sub c) en het nemen van passende technische en organisatorische maatregelen (artikel 24 AVG).

245. Voorzover het standpunt van Oracle en Salesforce is dat zij ten aanzien van (bepaalde van de) activiteiten die zij verrichten slechts als "verwerker" moeten worden aangemerkt, is dit onjuist. In het kader van de hierboven omschreven gegevensverwerking kwalificeren zij weldegelijk als "verwerkingsverantwoordelijke", zoals in het navolgende zal worden uiteengezet.

*4.4.1 De "verwerkingsverantwoordelijke"*

246. Artikel 4 lid 7 AVG definieert de verwerkingsverantwoordelijke als volgt.

> *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; […];"*

247. De verwerkingsverantwoordelijke speelt een fundamentele rol in het kader van de AVG en daarom is het van groot belang hem aan te wijzen. De verwerkingsverantwoordelijke heeft onder meer de verantwoordingsplicht om aan te tonen dat hij voldoet aan de beginselen inzake verwerking van persoonsgegevens (artikel 5 lid 2 AVG).

248. De verwerkingsverantwoordelijke moet worden onderscheiden van de "verwerker", die slechts ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 lid 8 AVG). De verwerker mag slechts persoonsgegevens verwerken op basis van schriftelijke instructies van de verwerkingsverantwoordelijke. De verwerking door een verwerker moet in een specifieke overeenkomst worden geregeld (artikel 28 lid 3 AVG).

249. De verwerkingsverantwoordelijke is, kort gezegd, degene die beslist *waarom* en *hoe* persoonsgegevens worden verwerkt. [188]

250. Artikel 4 lid 7 AVG maakt een onderscheid tussen het vaststellen van het "doel van" en de "middelen voor" de verwerking.

[188] Artikel 29 werkgroep, Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP169, p. 15. ('WP169 De begrippen "voor de verwerking verantwoordelijke" en "verwerker"'),

251. Het vaststellen van het doel is relevant vanwege het feit dat verwerkingen slechts rechtmatig zijn wanneer deze voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder mogen worden verwerkt op een wijze die met deze doeleinden onverenigbaar is (artikel 5 lid 1 sub b AVG). Dit betekent echter niet dat degene die de doelen vaststelt in de zin van artikel 4 lid 7 AVG ook steeds rechtmatige doelen vaststelt. Het gaat blijkens artikel 4 lid 7 AVG om degene die doel en middelen "vaststelt" en niet "rechtmatig vaststelt".

252. Ten aanzien van de vraag wie degene is die "vaststelt" geeft de European Data Protection Supervisor ("EDPS") het volgende aan:

> *"How can this be assessed in practice? In order to evaluate the 'factual influence' of a controller over the processing operation, the entirety of the factual elements should be evaluated, by answering the questions 'why is the processing taking place', 'who initiated the processing' and 'who benefits from the processing'."*[189]

253. Van belang is dus niet alleen waarom de verwerking plaatsvindt en wie het initiatief nam, maar ook wie voordeel geniet van de verwerking.

254. Het begrip "middelen" in artikel 4 lid 7 AVG heeft niet alleen betrekking op de technische en organisatorische manier waarop persoonsgegevens worden verwerkt. Het begrip heeft ook betrekking op de wijze waarop de verwerking geschiedt (het "hoe" van de verwerking). In dat verband is onder meer relevant om te bepalen wie degene is die bepaalt welke persoonsgegevens worden verwerkt, wie bepaalt welke derden toegang krijgen tot de persoonsgegevens, wanneer de persoonsgegevens worden gewist.[190]

255. Uit overweging 74 AVG volgt dat de verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgesteld voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd:

> *"De verantwoordelijkheid en aansprakelijkheid van de verwerkingsverantwoordelijke moeten worden vastgesteld voor elke verwerking van persoonsgegevens die door of namens hem wordt uitgevoerd. Meer bepaald dient de verwerkingsverantwoordelijke te worden verplicht passende en effectieve maatregelen uit te voeren en te kunnen aantonen dat elke verwerkingsactiviteit overeenkomstig deze verordening geschiedt, ook wat betreft de doeltreffendheid van de maatregelen. Bij die maatregelen moet rekening worden gehouden met de aard, de omvang, de context en het doel van de verwerking en het risico voor de rechten en vrijheden van natuurlijke personen."*

256. De WG29 geeft in zijn advies 1/2010 aan dat de verantwoordelijkheid blijkt uit de *feitelijke* invloed die de actoren hebben op de vaststelling van het doel en de middelen voor de

[189] European Data Protection Supervisor ("EDPS"), 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725', p. 7 (NB: deze guidelines zien weliswaar niet direct op de AVG maar op aanverwante wetgeving waarin de begrippen "verwerkingsverantwoordelijke en verwerker een zelfde betekenis hebben.).
[190] Ibidem, p. 16.

verwerking van de persoonsgegevens.[191] Het begrip verwerkingsverantwoordelijke is een "functioneel begrip".

257. De contractuele taakverdeling is slechts een aanwijzing ten aanzien van de werkelijke rol die partijen vervullen.[192]

*4.4.2 Ruime uitleg*

258. Uit de jurisprudentie van het HvJEU volgt dat het begrip "verwerkingsverantwoordelijke" ruim moet worden uitgelegd, mede gelet op de doelstelling van de AVG om een hoog niveau van gegevensbescherming te waarborgen. [193] De EDPS bevestigt dat die ruime uitleg van het HvJEU ook ten doel heeft te voorkomen dat er een gebrek aan verantwoordelijkheid bestaat en zodoende te waarborgen dat betrokkenen de garantie hebben van effectieve en volledige bescherming.[194]

259. In de zaak *Wirtschaftsakademie* bepaalde het HvJEU dat degene die een "fanpagina" aanmaakt op Facebook aangemerkt moet worden als (gezamenlijk) verwerkingsverantwoordelijke. In deze zaak was het Facebook die een cookie plaatste op de computer van degene die de fanpagina bezocht. Facebook verzamelde daarmee gegevens ten behoeve van haar advertentiesysteem van "behavioural targeting".[195] De beheerder van de fanpagina verkreeg geanonimiseerde statistieken over het websitebezoek van Facebook. Hieruit kon worden opgemaakt wat de kenmerken en het profiel zijn van de websitebezoekers, bijvoorbeeld ten aanzien van leeftijd, geslacht, interesses en online aankoopgedrag.[196]

260. De houder van de fanpagina werd aangemerkt als (gezamenlijk) verwerkingsverantwoordelijke, omdat hij Facebook onder meer in staat stelde om cookies te plaatsen en omdat hij dankzij de statistieken zijn informatieaanbod beter kon bepalen. Dat hij zelf geen beschikking kreeg over persoonsgegevens deed daar niet aan af, aldus het HvJEU (r.o. 42).

261. In de zaak *Jehovan todistajat* overwoog het HvJEU dat de gemeenschap van Jehova's getuigen gezamenlijk met de individuele Jehova's getuigen (leden) verwerkingsverantwoordelijke was omdat de gemeenschap de geloofsverkondigingsactiviteiten organiseert, coördineert en aanmoedigt. Het HvJEU acht het voor deze vaststelling van gezamenlijke verantwoordelijkheid niet nodig dat de gemeenschap toegang heeft tot de gegevens of dat zij haar leden schriftelijk instrueert.[197]

---

[191] WP169 De begrippen "voor de verwerking verantwoordelijke" en "verwerker", p. 9.
[192] Conclusie AG Bot van 24 oktober 2017 in zaak C-210/16, ECLI:EU:C:2017:796 (*Wirtschaftsakademie Schleswig-Holstein*), par. 60.
[193] HvJEU 29 juli 2019, C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 66; HvJEU 10 juli 2018, zaak C 25/17, (*Jehovan todistajat*), r.o. 66; HvJEU 5 juni 2018, C 210/16 (*Wirtschaftsakademie Schleswig-Holstein*), r.o. 28; HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain en Google*).
[194] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13. Zie ook HvJEU 5 juni 2018, zaak C 210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), r.o. 42.
[195] Conclusie AG Bot van 24 oktober 2017 in zaak C-210/16, ECLI:EU:C:2017:796 (*Wirtschaftsakademie Schleswig-Holstein*), par 4.
[196] HvJEU 5 juni 2018, zaak C 210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), r.o. 34 en 37.
[197] HvJEU 10 juli 2018, zaak C 25/17, (*Jehovan todistajat*), r.o. 75.

262. In de zaak *Fashion ID* bepaalde het HvJEU dat degene die een Facebook "Like" of "vind ik leuk"-knop op zijn website activeert, aangemerkt moet worden als (gezamenlijk) verwerkingsverantwoordelijke. Deze knop wordt geïnstalleerd door een hyperlink naar Facebook te maken. Bij een bezoek aan de website die de knop bevat, wordt automatisch verbinding gemaakt met de servers van Facebook en worden daaraan persoonsgegeven van de websitebezoeker gestuurd, ongeacht of hij of zij op de knop heeft geklikt en ongeacht of hij of zij een Facebook-account heeft.[198]

263. Degene die de "Like"-knop op zijn website activeerde, werd door het HvJEU aangemerkt als een verwerkingsverantwoordelijke omdat hij hiermee Facebook in staat stelde persoonsgegevens te verzamelen en daarvan op de hoogte was.[199] Door de "Like"-knop te installeren, stelde de websitehouder samen met Facebook de middelen vast voor de verwerking van persoonsgegevens. In het geval de knop niet zou zijn geïnstalleerd door de websitehouder zouden de persoonsgegevens immers niet zijn verwerkt.[200] Ook de doelen werden gezamenlijk vastgesteld, aldus het HvJEU, nu de websitehouder dankzij de "Like"-knop commercieel voordeel geniet door de reclame voor haar producten te optimaliseren door de zichtbaarheid op Facebook te vergoten.

264. In de hierboven besproken jurisprudentie stelde de betrokken partijen zich steeds op het standpunt slechts verwerker te zijn. Volgens het HvJEU ten onrechte. In twee van de drie zaken wordt geoordeeld dat de betrokken partij gezamenlijk verwerkingsverantwoordelijke is met Facebook. De rol die Facebook in deze zaken speelt lijkt in veel opzichten op die van Oracle en Salesforce. Niettemin waren partijen het erover eens dat Facebook primair het doel en de middelen van de gegevensverwerking vaststelde.

*4.4.3 Oracle en Salesforce zijn verwerkingsverantwoordelijke*

265. In de onderhavige zaak zijn het ook Oracle en Salesforce die primair aangemerkt moeten worden als verwerkingsverantwoordelijke.

266. Uit het feitelijk kader volgt dat Oracle en Salesforce op uiteenlopende manieren persoonsgegevens verwerken (zie paragraaf 3.2). In de eerste plaats geldt dat zij cookies plaatsen op de randapparatuur van de consument. In de tweede plaats wordt een rechtstreekse koppeling gemaakt tussen de aldus geplaatste cookies en het DMP van Oracle en Salesforce. Via deze koppeling verzamelen Oracle en Salesforce onder meer de unieke Cookie IDs, IP-adressen, gegevens over online aankopen en gegevens over de browser. Oracle en Salesforce creëren aan de hand van verschillende identificatoren een "ID Graph" of digitale vingerafdruk om diverse unieke identificatoren aan elkaar te koppelen. Deze informatie wordt vervolgens, ten derde, verrijkt met informatie die verkregen is uit andere bronnen. Aan de hand hiervan worden ten vierde profielen opgesteld. In de vijfde plaats stellen Oracle en Salesforce deze profielen ter beschikking aan adverteerders die in het RTB-proces meedingen om advertentieruimte op websites die consumenten bezoeken te kopen. In het kader van RTB

[198] HvJEU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 26 en 27.
[199] HvJEU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 75.
[200] HvJEU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 78-79.

wordt, ten slotte, door middel van cookie syncing koppelingen gemaakt met cookies van derden. Deze handelingen verrichten zij geautomatiseerd door middel van software.

267. Het zijn Oracle en Salesforce die zelfstandig hebben besloten op deze wijze persoonsgegevens te verwerken. Het zijn ook Oracle en Salesforce die het resultaat en de gevolgen van de gegevensverwerking hebben bepaald. Oracle en Salesforce bepalen welke persoonsgegevens worden verzameld, over welke betrokkenen, hoe lang de gegevens bewaard blijven, wie toegang heeft tot de persoonsgegevens en hoe de gegevensverwerking wordt beveiligd.

268. Het zijn Oracle en Salesforce die het cruciale middel verstrekken om persoonsgegevens te verzamelen en consumenten te identificeren, namelijk de cookies en de DMP. Het zijn Oracle en Salesforce die gebruikers kunnen herkennen op alle websites die van hun technieken gebruiken maken. Oracle en Salesforce volgen of tracken de gebruiker over het internet, onder meer aan de hand van het Cookie ID dat zij aan hun cookies meegeven. Het zijn Oracle en Salesforce die de koppeling maken tussen gegevens die zijn verzameld via de laptop, tablet, mobiel, werkcomputer en zelfs over het offline leven van de internetgebruiker. Het zijn Oracle en Salesforce die op grote schaal Cookie IDs uitwisselen met andere partijen die actief zijn in het RTB-proces, zodat al deze partijen te allen tijde elkaars internetgebruikers kunnen herkennen en gegevens kunnen uitwisselen. Zonder het aanbieden van de DMP zou alle verzamelde informatie niet aan elkaar gekoppeld, verrijkt, geanalyseerd en gedeeld kunnen worden. Oracle en Salesforce doen dit voor hun eigen commerciële belang, namelijk om de gegevens die zij verkrijgen te verrijken en commercieel te exploiteren door ze beschikbaar te maken voor derden. Oracle en Salesforce hebben van dit alles vanzelfsprekend wetenschap.

269. Bovendien volgt uit het feitelijk kader dat Oracle en Salesforce haar klanten en/of partners een groot aantal middelen aanbiedt waarmee zij het “hoe” van de gegevensverwerkingen bepalen (zie randnummer 64). Het gaat onder meer om een softwareplatform dat voortdurend ontwikkeld en onderhouden wordt ten behoeve van het verzamelen, bewaren en verrijken van gegevens en het ontwikkelen en onderhouden van algoritmes om één betrokkene te identificeren en zijn activiteiten te volgen over meerdere apparaten. Het zijn Oracle en Salesforce die algoritmes ontwikkelen met als doel om van de verschillende gegevenssets profielen en interessesegmenten te maken. Het zijn Oracle en Salesforce die zoekinstrumenten ontwikkelen waarmee de klanten van Oracle en Salesforce specifieke doelgroepen of interessesegmenten kunnen vinden.

270. Het is voor een adverteerder of websitehouder kinderlijk eenvoudig de diensten van Oracle en Salesforce te integreren. Een websitehouder kan met slechts enkele klikken op de knop of het toevoegen van een paar regels aan de code van de website ervoor zorgdragen dat via zijn websites cookies worden geplaatst. De DMP doet vervolgens de rest zoals het plaatsen van de cookies, het uitlezen van de cookies en het verzamelen van data. Klanten krijgen toegang tot een overzichtelijk DMP-dashboard waarmee ze hun eigen gegevens en die van derde partijen kunnen koppelen. Daarnaast laten ze weten aan welke doelgroepen ze de voorkeur geven aan wie ze op basis van persoonlijke informatie advertenties willen tonen.

271. Uit het bovenstaande volgt dat Oracle en Salesforce de doelen en middelen van de gegevensverwerkingen vaststellen.

272. Zoals gezegd, stelt Oracle zich in haar brief van 18 juni 2020 echter op het standpunt dat zij als een "verwerker" moet worden beschouwd ten aanzien van haar DMP dienst (**Productie 5**). Met andere woorden, Oracle stelt zich op het standpunt dat zij niet het "waarom" en het "hoe" van gegevensverwerkingen bepaalt. Dat is voor een partij die zichzelf omschrijft als "enabler" van online marketing een opmerkelijk standpunt. Volgens Oracle zijn het haar klanten en/of partners die kwalificeren als verwerkingsverantwoordelijken. Uit het voorgaande blijkt dat dit niet juist is. Het is Oracle die het initiatief neemt tot de gegevensverwerking, de middelen ertoe vaststelt, het grootste commerciële belang erbij heeft.

273. Oracle plaatst de cookies op de apparatuur van eindgebruikers en leest deze uit. Zij stelt dat slechts sprake is van "first-party" cookies die door de Publisher zelf zouden worden geplaatst maar uit onderzoek blijkt dat Oracle zelf de cookies plaatst vanuit haar eigen domein (**Productie 16**). Zelfs als dat niet het geval zou zijn, dan geldt nog steeds dat het Oracle is die de software of code voor de cookies aanlevert. Ook is het Oracle die de cookies zodanig heeft ingericht dat de verzamelde gegevens automatisch worden opgenomen in de DMP database. Bovendien is het Oracle die ervoor kiest om cookie syncing toe te passen. Het is ook Oracle die de middelen bepaalt om (de toegang tot) persoonsgegevens te beveiligen.

274. Salesforce erkent in haar Audience Studio Privacy Policy dat zij voor haar DMP gegevens verzamelt over onder meer websitebezoek van consumenten, welke zoekmachines zij gebruiken, de zoektermen die zij gebruiken, demografische informatie en IP-adressen.[201] Salesforce geeft echter aan dat het haar klanten zijn, adverteerders, die bepalen of deze data wordt verzameld. Daarmee gaat Salesforce er aan voorbij dat zij voor haar klanten de middelen vaststelt om dit te doen.

275. Salesforce geeft zelfs aan dat haar klanten die gebruik maken van Salesforce' data partners, zelf verantwoordelijk zijn voor het gebruik van die gegevens:

> *"● Customers are solely responsible for any content their users or consumers provide to any Third-Party Platform.*
>
> *● Customers are solely responsible for any information accessed by their users, consumers or any third party from any Third-Party Platform."*[202]

276. Gebruik maken van die gegevens is voor de klanten van Salesforce niet meer dan een druk op de knop (zie randnummers 102 e.v.). De gegevens zijn dan echter al beschikbaar gesteld middels het platform van Salesforce. Dit beschikbaar maken van die gegevens via haar platform valt dan ook binnen de verantwoordelijkheid van Salesforce. Opvallend is ook dat Oracle zichzelf voor diezelfde dienst (bij Oracle aangemerkt als ADM) wel aanmerkt als verwerkingsverantwoordelijke.

277. Bovendien geeft Salesforce aan dat zij zelfstandig bepaalt of verschillende apparaten van dezelfde gebruiker zijn en deze informatie opslaat.[203] Salesforce erkent ook dat de gegevens opgeslagen in haar DMP worden verrijkt met bijvoorbeeld geolocatie data verstrekt door

[201] Salesforce Audience Studio Privacy Policy (**Productie 23.d**).
[202] Audience Studio Notice and License Information (**Productie 23.f**), onder "Third Party Platforms".
[203] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', geraadpleegd op 22 juli 2020 (tevens **Productie 23.d**).

derden "*in order to better target advertisements, to enable Customers to better understand users across multiple computers and devices, and for ad delivery and reporting purposes*".[204] Uit het voorgaande volgt dat Salesforce verwerkingsverantwoordelijke is voor de DMP dienst.

278. Dat het standpunt dat Oracle en Salesforce geen verwerkingsverantwoordelijke zouden zijn onhoudbaar is, blijkt ook uit het feit dat zij niet louter de instructies van derden volgen ten aanzien van de gegevensverwerking. Het zijn ook Oracle en Salesforce die bepalen op welke grondslag de gegevens worden verwerkt (namelijk op basis van toestemming). Oracle geeft betrokkenen zelfs de mogelijkheid om toestemming in te trekken. Het zijn ook Oracle en Salesforce die bewaartermijnen bepalen en aan wie een verzoek tot inzage conform artikel 15 AVG kan worden gericht.

279. Voor zover in een verwerkersovereenkomst anders zou zijn bepaald, geldt dat niet de juridische afspraken maar de feitelijke gedragingen doorslaggevend zijn om de verwerkingsverantwoordelijke te bepalen. Overigens maakt de contractuele documentatie van partijen ook niet duidelijk of Oracle (**Productie 24**) en Salesforce (**Productie 25**) zichzelf in het kader van hun DMP dienst als verwerker of verwerkingsverantwoordelijke zien.

280. Uit de hierboven besproken jurisprudentie volgt dat meerdere partijen gezamenlijk verwerkingsverantwoordelijke kunnen zijn.[205] Dit volgt ook uit artikel 4 lid 7 AVG. Van belang is in dit kader of er meerdere partijen zijn die invloed uitoefenen op het bepalen van het doel en de middelen van de verwerking, en tevens of er meerdere partijen zijn die commercieel belang hebben bij de verwerking.[206]

281. Artikel 26 AVG bepaalt dat wanneer meerdere partijen gezamenlijk verwerkingsverantwoordelijke zijn, zij onderling op transparante wijze hun verantwoordelijkheden op grond van de AVG vaststellen. In het bijzonder die ten aanzien van de informatieverplichtingen op grond van artikelen 13 en 14 AVG.

282. Artikel 26 AVG luidt als volgt:

> *"1. Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, zijn zij gezamenlijke verwerkingsverantwoordelijken. Zij stellen op transparante wijze hun respectieve verantwoordelijkheden voor de nakoming van de verplichtingen uit hoofde van deze verordening vast, met name met betrekking tot de uitoefening van de rechten van de betrokkene en hun respectieve verplichtingen om de in de artikelen 13 en 14 bedoelde informatie te verstrekken, door middel van een onderlinge regeling, tenzij en voor zover de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijken zijn vastgesteld bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijken van toepassing is. In de regeling kan een contactpunt voor betrokkenen worden aangewezen.*

[204] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', geraadpleegd op 22 juli 2020 (tevens **Productie 23.d**).
[205] Zie ook HvJEU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 66; HvJEU 10 juli 2018, C 25/17, ECLI:EU:C:2018:551 (*Jehovan todistajat*), r.o. 66.
[206] Vgl. HvJEU 29 juli 2019, zaak C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 80.

*(...)"*

283. In de onderhavige procedure zijn verschillende entiteiten uit de concerns van Oracle en Salesforce gedagvaard. In het geval van concernverhoudingen, zoals hier aan de orde, wordt de rechtspersoon onder wiens bevoegdheid de operationele gegevensverwerking plaatsvindt in beginsel als de verwerkingsverantwoordelijke beschouwd. Dat laat onverlet dat gezamenlijk met andere entiteiten binnen het concern het doel van en de middelen voor de gegevensverwerking worden vastgesteld. Zoals in verderop in paragraaf 4.5 uiteengezet, zijn alle gedagvaarde partijen betrokken bij de verwerking in het kader van de DMPs van Oracle en Salesforce. De verschillende entiteiten zijn daarmee als gezamenlijke verwerkingsverantwoordelijke in de zin van artikel 26 lid 1 AVG aan te merken. Elk van de verwerkingsverantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerking en de naleving van de daarmee samenhangende verplichtingen (artikel 26 lid 3 en 82 lid 2 AVG).

284. Voor zover Oracle en Salesforce niet aangemerkt moeten worden als de primaire, zelfstandige verwerkingsverantwoordelijken, dan geldt dat zij in ieder geval gezamenlijk verwerkingsverantwoordelijken zijn met hun klanten en/of andere partijen in het RTB ecosysteem. In dat geval geldt het navolgende:

a. Oracle en Salesforce zijn de gezamenlijke verwerkingsverantwoordelijke met de Publishers voor zover het gaat om het verzamelen van persoonsgegevens via cookies op de websites van Publishers en voor het delen van persoonsgegevens voor zover dat direct verband houdt met het aanbieden van advertentieruimte op de websites van Publishers (al dan niet met gebruikmaking van een SSP);

b. Oracle en Salesforce zijn de gezamenlijke verwerkingsverantwoordelijke met Advertisers voor het delen van gegevens uit de DMP met Advertisers (al dan niet met gebruikmaking van een DSP);

c. Oracle en Salesforce zijn de gezamenlijke verwerkingsverantwoordelijke voor de uitwisseling van gegevens via cookie syncing met alle partijen met wie zij op deze wijze gegevens uitwisselen.

285. Voorzover Oracle en Salesforce zich echter op het standpunt zouden stellen dat zij slechts "verwerker" zijn, is dat standpunt, gelet op het bovenstaande, onhoudbaar. Het zou ook in strijd zijn met het uitgangspunt dat er geen gebrek aan verantwoordelijkheid dient te bestaan teneinde te garanderen dat betrokkenen gewaarborgd zijn van effectieve en volledige bescherming.[207]

## 4.5 Territoriale toepasselijkheid

### *4.5.1 Territoriale toepasselijkheid AVG*

286. Artikel 3 AVG regelt het territoriale toepassingsbereik van de AVG:

[207] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13. Zie ook HvJEU 5 juni 2018, zaak C 210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie Schleswig-Holstein*), r.o. 42.

*"Artikel 3*

*Territoriaal toepassingsgebied*

*1. Deze verordening is van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.*

*2. Deze verordening is van toepassing op de verwerking van persoonsgegevens van betrokkenen die zich in de Unie bevinden, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, wanneer de verwerking verband houdt met:*

*a) het aanbieden van goederen of diensten aan deze betrokkenen in de Unie, ongeacht of een betaling door de betrokkenen is vereist; of*

*b) het monitoren van hun gedrag, voor zover dit gedrag in de Unie plaatsvindt.*

*[...]"*

287. Op grond van artikel 3 lid 1 AVG is de AVG van toepassing op verwerkingen in het kader van activiteiten van een vestiging van een verantwoordelijke in de Europese Unie ("**EU**").

288. Overweging 22 licht dit als volgt toe:

> *"De verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie dient overeenkomstig deze verordening te worden verricht, ongeacht of de eigenlijke verwerking in de Unie plaatsvindt. Vestiging veronderstelt het effectief en daadwerkelijk uitoefenen van activiteiten via bestendige verhoudingen. De rechtsvorm van dergelijke verhoudingen, of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid, is daarbij niet doorslaggevend."*

289. Overweging 19 bij de Privacyrichtlijn bevatte een vergelijkbare tekst die door het HvJEU verschillende keren is aangehaald in jurisprudentie over het toepassingsbereik van die richtlijn.[208] Uit die jurisprudentie valt af te leiden dat:

a. een "vestiging" "*iedere vorm van, zelfs geringe, reële en daadwerkelijke activiteit die via een duurzame vestiging wordt uitgeoefend*" is;[209]

[208] HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), HvJEU 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), HvJEU 28 juli 2016, C-191/15 ECLI:EU:C:2016:612 (*Amazon*) en HvJEU 5 juni 2018, C-210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie*); zie tevens EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)', version 2.1 ('EDPB Guidelines 3/20 Territorial Scope'), p. 6.

[209] HvJEU 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), r.o. 31.

b. van een "*duurzame vestiging*" of "*bestendige verhoudingen*"[210] reeds sprake kan zijn als er één medewerker in een land in de EU aanwezig is;[211]

c. de zinsnede "*in het kader van de activiteiten van een vestiging*" ruim moet worden uitgelegd.[212]

290. Wanneer een voornamelijk buiten de EU gevestigde onderneming over een of meer vestigingen beschikt in de EU en de activiteiten "*onlosmakelijk met elkaar verbonden*" zijn, worden de verwerkingen geacht plaats te vinden in het kader van de activiteiten van die vestiging(en) in de EU.[213] Van een dergelijke verbondenheid is snel sprake, bijvoorbeeld als een Europese vestiging zich bezighoudt met het verkopen van advertentieruimte die het aanbieden van een gratis zoekmachine of sociaal media platform mogelijk maakt.[214]

291. Echter, zelfs als een verantwoordelijke niet via een vestiging in de EU onder het toepassingsbereik van de AVG valt, geldt dat de AVG op grond van artikel 3 lid 2 AVG van toepassing is indien het gaat om verwerkingen van betrokkenen in de EU in verband met het aanbieden van goederen of diensten of monitoring.

292. In het geval van monitoring is de AVG uitsluitend van toepassing wanneer het gaat om het monitoren van gedrag van een betrokkene die zich in de EU bevindt, terwijl dat gedrag tevens in de EU plaatsvindt.[215]

293. Overweging 24 licht dit als volgt toe:

> *"De verwerking van persoonsgegevens van betrokkenen in de Unie door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker moet ook onder deze verordening vallen wanneer dat verband houdt met het controleren van het gedrag van de betrokkenen voor zover zich dat binnen de Unie situeert. Om uit te maken of een verwerking kan worden beschouwd als controle van het gedrag van betrokkenen, dient te worden vastgesteld of natuurlijke personen op het internet worden gevolgd, en onder meer of in dat verband eventueel persoonsgegevensverwerkingstechnieken worden gebruikt waarbij een profiel wordt opgesteld van een natuurlijke persoon, in het bijzonder om besluiten ten aanzien van hem te nemen of om zijn persoonlijke voorkeuren, gedragingen en attitudes te analyseren of te voorspellen."*

294. Hieruit volgt duidelijk dat de bepaling in ieder geval van toepassing is bij het volgen van het gedrag van personen op internet. De EDPB acht daarbij bovendien relevant voor welke doeleinden de verzamelde gegevens gebruikt worden en of profielen worden opgesteld en gedragsanalyse plaatsvindt. De EDPB noemt onder meer "behavioural advertising" en "online

[210] Overweging 19 Privacyrichtlijn spreekt van "duurzame vestiging" overweging 22 AVG van "bestendige verhoudingen, terwijl beiden in de Engelse taalversies over "stable arrangements" spreken. Het gaat hier dus feitelijk om hetzelfde begrip.
[211] HvJEU 1 oktober 2015, C-230/14, ECLI:EU:C:2015:639 (*Weltimmo*), r.o. 30.
[212] HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), r.o. 53.
[213] HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), r.o. 56 en EDPB Guidelines 3/20 Territorial Scope , p. 8-9.
[214] HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain*), r.o. 56 en 57 r.o. en HvJEU 5 juni 2018, C-210/16, ECLI:EU:C:2018:388 (*Wirtschaftsakademie*), r.o. 58-60.
[215] EDPB Guidelines 3/20 Territorial Scope, p. 19.

tracking" door middel van cookies als voorbeelden van monitoring activiteiten die onder artikel 3 lid 2 sub b AVG vallen. [216]

295. Uit artikel 3 lid 1 en artikel 3 lid 2 sub b AVG volgt dat de AVG van toepassing is op de verwerking van persoonsgegevens van Oracle en Salesforce.

296. De Oracle DMP dienst wordt primair aangeboden door het hoofdkantoor van het Oracle concern: Oracle Corporation in de Verenigde Staten. Oracle Corporation lijkt ook de eigenaar te zijn van de domeinnaam die gebruikt wordt voor het plaatsen van de bku cookies (bluekai.com).[217]

297. De rol van Oracle Corporation in verband met de DMP dienst wordt bevestigd in het Privacybeleid voor Oracle Data Cloud. Daaruit kan voorts worden opgemaakt dat ook Oracle America, Inc. een belangrijke rol speelt. Oracle merkt namelijk Oracle Corporation en Oracle America, Inc. aan als verantwoordelijke voor de gegevensverwerking:

> *"Oracle Corporation en Oracle America, Inc., met hun geregistreerde adres op 500 Oracle Parkway, Redwood Shores, CA, 94065, Verenigde Staten, zijn verantwoordelijk voor de verwerking van uw persoonlijke gegevens binnen het kader van dit Privacybeleid."*

298. Oracle geeft voorts aan dat zij activiteiten heeft in meer dan 80 landen en dat de gegevens wereldwijd worden verwerkt.[218] In het AddThis Privacy Policy (dat alleen in het Engels beschikbaar is) staat als verantwoordelijke voor de gegevensverwerking vermeld:

> *"Oracle Corporation and its affiliated entities are responsible for processing AddThis Data described in this Privacy Policy. A list of Oracle entities is available here. Please select a region and country to view the registered address and contact details of the Oracle entity or entities located in each country."*

299. De lijst van Oracle entiteiten verwijst voor Nederland naar Oracle Nederland B.V. Nu AddThis onderdeel uitmaakt van haar DMP, geeft Oracle hiermee aan dat ook Oracle Nederland B.V. een rol speelt bij het aanbieden van de DMP dienst. Het Algemeen privacybeleid van Oracle bevat overigens een vergelijkbare bepaling (in het Nederlands):

> *"Oracle Corporation en zijn gelieerde entiteiten zijn verantwoordelijk voor de verwerking van uw persoonlijke informatie zoals beschreven in dit Privacybeleid. Zie de lijst met Oracle-entiteiten. Selecteer een regio en land om het geregistreerde adres en de contactgegevens van de Oracle-entiteit of -entiteiten in elk land te bekijken."*

300. Uit het uittreksel van de KvK (**Productie 26**) blijkt dat Oracle Nederland B.V. 1801 werkzame personen heeft en actief is in onder meer het "ontwikkelen, produceren en uitgeven van software", en "overige dienstverlenende activiteiten op het gebied van informatietechnologie". Oracle Nederland B.V. is onder meer betrokken bij de verkoop en levering van de producten

[216] EDPB Guidelines 3/20 Territorial Scope, p. 20.
[217] https://who.is/whois/bluekai.com, geraadpleegd op 22 juli 2020.
[218] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder 9, geraadpleegd op 23 april 2020 (tevens **Productie 22.a**).

van het Oracle concern in Nederland, waaronder het DMP. Dat volgt onder meer uit het feit dat de 'Director Oracle Cloud Strategy – Northern Europe' in Nederland gevestigd is.

301. De Salesforce DMP dienst lijkt primair te worden aangeboden door het hoofdkantoor van het Salesforce concern: Salesforce.com, Inc. in de Verenigde Staten. Salesforce.com, Inc. is ook de eigenaar van de domeinnaam die gebruikt wordt voor het plaatsen van cookies (krxd.net).[219] Ook Salesforce biedt de DMP dienst wereldwijd aan, waaronder aan klanten in Nederland.

302. In de volledige privacyverklaring worden Salesforce.com, Inc. en "de desbetreffende gelieerde ondernemingen" aangemerkt als verantwoordelijke "tenzij anders vermeld."[220] In de lijst van gelieerde ondernemingen staat onder meer "SFDC Netherlands B.V."[221] Salesforce maakt hierbij niet duidelijk welke entiteit verantwoordelijk is voor welke verwerkingen.

303. Uit het uittreksel van de KvK (**Productie 27**) blijkt dat SFDC Netherlands B.V. 191 werkzame personen heeft in Nederland en activiteiten heeft op het gebied van "Het verlenen van diensten op het gebied van software applicaties teneinde organisaties te ondersteunen bij het beheer van relatiegegevens en documenten." SFDC Netherlands B.V. is onder meer betrokken bij de verkoop en levering van de producten van het Salesforce concern in Nederland, waaronder het DMP. Dat volgt onder meer uit het feit dat de 'Senior Regional Vice President, Marketing Cloud' in Nederland gevestigd is.

304. Oracle Nederland B.V. en SFDC Netherlands B.V. zijn ondernemingen in Nederland. Alle verwerkingen in het kader van hun activiteiten vallen binnen het bereik van de AVG. Daaronder vallen ook de verwerkingen in het kader van de DMP dienst, bestaande uit het verzamelen, combineren, verrijken, evalueren en verkopen van de persoonsgegevens van Nederlandse internetgebruikers. De AVG is derhalve op deze verwerkingen door Oracle Nederland B.V. en SFDC Netherlands B.V. van toepassing.

305. De ondernemingen zijn bovendien in het kader van voornoemde jurisprudentie te beschouwen als "vestiging" van de internationale ondernemingen Oracle en respectievelijk Salesforce. Oracle Nederland B.V. en SFDC Netherlands B.V. zijn duurzame vestigingen c.q. bestendige verhoudingen. De entiteiten zijn betrokken bij onder andere de verkoop van de DMP dienst aan publishers en adverteerders in Nederland. Die activiteiten zijn onlosmakelijk verbonden met verwerkingsactiviteiten waarvoor Oracle Corporation, Oracle America Inc. en respectievelijk Salesforce.com Inc. (mede) verantwoordelijk zijn. In de zin van artikel 3 lid 1 AVG kunnen Oracle Nederland B.V. en SFDC Netherlands B.V. derhalve worden beschouwd als vestiging van die buitenlandse entiteiten. De verwerkingsactiviteiten vinden (mede) plaats in het kader van een vestiging van de verantwoordelijken in de EU. Derhalve is de AVG ook van toepassing op de verwerkingen waarvoor Oracle Corporation, Oracle America Inc. en respectievelijk Salesforce.com Inc. (mede) verantwoordelijk zijn.

306. Voor zover de verwerkingsactiviteiten van Oracle Corporation, Oracle America Inc. en Salesforce.com Inc, niet geacht kunnen worden plaats te vinden in het kader van de activiteiten van een vestiging in de EU, geldt dat de AVG alsnog van toepassing is op grond van artikel 3

[219] Who.is, *krxd.net,* te raadplegen via: https://who.is/whois/krxd.net.
[220] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder "1. Verantwoordelijke Salesforce-entiteit" en in de alinea net daarvoor, geraadpleegd op 24 juli 2020.
[221] https://www.salesforce.com/nl/company/locations/, geraadpleegd op 22 juli 2020.

lid 2 sub b AVG. Het gaat immers om een verwerking van de persoonsgegevens van in de EU gevestigde betrokkenen die verband houdt met het monitoren van het gedrag van betrokkenen in de EU.

307. Oracle en Salesforce verzamelen persoonsgegevens door middel van cookies die onder meer geplaatst worden op een groot aantal populaire Nederlandse websites, althans websites die veel door Nederlanders bezocht worden (**Productie 16**). Daarmee volgen Oracle en Salesforce het online gedrag van vrijwel alle Nederlandse internetgebruikers. Zij zijn gevestigd in Nederland en het gedrag dat gevolgd wordt vindt doorgaans plaats in Nederland, en dus in de EU. Oracle en Salesforce gebruiken de gegevens om profielen te maken en gedrag te analyseren en beïnvloeden. Er is sprake van online tracking door middel van cookies en behavioural advertising.[222] Er is sprake van cookie syncing ten behoeve van RTB. De verwerkingsactiviteiten van Oracle en Salesforce vallen daarmee bij uitstek onder artikel 3 lid 2 sub b AVG. Oracle Corporation, Oracle America Inc. en respectievelijk Salesforce.com Inc. zijn de partijen die uiteindelijk (binnen het Oracle en Saleforce concern) verantwoordelijk zijn voor het aanbieden van de DMP diensten waar dan ook ter wereld en dus ook voor de monitoring die dat in de EU met zich meebrengt.

*4.5.2 Territoriale toepasselijkheid artikel 11.7a Tw*

308. Artikel 11.7a Tw is van toepassing op "eenieder" die gegevens opslaat of uitleest op randapparatuur (zoals een computer of een mobiele telefoon) van een eindgebruiker, ongeacht waar de partij gevestigd is. Daarbij is volgens de ACM bepalend dat de norm bedoeld is om eindgebruikers in Nederland te beschermen. Daarom zijn het informatie- en toestemmingsvereiste bij het gebruik van cookies van toepassing op Nederlandse en buitenlandse websites die zich (mede) op Nederlandse gebruikers richten. Of websites zich richten op Nederlandse gebruikers kan worden afgeleid uit bijvoorbeeld de aard van de informatie op de website, de mogelijkheid om producten te laten bezorgen in Nederland of de beschikbaarheid van de website in de Nederlandse taal. De domeinnaam extensie (.nl / .eu / .com / .net / etc.) van de website is niet doorslaggevend.[223]

309. Uit onderzoek (**Productie 16**) blijkt dat Oracle en Salesforce cookies plaatsen via een groot aantal op Nederland gerichte websites. Het gaat om bijvoorbeeld de website buienradar.nl, die actuele informatie over regen in Nederland biedt en die dus naar zijn aard op Nederland gericht is. Beide partijen plaatsen derhalve cookies op de randapparatuur van Nederlandse internetgebruikers en lezen deze uit. Daarmee valt hun gedrag binnen het bereik van artikel 11.7a Tw en moeten zij ervoor zorgen dat zij aan het informatie- en toestemmingsvereiste voldoen.

## 4.6 Schending AVG en Tw

310. De in het feitelijk kader omschreven gegevensverwerking van Oracle en Salesforce is in strijd met het fundamentele recht op eerbiediging van het privéleven (artikel 7 Handvest) en het fundamentele recht op bescherming van persoonsgegevens (artikel 8 Handvest), zoals onder meer uitgewerkt in de AVG en de Telecommunicatiewet. In het navolgende worden de

[222] Overweging 24 AVG en EDPB Guidelines 3/20 Territorial Scope, p. 20.
[223] *Kamerstukken I* 2011/12, 32549, E, p. 7-8.

relevante beginselen en bepalingen uit de AVG en de Tw toegelicht en de schending onderbouwd.

311. In de eerste plaats is van belang dat de handelingen die Oracle en Salesforce verrichten kwalificeren als “profilering” in de zin van artikel 4 lid 4 AVG en, gelet op de feiten en omstandigheden, verboden zijn op grond van artikel 22 AVG. In de tweede plaats geldt dat Oracle en Salesforce niet beschikken over een geldige grondslag voor het plaatsen en uitlezen van cookies, in het bijzonder ontbreekt het Oracle en Salesforce aan geldige toestemming om deze handelingen te verrichten. In de derde plaats voldoen Oracle en Salesforce niet aan de vereiste transparantieplicht over hun handelingen, die grotendeels buiten het zicht van de internetgebruiker plaatsvinden. In de vierde plaats is de gigantische verzameling van gegevens strijdig met het beginsel van dataminimalisatie. In de vijfde plaats voldoen Oracle en Salesforce niet aan de beginselen integriteit en vertrouwelijkheid en de wijze waarop deze zijn uitgewerkt in specifieke AVG-bepalingen. In de zesde plaats voldoen Oracle en Salesforce niet aan hun verantwoordingsplicht, ook een kernbeginsel van de AVG.

312. In het navolgende wordt deze zeer ernstige schending nader onderbouwd. Hierboven is al de schending van fundamentele rechten door Oracle en Salesforce besproken. Hieronder zal eerst ingegaan worden op de schending van het profileringsverbod. Aansluitend worden de zes in de vorige alinea genoemde schendingen toegelicht. Ten slotte zal worden aangetoond dat Oracle en Salesforce ook op diverse andere manieren de AVG schenden.

*4.6.1 Geautomatiseerde besluitvorming waaronder profilering*

313. In het feitelijke kader is toegelicht dat één van de belangrijkste activiteiten van Oracle en Salesforce bestaat uit het creëren van gedetailleerde profielen van internetgebruikers. Oracle en Salesforce vergaren informatie uit uiteenlopende bronnen en geven adverteerders de middelen om daarmee zeer eenvoudig “segments” of “audiences” te creëren. Oracle en Salesforce nemen de adverteerders aan de hand en leggen uit hoe deze met een paar muisklikken de doelgroep steeds specifieker kunnen maken. De software van Oracle en Salesforce koppelt de kenmerken vervolgens aan de gegevens die zij uit verschillende bronnen verzamelt. Doel van deze gegevensverzameling is om precieze conclusies te trekken over het privéleven van personen. De gegevens leggen tal van eigenschappen bloot, zoals dagelijkse gewoonten, permanente of tijdelijke verblijfplaats, het online leesgedrag, informatie over aankopen.

314. Wanneer sprake is van profilering past het HvJEU de relevante grondrechten en de AVG en Tw bijzonder stringent toe. De enkele mogelijkheid aan de hand van gegevens een profiel te maken, leidt tot de conclusie dat het gaat om zeer gevoelige informatie, die de bescherming van de fundamentele rechten die de artikelen 7 en 8 Handvest beschermen in de kern raken. In de zaak *Tele2* verwoordt het HvJEU het als volgt:

> *“Zoals de advocaat-generaal in de punten 253, 254 en 257 tot en met 259 heeft opgemerkt, kan aan de hand van deze gegevens het profiel van de betrokken*

*personen worden bepaald, informatie die, wat het recht op bescherming van het privéleven betreft, even gevoelig is als de inhoud zelf van de communicaties."*[224]

315. Op dezelfde wijze als een zoekmachine zoals Google een "beslissende rol" vervult bij het toegankelijk maken van websites door deze aan de hand van bepaalde kenmerken doorzoekbaar te maken, spelen ook Oracle en Salesforce een beslissende rol bij het online volgen en *targeten* van internetgebruikers. Zonder Oracle en Salesforce is het immers niet mogelijk de profielen op te stellen, laat staan de mate van detail daarvan te creëren.[225] Terwijl de zoekresultaten van Google volgens het HvJEU slechts in een "min of meer gedetailleerd profiel van de betrokkene" kunnen resulteren[226], leiden de activiteiten van Oracle en Salesforce tot een zeer fijnmazig profiel van een identificeerbare persoon, een profiel dat bovendien steeds meer verfijnd wordt in het kader van RTB en toevoeging van additionele informatie. De eigenschappen die daarbij in kaart kunnen worden gebracht, vormen gevoelige of bijzondere persoonsgegevens, bijvoorbeeld etniciteit, gezondheid en fitness, politiek, religie en spiritualiteit.

316. WG29 verwijst in haar Richtsnoeren over profilering naar een onderzoek waarin simpele Facebook-"likes" worden gecombineerd met gegevens uit andere bronnen. De onderzoekers waren in staat om in 88% van de gevallen de seksuele geaardheid van mannelijke gebruikers vast te stellen. In 95% van de gevallen was de etnische afkomst goed in te schatten. In 82% maakten de onderzoekers een juiste voorspelling of de internetgebruiker christen of moslim was.[227]

317. De tools van Oracle en Salesforce maken het mogelijk om steeds specifieker te worden. "Digging a little deeper," noemt Oracle dat.[228] Nadat aan de hand van diverse specifieke eigenschappen een doelgroep is gemaakt aan wie advertenties worden getoond, laten Oracle en Salesforce zien hoe groot de doelgroep is die getarget wordt met advertenties.[229] Oracle en Salesforce knopen alle bekende informatie aan elkaar en komen tot een gedetailleerd profiel op basis waarvan ze kunnen beoordelen of iemand binnen een doelgroep past. Ook kunnen ze doelgroepen specificeren met behulp van de profielen van personen die binnen de doelgroep vallen. Dankzij cookie syncing, zoals hierboven omschreven, worden de profielen nog specifieker.

318. Zo ontstaat een fijnmazig web van profielen, waarbij iedere internetgebruiker in een hokje wordt gestopt op basis van hun veronderstelde voorkeuren en interesses. WG29 geeft in haar Richtsnoeren diverse risico's van profilering, onder meer het ondermijnen van de keuzevrijheid voor bepaalde producten of diensten.

---

[224] HvJEU 21 december 2016, gevoegde zaken C-203/15 en C-698/15, ECLI:EU:C:2016:970, (*Tele2*), r.o. 99.
[225] Zie HvJEU 24 september 2019, C-136-17, ECLI:EU:C:2019:773 (*Google*), r.o. 36, waarin Google wordt omschreven als een partij die een "beslissende rol" speelt bij het toegankelijk maken van gegevens.
[226] Zie HvJEU 24 september 2019, C/136-17, ECLI:EU:C:2019:773 (*Google*), r.o. 36.
[227] Artikel 29 werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, zoals laatstelijk gewijzigd en vastgesteld op 6 februari 2018, WP251rev.01, p. 18 ('WP251 Profilering').
[228] Oracle Create Audience Segments, **Productie 13**, tevens beschikbaar via: https://learn.oracle.com/ords/launchpad/learn?page=create-audience-segments&context=0:41799:41822, geraadpleegd op 22 juli 2020.
[229] Salesforce Segment Builder Guide, **Productie 14**, tevens beschikbaar op https://konsole.zendesk.com/hc/en-us/articles/217950467-Segment-Builder-Guide, geraadpleegd op 22 juli 2020.

> *"Het kan er ook voor zorgen dat personen in 'hokjes' worden geplaatst en zo worden vastgepind op hun veronderstelde voorkeuren. Hierdoor kan hun vrijheid om te kiezen, bijvoorbeeld bepaalde producten of diensten zoals boeken, muziek of nieuwsberichten, worden ondermijnd. In sommige gevallen kan profilering tot onjuiste voorspellingen leiden. In andere gevallen kan profilering tot weigering van dienstverlening en goederen en tot ongerechtvaardigde discriminatie leiden."* [230]

319. In artikel 4 lid 4 AVG wordt "profilering" als volgt gedefinieerd:

> *"elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;"*

320. Dit is precies de activiteit die Oracle en Salesforce verrichten. Het gaat immers om een vorm van *geautomatiseerde* verwerking. De diensten van Oracle en Salesforce zijn typische voorbeelden van big data toepassingen. Dagelijks worden miljoenen gegevens verzameld via cookies, verrijkt met andere bronnen en gekoppeld aan andere cookie identificatoren, die geautomatiseerd wordt geanalyseerd om verbanden te herkennen. Zoals WG29 in haar Richtsnoeren aangeeft is een zekere mate van geautomatiseerde verwerking voldoende; menselijke tussenkomst betekent niet dat de activiteit niet onder de definitie valt.[231] De gegevensverwerking van Oracle en Salesforce heeft bovendien betrekking op persoonsgegevens (het tweede vereiste). In de derde plaats heeft deze tot doel van persoonlijke aspecten van een natuurlijk persoon te evalueren.

4.6.1.1 <u>Verbod op uitsluitend geautomatiseerde besluitvorming</u>

321. De activiteiten van Oracle en Salesforce zijn in strijd met artikel 22 AVG. De AVG bevat specifieke nieuwe bepalingen voor de bestrijding van de risico's die ontstaan door profilering en geautomatiseerde besluitvorming. Met 22 lid 1 AVG heeft de Europese wetgever niet minder dan een verbod geïntroduceerd om besluiten te nemen die uitsluitend zijn gebaseerd op een geautomatiseerde verwerking van persoonsgegevens, als die besluiten rechtsgevolgen hebben of de betrokkene anderszins in aanmerkelijke mate treffen.[232] Artikel 22 lid 1 AVG luidt als volgt:

> *"De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan*

[230] WP251 Profilering, p. 6.
[231] WP251 Profilering, 7.
[232] Hoewel de tekst van artikel 22 lid 1 is geformuleerd als recht ("De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat het anderszins in aanmerkelijke mate treft."), is dit niet een recht dat de dient in te roepen maar een verbod. Zie ook WP251 Profilering, p. 23: " Het woord "recht" in deze bepaling betekent niet dat artikel 22, lid 1, alleen van toepassing is wanneer de betrokkene er specifiek een beroep op doet. Artikel 22, lid 1, voorziet in een algemeen verbod op uitsluitend op geautomatiseerde verwerking gebaseerde besluitvorming. Dit verbod is van toepassing, ongeacht of de betrokkene wel of niet actie onderneemt met betrekking tot de verwerking van zijn persoonsgegevens."

*voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft."*

322. Een besluit met rechtsgevolg is bijvoorbeeld de beëindiging van een overeenkomst of de weigering van een vergunning. Artikel 22 lid 1 AVG beperkt zich echter niet tot besluiten met rechtsgevolgen. In haar Richtsnoeren benoemt WG29 expliciet dat online reclame, wanneer gebruik gemaakt wordt van geautomatiseerde instrumenten, de betrokkene in aanmerkelijke mate kan treffen en daarmee onder het verbod kan vallen. Zoals beschreven is het plaatsen van cookies, cookie syncing en het RTB-proces bij uitstek een uitsluitend geautomatiseerd proces dat zich in enkele seconden voltrekt, en dat zich, gezien de snelheid, de hoeveelheid gegevens en de hoeveelheid spelers, niet anders dan uitsluitend geautomatiseerd kan voltrekken. Hetzelfde geldt voor de wijze waarop data wordt verrijkt door de DMPs.

323. WG29 benoemt als factoren die relevant zijn voor de beoordeling of online reclame onder het verbod valt:

*"• het indringende karakter van het profileringsproces, zoals opsporing via verschillende websites, apparaten en diensten;*

*• de verwachtingen en wensen van de betrokken personen;*

*• de manier waarop de advertentie wordt gepresenteerd; of*

*• het gebruik van kennis over de kwetsbaarheden van de benaderde betrokkenen."*[233]

324. Dit zijn bij uitstek kenmerken van de handelwijze van Oracle en Salesforce zoals hiervoor beschreven. Immers, onder meer door middel van cookie syncing is sprake van een grootschalig en indringend profileringsproces waarbij persoonsgegevens worden verzameld via verschillende websites, apparaten en diensten. De betrokken personen zijn zich in het geheel niet bewust van de grootschaligheid, de hoeveelheid op de achtergrond betrokken spelers en mate van detail van de profilering. Juist door het fijnmazige profiel kan de betrokkene zeer specifiek worden *getarget* en kunnen hem de meest relevante advertenties getoond worden, waarbij ten volle gebruik gemaakt kan worden van kennis over kwetsbaarheden van betrokkenen.

325. Inherent aan de mate van detail van profilering, *digging a little deeper*, en de grootschaligheid en efficiëntie van het geautomatiseerde proces van de DMPs is dat gebruik gemaakt zal worden van kwetsbaarheden van betrokkenen. Dit benadrukt WG29 in de Richtsnoeren over profilering:

*"Verwerking die personen in het algemeen weinig treft, kan bepaalde groepen van de maatschappij, zoals minderheden of kwetsbare volwassenen, mogelijk in aanmerkelijke mate treffen. Als bijvoorbeeld een persoon waarvan bekend is dat hij financiële moeilijkheden heeft of die waarschijnlijk in financiële moeilijkheden verkeert, regelmatig advertenties voor leningen met een hoge rente wordt getoond,*

[233] WP251 Profilering, p. 26.

*is het mogelijk dat hij zich voor deze aanbiedingen aanmeldt en zich dieper in de schulden steekt."*[234]

326. Op het verbod op geautomatiseerde besluitvorming, waaronder profilering, worden drie uitzonderingen gemaakt in artikel 22 lid 2 AVG. Op geen van deze uitzonderingen kunnen Oracle en Salesforce een beroep doen.

327. Vooropgesteld zij dat volgens vaste rechtspraak van het HvJEU uitzonderingen op de AVG strikt moeten worden uitgelegd, aangezien zij de bescherming waarin de verordening voorziet opzij zetten en daarmee afwijken van het met de AVG beoogde doel, de bescherming van fundamentele rechten.[235]

328. De eerste uitzondering is van toepassing wanneer de verwerkingsverantwoordelijke kan aantonen dat profilering noodzakelijk is om de overeenkomst aan te gaan of uit te voeren, bijvoorbeeld een abonnement op een streamingdienst die zo specifieke mogelijke suggesties doet aansluitend bij de interesses van de abonnee op basis van een profiel. Nu er geen sprake is van een overeenkomst tussen Oracle of Salesforce enerzijds en de betrokkene anderzijds geldt deze uitzondering niet.

329. De tweede uitzondering is van toepassing wanneer geautomatiseerde besluitvorming en profilering uitdrukkelijk is toegestaan bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Een voorbeeld is een wet die geautomatiseerde besluitvorming toestaat om belastingfraude op te sporen. Van een dergelijke wettelijke uitzondering is wat de praktijken van Oracle en Salesforce betreft geen sprake.

330. Het commerciële belang van grote spelers in de *ad-tech* markt om indringende digitale profielen van Europese betrokkenen te creëren en op grote schaal internationaal uit te wisselen is niet een belang dat de wetgever zal willen erkennen met een wettelijke uitzondering. Integendeel, juist met de AVG heeft de Europese wetgever een krachtig en coherent wettelijk kader, gesteund door strenge handhaving, willen introduceren om in tijden van snelle technologische ontwikkelingen en globalisering betrokkenen een consistent en hoog niveau van bescherming te kunnen geven.

331. De derde uitzondering geldt wanneer de betrokkene *uitdrukkelijke* toestemming heeft gegeven voor de geautomatiseerde besluitvorming en profilering. Zoals hierna beschreven zal worden, is geen sprake van geldige toestemming, laat staan van uitdrukkelijke toestemming specifiek ten aanzien van de geautomatiseerde besluitvorming en profilering.

332. Voor zover de eerste (overeenkomst) of derde (uitdrukkelijke toestemming) al in aanmerking komt, kan van deze uitzonderingen slechts gebruik worden gemaakt indien de verwerkingsverantwoordelijke passende maatregelen heeft genomen ter bescherming van de betrokkene. In elk geval moet specifieke informatie over de verwerking worden verstrekt aan de betrokkene (overweging 71 AVG). Verder moet de betrokkene de mogelijkheid hebben om iemand daarbij te betrekken ("recht op menselijke tussenkomst"), om zijn of haar standpunt kenbaar te maken, om uitleg over het aldus genomen besluit te krijgen en om het besluit aan te vechten. Voorzover Oracle en Salesforce zich al succesvol op een van bovengenoemde

[234] WP251 Profilering, p. 26.
[235] HvJEU 14 februari 2019, C-345/17, ECLI:EU:C:2019:122, (*Buivids*), r.o. 41 en de daar aangehaalde jurisprudentie.

uitzonderingen zouden kunnen beroepen, dan is bijvoorbeeld aan de specifieke informatieplicht al niet voldaan zoals hieronder zal worden toegelicht.

333. Zoals al blijkt uit de hiervoor geciteerde passage van WG29 over Facebook-likes, is aan de grootschalige en fijnmazige profilering overigens welhaast inherent dat bijzondere persoonsgegevens zullen worden verwerkt, voor zover dit niet al doelbewust gebeurt. Door koppeling van informatie uit verschillende bronnen zijn dusdanige juiste voorspellingen te doen over bijvoorbeeld seksuele of religieuze voorkeuren of gezondheid, dat het intensieve actieve handelingen zal vereisen bijzondere persoonsgegevens *niet* te verwerken.

334. Voor zover Oracle en Salesforce al gebruik kunnen maken van de uitzonderingen op het verbod op geautomatiseerde besluitvorming en profilering geldt dat geen gebruik mag worden gemaakt van bijzondere gegevens, tenzij sprake is van de uitdrukkelijke toestemming van de betrokkene (artikel 9 lid 2 sub a AVG) of er sprake is van een zwaarwegend algemeen belang (artikel 9 lid 2 sub g AVG). Aan deze voorwaarden voldoen Oracle en Salesforce niet. In beide gevallen moet de verwerkingsverantwoordelijke overigens passende maatregelen treffen om de rechten en vrijheden en het gerechtvaardigde belang van de betrokkene te waarborgen.

335. Hoewel in artikel 22 zelf geen onderscheid gemaakt wordt tussen volwassenen en kinderen, wordt in overweging 71 vermeld dat uitsluitend geautomatiseerde besluitvorming, met inbegrip van profilering, waaraan rechtsgevolgen verbonden zijn of die de betrokkene anderszins in aanmerkelijke mate treft, niet van toepassing mag zijn op kinderen. WG29 licht in haar Richtsnoeren toe dat dit zo moet worden uitgelegd dat verwerkingsverantwoordelijken in beginsel geen gebruik mogen maken van de vrijstellingen van artikel 22, lid 2, om dit soort verwerking te rechtvaardigen.[236] Hier voegt WG29 overigens nog aan toe dat organisaties *in het algemeen* moeten afzien van profilering van kinderen voor marketingdoeleinden.[237]

4.6.1.2 <u>Overige specifieke vereisten voor profilering</u>

336. De AVG richt zich niet alleen op de besluiten die worden genomen op basis van geautomatiseerde verwerking of profilering, maar is van toepassing op de verzameling van gegevens voor het aanmaken van profielen en de toepassing van deze profielen op personen. Ook buiten het kader van de uitzonderingen op het verbod op geautomatiseerde besluitvorming, verwijst de wetgever op verschillende plekken expliciet naar aanvullende passende waarborgen die getroffen moeten worden in het kader van profilering in het algemeen.

337. Zo gelden specifieke vereisten in verband met transparantie, zoals ook beschreven in overweging 60:

> *"Voorts moet de betrokkene worden geïnformeerd over het bestaan van profilering en de gevolgen daarvan."*

338. In overweging 63 wordt dit aangevuld:

[236] WP251 Profilering, p. 34.
[237] WP251 Profilering, p. 35.

> *"Elke betrokkene dient dan ook het recht te hebben te weten en te worden meegedeeld [...] welke logica er ten grondslag ligt aan een eventuele automatische verwerking van de persoonsgegevens en, ten minste wanneer de verwerking op profilering is gebaseerd, wat de gevolgen van een dergelijke verwerking zijn."*

339. Ook hebben betrokkenen het recht bezwaar te maken tegen profilering en specifiek profilering voor marketingdoeleinden, zoals ook beschreven in overweging 70:

> *"Wanneer persoonsgegevens worden verwerkt ten behoeve van direct marketing dient de betrokkene, ongeacht of het een aanvankelijke dan wel een verdere verwerking betreft, het recht te hebben te allen tijde en kosteloos bezwaar te maken tegen deze verwerking, ook in het geval van profilering voor zover deze betrekking heeft op de direct marketing. Dat recht moet uitdrukkelijk, op duidelijke wijze en gescheiden van overige informatie, onder de aandacht van de betrokkene worden gebracht."*

340. Overigens gelden in het kader van profilering strengere verplichtingen in verband met de verantwoordingsplicht (bijvoorbeeld op grond van artikel 37 lid 1 sub b AVG) en bestaat er, indien aan bepaalde voorwaarden is voldaan, de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren (artikel 35 lid 3 sub a AVG).

4.6.1.3 Conclusie ten aanzien van geautomatiseerde besluitvorming en profilering

341. Gelet op het voorgaande handelen Oracle en Salesforce in strijd met artikel 22 AVG. Voor zover uw rechtbank van oordeel zou zijn dat Oracle en Salesforce in weerwil van het bovenstaande in overeenstemming met artikel 22 handelen, brengt dat geenszins met zich mee dat de handelwijze van Oracle en Salesforce geoorloofd is. Het feit dat sprake is van profilering in de zin van artikel 4 lid 4 AVG brengt met zich mee dat de overige voorwaarden van de AVG extra stringent zullen moeten worden beoordeeld. Hieronder zal worden toegelicht dat Oracle en Salesforce hoe dan ook niet voldoen aan, onder meer, de beginselen van rechtmatigheid, transparantie en dataminimalisatie.

*4.6.2 Rechtmatigheid – verwerking niet rechtmatig, geen geldige toestemming*

4.6.2.1 Toestemming is de enige grondslag die in aanmerking komt

342. Een verwerking van persoonsgegevens moet altijd gebaseerd worden op één van de zes limitatieve grondslagen uit artikel 6 AVG.[238] Indien geen van deze grondslagen van toepassing is, is de verwerking onrechtmatig. Voor de verwerkingen waarop deze zaak ziet, komen alleen de grondslagen "toestemming" (sub a) en "gerechtvaardigd belang" (sub f) in aanmerking.

343. Artikel 6 AVG luidt, voorzover van belang:

> *"Rechtmatigheid van de verwerking*
>
> *1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:*

[238] Autoriteit Persoonsgegevens, "Normuitleg grondslag 'gerechtvaardigd belang'," 1 november 2019, p. 1.

*a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;*

*[…]*

*f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.*

*[…]"*

344. Oracle erkent dat de gegevensverwerking die zij verricht slechts gelegitimeerd kan worden op basis van "toestemming". Oracle geeft dat in haar Privacybeleid voor Oracle Data Cloud nadrukkelijk aan:

> *"Wij hebben uw toestemming nodig om klanten en partners van Oracle Marketing & Data Cloud in staat te stellen producten en services onder uw aandacht te brengen, inclusief metingen en analyses van campagneprestaties, personalisatie, modellering, onboarding en koppeling (zie Sectie 5 hierboven voor meer informatie over deze doeleinden). Uw toestemming wordt verkregen ten behoeve van Oracle en de klanten en partners van Oracle Marketing & Data Cloud via onze externe gegevensleveranciers* (…)"[239]

345. Oracle meent echter dat zij niet verantwoordelijk is voor het verkrijgen van deze toestemming. Zij vindt dat de partners van Oracle namens Oracle die toestemming moeten vragen.

346. Uit de privacy documentatie van Salesforce blijkt niet of niet voldoende duidelijk op welke grondslag zij haar gegevensverwerking baseert. Salesforce geeft in haar "Trust and Compliance Documentation" aan dat haar partners verantwoordelijk zijn om toestemming te vragen, althans voor zover wettelijk vereist:

> *"The Audience Studio Services enable customers to use cookies and/or other tracking technologies. Customers shall be solely responsible (i) for assessing whether such technologies can be used in compliance with applicable legal requirements, and (ii) for providing notice and/or obtaining consent, as may be required by law, for such use of cookies and/or other tracking technologies. Salesforce disclaims any liability to customers or any third parties arising from customers' use of any cookies and tracking technologies." (**Productie 23.f**)*

347. Deze "Trust and Compliance Documentation" is overigens gericht op (potentiele) klanten van Salesforce en voor een Nederlandse internetgebruiker zeer lastig vindbaar (zie tevens paragraaf 4.3.1.2). Hieruit blijkt echter wel dat ook Salesforce niet uitsluit dat toestemming gevraagd moet worden. Ook Salesforce laat het vragen daarvan over aan haar klanten. Op basis

[239] Privacybeleid voor Oracle Data Cloud, onder 6 "wat is onze wettelijke basis voor informatie over u verzameld in de EU/EER?", zie https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 14 juli 2020 (tevens **Productie 22.a**).

van welke grondslag haar gegevenspartners persoonsgegevens verzamelen, verwerken en verstrekken aan Salesforce is niet duidelijk.

348. Opgemerkt zij dat een eenmaal gemaakte keuze voor een grondslag later niet kan worden gewijzigd.[240] Het staat Oracle en Salesforce dan ook niet (langer) vrij een aanvullende of andere grondslag (zoals gerechtvaardigd belang) aan te voeren, althans, indien zij dat doen zou dat wederom een schending van de AVG opleveren.

349. De cruciale rol van toestemming wordt benadrukt in artikel 8 van het Handvest, zo bevestigen ook de WG29 en de EDPB.[241]

350. In het navolgende zal worden toegelicht dat "toestemming" in casu de enige geldige grondslag is voor de gegevensverwerking, dat Oracle en Salesforce het verkrijgen van die toestemming niet kunnen delegeren aan hun klanten en dat de toestemming, die al dan niet via deze klanten is verkregen, niet voldoet aan de criteria van rechtsgeldige toestemming.

Beroep op gerechtvaardigd belang niet mogelijk

351. Vooropgesteld zij dat de grondslag van artikel 6 sub f AVG niet in aanmerking komt. Allereerst geldt dat voor het plaatsen en uitlezen van cookies artikel 11.7a Tw bepaalt dat toestemming de enig mogelijke grondslag is. [242] Bovendien volgt dat ook uit het arrest van het HvJEU in de zaak *FashionID*, met betrekking tot het plaatsen van een social plug/in, een techniek vergelijkbaar met cookies waarop artikel 5 lid 3 van de ePrivacyrichtlijn (artikel 11.7a Tw) van toepassing is:

> *"87. Met zijn vierde vraag wenst de verwijzende rechter in wezen te vernemen of in een situatie als die welke in het hoofdgeding aan de orde is, waarin de beheerder van een internetsite op deze site een social plug-in invoegt die ervoor zorgt dat de browser van een bezoeker van deze site content van de aanbieder van die plug-in opvraagt en daartoe persoonsgegevens van de bezoeker aan deze aanbieder doorzendt, voor de toepassing van artikel 7, onder f), van richtlijn 95/46 het gerechtvaardigde belang van die beheerder dan wel dat van die aanbieder in aanmerking dient te worden genomen.*
>
> *88. Vooraf zij opgemerkt dat deze vraag volgens de Commissie niet relevant is voor de beslechting van het hoofdgeding, omdat de op grond van artikel 5, lid 3, van richtlijn 2002/58 vereiste toestemming van de betrokkenen niet is verkregen.*
>
> *89. In dit verband moet worden geconstateerd dat de lidstaten er volgens die bepaling zorg voor moeten dragen dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken*

[240] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, ('EDPB Guidelines 05/2020 Consent') 4 mei 2020, p. 25, par. 120; Artikel 29 werkgroep, Advies 15/11 over de definitie van toestemming, 13 juli 2011, WP187, p. 8 ('WP187 Definitie van toestemming'), p. 21.
[241] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, ('EDPB Guidelines 05/2020 Consent') 4 mei 2020; Artikel 29 werkgroep, Advies 15/11 over de definitie van toestemming, 13 juli 2011, WP187, p. 8 ('WP187 Definitie van toestemming').
[242] Zie artikel 11.7a lid 3 Tw.

*abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig richtlijn 95/46, onder meer over de doeleinden van de verwerking."*[243]

352. Voor zover Oracle en Salesforce wel (alsnog) een beroep op de grondslag gerechtvaardigd belang zouden doen, geldt bovendien dat deze niet van toepassing is, omdat:

a. Geen sprake is van een gerechtvaardigd belang, namelijk louter een zuiver commercieel belang;

b. De verwerking niet noodzakelijk is, omdat deze niet proportioneel is;

*c.* De belangen, grondrechten en fundamentele vrijheden van betrokkenen zwaarder wegen dan de louter commerciële belangen van Oracle en Salesforce.[244]

4.6.2.2 Delegeren verkrijging toestemming niet mogelijk

353. Oracle en Salesforce kunnen het verkrijgen van toestemming niet delegeren aan hun klanten om ten minste drie redenen.

354. In de eerste plaats geldt dat het niet de klanten van Oracle en Salesforce zijn die cookies plaatsen, maar Oracle en Salesforce zelf (zie onder paragraaf 3.2.1). Dat blijkt onder meer uit het feit dat de cookies de namen die Oracle en Salesforce daaraan toegekend hebben dragen en technisch gekoppeld zijn aan het domein van Oracle en Salesforce. De gegevenstransmissie vindt plaats tussen de randapparatuur van de internetgebruiker en de servers van Oracle en Salesforce. Het zijn ook Oracle en Salesforce die hier (verwerkings)verantwoordelijk voor zijn. Dat geldt ook voor de handelingen die zij verrichten aansluitend op het plaatsen van de cookie en het daarmee vergaren van informatie, namelijk profilering, het verrijken van profielen met informatie uit andere bronnen, het aanbieden van profielen in het kader van real-time bidding en de cookie syncing.

355. In de tweede plaats geldt dat de klanten van Oracle en Salesforce geen rechtsgeldige toestemming kunnen vragen voor deze activiteiten omdat zij daar niet (volledig) van op de hoogte zijn. De klanten van Oracle en Salesforce zijn bijvoorbeeld niet op de hoogte van de wijze waarop een DMP met andere partners in de *ad-tech* industrie unieke identificatoren van cookies uitwisselt en de aldus verkregen informatie aan elkaar knoopt door middel van cookie syncing.

356. In de derde plaats kunnen deze klanten onmogelijk rechtsgeldige toestemming verkrijgen omdat zij internetgebruikers nooit volledig en specifiek kunnen informeren over de reikwijdte van de gegevensverwerking. Gegevens worden bij iedere veiling in het kader van RTB met honderden partijen gedeeld. Oracle en Salesforce delen gegevens met een dusdanige grote, gevarieerde groep dat deze bij aanvang van een veiling niet eens bekend kan zijn. (bij aanvang onbekende) partijen. Het is feitelijk onmogelijk om voor een dergelijk omvangrijke verwerking, door een veelvoud aan partijen, adequate informatie te verstrekken over onder

[243] HvJEU 29 juli 2019, C-40/17, ECLI:EU:C:2019:629 (*Fashion ID*).
[244] Vgl. Autoriteit Persoonsgegevens, Normuitleg grondslag 'gerechtvaardigd belang', 1 november 2019.

meer de identiteit van die partijen. Ook is het onmogelijk om adequaat te informeren over alle verwerkingsdoelen van al die partijen.

357. Voorzover uw rechtbank zou oordelen dat Salesforce en/of Oracle het verkrijgen van toestemming in casu kunnen delegeren aan hun klanten en/of partners, geldt dat de eventueel door hen verkregen toestemming niet voldoet aan de voorwaarden die de AVG en Tw daaraan stellen. De bewijslast dat rechtsgeldige toestemming is verkregen rust op Oracle en Salesforce (o.a. artikel 7 lid 1 AVG).

4.6.2.3 Geen sprake van geldige toestemming

358. Artikel 4 sub 11 AVG definieert "toestemming" als volgt (onderstreping advocaat):

> *"elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;"*

359. Dat betekent dat toestemming alleen een geldige grondslag onder artikel 6 AVG oplevert wanneer deze (i) vrij, (ii) specifiek, (iii) geïnformeerd, en (iv) ondubbelzinnig is. Toestemming op grond van artikel 11.7a Tw moet aan dezelfde voorwaarden voldoen als toestemming op grond van artikel 6 AVG. Dat blijkt ook uit het arrest van het HvJEU in de zaak *Planet49*[245]en uit de bewoording van artikel 11.7a Tw.

360. De verwerking van persoonsgegevens door Oracle en Salesforce voldoet niet aan deze voorwaarden.

(i) Vrij

361. In de eerste plaats is geen sprake van vrije toestemming. Vrije toestemming houdt in dat de betrokkene een daadwerkelijke keuze kan maken. Als de betrokkene zich min of meer gedwongen voelt of als het voor hem negatieve gevolgen heeft als hij zijn toestemming weerhoudt of intrekt, is geen sprake van een geldige toestemming. Het is aan de verantwoordelijke om aan te tonen dat betrokkene daadwerkelijk een vrije keuze had, en dat het mogelijk was om geen toestemming te geven of de toestemming in te trekken zonder nadeel (overweging 42 AVG). [246]

362. Het is in verband met het vereiste dat toestemming vrij moet zijn, niet toegestaan om toestemming te verlangen als (indirecte) tegenprestatie voor het leveren van een prestatie (waaronder een dienst). Wanneer de verwerking niet noodzakelijk is voor het leveren van de prestatie, mag het leveren van die prestatie niet afhankelijk worden gesteld van het verkrijgen van de persoonsgegevens op grond van toestemming (artikel 6 lid 4 en overweging 43 AVG).[247]

363. Opmerkelijk is dat een groot deel van de websites in het geheel geen toestemming vragen voordat de cookies worden geplaatst. Uit het technisch onderzoek blijkt dat ten minste 22 van de 100 onderzochte websites cookies plaatsen voor of zonder dat zij toestemming vragen,

[245] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[246] EDPB Guidelines 05/2020 Consent, p. 13.
[247] Zie voorts EDPB Guidelines 05/2020 Consent, p. 10-12.

waarvan op 12 websites Salesforce cookies en op 10 websites Oracle cookies werden geplaatst (**Productie 16**).

364. Andere websites stellen het geven van toestemming voor het gebruik van cookies als voorwaarde voor het bezoeken van de website, dit wordt ook wel een "cookiewall" genoemd. Uit **Productie 18** blijkt dat zeker 9 van de websites via welke Oracle en Salesforce hun cookies (mede) gericht op Nederlandse internetgebruikers plaatsen, gebruik maken van een cookiewall. Deze toestemming is niet vrij. Het is dan voor betrokkene immers niet mogelijk om toestemming te onthouden zonder daarvan nadeel te ondervinden.[248] Het leveren van de dienst, toegang tot de website, wordt daarmee afhankelijk gemaakt van het geven van toestemming, terwijl de verwerking niet noodzakelijk is voor het leveren van de dienst.[249] Uit het arrest van het HvJEU in de zaak *Planet49* volgt dat het op een dergelijke wijze vragen van toestemming, die geen actieve handeling vereist, niet geoorloofd is.[250]

365. Ook de Autoriteit Persoonsgegevens is er zeer duidelijk over dat met een cookiewall geen geldige toestemming kan worden verkregen:

> *"Mag ik als organisatie een cookiewall gebruiken?*
>
> *Bij een cookiewall hebben websitebezoekers geen echte of vrije keuze. Weliswaar kunnen ze tracking cookies weigeren, maar dat kan niet zonder nadelige gevolgen. Want tracking cookies weigeren, betekent dat ze geen toegang krijgen tot de website. Daarom zijn cookiewalls onder de AVG verboden."*[251]

366. In de tweede plaats is geen sprake van vrije toestemming wanneer de toestemming voor verschillende verwerkingsactiviteiten of doeleinden aan elkaar worden verbonden. Wanneer een dienst meerdere verwerkingsactiviteiten of doeleinden omvat, moet de betrokkene vrij kunnen kiezen voor welke verwerkingen en/of doeleinden hij toestemming geeft, en voor welke niet. Als een betrokkene slechts toestemming kan geven voor een pakket verwerkingen en/of doeleinden, wordt de toestemming niet als vrij beschouwd (overweging 32 en 43 AVG).[252] Of zoals de WG29 het formuleerde:

> *"Indien de verwerkingsverantwoordelijke verschillende doeleinden voor verwerking heeft samengevoegd, en niet heeft getracht om voor elk doel afzonderlijke toestemming te krijgen, is er sprake van een gebrek aan vrijheid."*[253]

367. Dit laatste sub-vereiste wordt ook wel "granulariteit" genoemd en hangt samen met het vereiste dat de toestemming specifiek moet zijn (zie hierna). Aan dit vereiste wordt door Oracle

---

[248] Vgl. EDPB Guidelines 05/2020 Consent, p.10.
[249] Vgl. EDPB Guidelines 05/2020 Consent, p. 10-12.
[250] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[251] Autoriteit Persoonsgegevens, 'Cookies', te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies; Vgl. tevens EDPB Guidelines 05/2020 Consent, p. 12, par. 39.
[252] EDPB Guidelines 05/2020 Consent, p.12, par. 42-44.
[253] Artikel 29 werkgroep, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, WP259 rev. 01, zoals laatstelijk gewijzigd en vastgesteld op 10 april 2018 en zoals bekrachtigd door de EDPB op 25 mei 2018 ('WP259 Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679') 11; een vrijwel identieke tekst is nog altijd opgenomen in de meest recente versie van deze richtsnoeren die uitsluitend in het Engels beschikbaar zijn, zie EDPB Guidelines 05/2020 Consent, p. 12, par. 44.

en Salesforce niet voldaan. De betrokkene moet immers vrijwel altijd voor een geheel pakket aan tracking cookies van verschillende partijen, voor verschillende verwerkingen en voor verschillende doeleinden toestemming geven (zie randnummer 389). Oracle en Salesforce verkrijgen derhalve geen vrije toestemming.

368. Dat de toestemming niet vrij wordt gegeven blijkt ook uit de vele publieksonderzoeken die zijn gedaan naar het gebruik van tracking technologieën. Slechts 20% van de Europeanen is akkoord met het delen van data met derde partijen voor advertentiedoeleinden.[254] 37% gebruikt software om zich te wapenen tegen tracking technologieën. Een recent onderzoek waarbij gebruikers een website aangeboden kregen waarbij de bezoekers zelf actief een opt-in moesten aanklikken voor het gebruik van tracking technologieën resulteerde in 0,1% van gebruikers die opt-in gaf.[255]

(ii) Specifiek

369. Het vereiste dat toestemming specifiek moet zijn, houdt in dat het voor de betrokkene duidelijk moet zijn waarvoor hij precies toestemming geeft. De eis beoogt controle en transparantie voor betrokkenen te verzekeren.

370. Het moet in dit kader duidelijk zijn voor welke doeleinden de verantwoordelijke toestemming vraagt. Daarbij geldt bovendien wederom het vereiste van granulariteit: betrokkene moet per verwerking en doeleinde kunnen kiezen of hij toestemming geeft of niet. Een algemene toestemming voor verwerkingen "voor advertentiedoeleinden" voldoet hier niet aan. Samen met het beginsel van doelbinding (artikel 5 lid 1 sub b AVG) dient het vereiste dat toestemming specifiek moet zijn als bescherming tegen het geleidelijk uitbreiden van een verwerking (ook wel "function creep").[256]

371. Ook moet de toestemming voldoende specifiek zijn over de gegevens die worden verwerkt.[257] In het algemeen moet de toestemming dusdanig specifiek zijn dat de betrokkene precies weet waarvoor hij toestemming geeft:

> *"Toegevoegd moet worden dat de wilsuiting van artikel 2, onder h), van richtlijn 95/46 met name in die zin „specifiek" moet zijn dat deze precies op de verwerking van de betrokken gegevens gericht moet zijn en niet kan worden afgeleid uit een algemene wilsuiting die op iets anders betrekking heeft."* [258]

372. De toestemming voor de verwerking van persoonsgegevens door Oracle en Salesforce is niet specifiek. Het is voor de betrokkene volstrekt niet duidelijk waarvoor hij precies toestemming geeft als hij op "toestemming" of "accepteer cookies" klikt op de website van een partner van Oracle en Salesforce. Oracle en Salesforce vragen toestemming voor verschillende verwerkingen en doeleinden (het verzamelen, verrijken, delen, analyseren en verkopen) in één keer. Zij maken daarbij niet duidelijk welke gegevens precies worden verwerkt.

---

[254] GfK, "Europe Online: an Experience Driven by Advertising. Summary results", september 2017, p. 7, te raadplegen via: https://datadrivenadvertising.eu/wp-content/uploads/2017/09/EuropeOnline_FINAL.pdf

[255] C. Utz, e.a. '(Un)informed Consent: Studying GDPR Consent Notices in the Field', 22 oktober 2019, geraadpleegd op 4 mei 2020, op: https://arxiv.org/pdf/1909.02638.pdf.

[256] EDPB Guidelines 05/2020 Consent, p. 14 en 15.

[257] EDPB Guidelines 05/2020 Consent, p. 15, par. 61

[258] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*); zie tevens X.

(iii) Geïnformeerd

373. De toestemming die (de klanten en/of partners) van Oracle en Salesforce verkrijgen is ook niet "geïnformeerd".

374. Het verstrekken van informatie aan betrokkenen voordat zij toestemming geven is noodzakelijk om hen in staat te stellen een geïnformeerde beslissing te nemen en te begrijpen waarmee ze instemmen. Dit is nodig om de betrokkene in staat te stellen de controle uit te oefenen over wat er met zijn gegevens gebeurt. Er geldt een hoge standaard voor de duidelijkheid en toegankelijkheid van de te verstrekken informatie. Wanneer toestemming wordt gevraagd, moet dat in heldere en duidelijke taal, die begrijpelijk is voor een gemiddelde persoon. Informatie die relevant is voor het nemen van een weloverwogen beslissing over het al dan niet geven van toestemming mag niet verborgen zijn in algemene voorwaarden.[259]

375. Volgens de WG29 zal om geïnformeerd toestemming te kunnen geven, in ieder geval tevens de volgende informatie moeten worden verstrekt:

a. De identiteit van de verantwoordelijke;

b. De doeleinden van de verwerkingen waarvoor toestemming wordt gevraagd;

c. Welke (soort) gegevens worden verwerkt;

d. Het recht om toestemming in te trekken;

e. Informatie over geautomatiseerde besluitvorming; en

f. Informatie over doorgifte van persoonsgegevens buiten de EU.[260]

376. Wanneer sprake is van meerdere (gezamenlijk) verantwoordelijken die zich op toestemming beroepen, zullen zij allen genoemd moeten worden.[261] De verantwoordelijke moet ervoor zorgen dat toestemming slechts wordt verleend op basis van informatie die de betrokkene in staat stelt om gemakkelijk vast te stellen wie de verantwoordelijke is of de (gezamenlijk) verantwoordelijken zijn.[262]

377. Het HvJEU heeft in de zaak *Planet49* voorts benadrukt dat ook moet worden geïnformeerd over de duur dat cookies actief zijn en of derden al dan niet toegang krijgen tot de cookies:

> *"Gelet op een en ander moet op de tweede vraag worden geantwoord dat artikel 5, lid 3, van richtlijn 2002/58 aldus moet worden uitgelegd dat de aanbieder van diensten de gebruiker van een website onder meer moet informeren over de vraag hoelang de cookies actief blijven en of derden al dan niet toegang tot de cookies kunnen hebben."* [263]

[259] EDPB Guidelines 05/2020 Consent, p. 16, par. 67.
[260] EDPB Guidelines 05/2020 Consent, p. 15.
[261] EDPB Guidelines 05/2020 Consent, p. 16.
[262] EDPB Guidelines 05/2020 Consent, p. 16.
[263] HvJEU 1 oktober 2019, C—673/17, ECLI:EU:C:2019:801 (*Planet49*), r.o. 72 t/m 81.

378. Nu de activiteiten van Oracle en Salesforce moeten worden gekwalificeerd als "profilering" geldt een verzwaarde verplichting tot duidelijke communicatie, zodat de betrokkene precies begrijpt waarvoor hij toestemming verleent, zo benadrukt ook WG29:

> *"Profilering kan een ondoorzichtig proces zijn, dat vaak berust op gegevens die van andere gegevens zijn afgeleid en niet op gegevens die rechtstreeks door de betrokkene zijn verstrekt. Verwerkingsverantwoordelijken die toestemming als rechtsgrond voor profilering willen hanteren, moeten aantonen dat de betrokkenen precies begrijpen waarvoor zij toestemming verlenen en moeten zich ervan bewust zijn dat toestemming niet altijd een passende rechtsgrond is voor de verwerking. In alle gevallen moeten betrokkenen over voldoende relevante informatie beschikken over het voorgenomen gebruik en de gevolgen van de verwerking, om zeker te stellen dat de toestemming die zij verlenen een geïnformeerde keuze vormt."*[264]

379. Oracle en Salesforce hebben getracht de informatieverstrekking deels te delegeren aan de klanten en/of partners die de website aanbieden waarop de cookies worden geplaatst. Voorzover dat mogelijk is, rust de bewijslast dat rechtsgeldige toestemming is verleend, zoals gezegd, ingevolge artikel 7 lid 1 op Oracle en Salesforce. Zonder daarmee te suggereren dat de bewijslast hiervan (mede) op de Stichting rust, merkt zij op dat uit haar onderzoek volgt dat een groot deel van de websites van haar klanten en/of partners geheel geen of nauwelijks informatie bevat.

380. **Productie 18** laat een overzicht zien van 41 websites die, blijkens het onderzoek van dr. Bashir (**Productie 16**), gebruik maken van de cookies van Oracle en/of Salesforce. Daaruit volgt dat zeker 16 websites in het geheel geen melding maken van het gebruik van de cookies of diensten van Oracle en/of. Nog eens 4 websites plaatsen daarbij geen link naar de privacy documentatie van Oracle en/of Salesforce en nog eens 11 websites plaatsen wel een link, maar naar het verkeerde document. Via 31 van de 41 websites is het daarmee niet mogelijk om überhaupt bij de relevante informatie van Oracle en Salesforce terecht te komen. In **Productie 28** is een aantal voorbeelden opgenomen van de wijze waarop partijen wijzen op het gebruik van cookies op hun website.

381. Wanneer wel informatie wordt aangeboden door de klanten en/of partners van Oracle en Salesforce, gebeurt dat overwegend in verschillende lagen. In de meest gunstige opzet ziet dat er als volgt uit:

a. De eerste informatie-laag is zogenaamde *cookie banner* die verschijnt wanneer de betrokkene een website voor het eerst bezoekt. Een cookie banner is doorgaans een balk onder of bovenaan de pagina, waarbij de bezoeker kan kiezen of hij deze sluit of laat staan. De balk bevat slechts beperkte informatie, zoals dat de website cookies voor advertentiedoeleinden gebruikt. Verder bevat de balk vaak een link die verwijst naar meer informatie over cookies.

[264] Artikel 29 werkgroep, Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679, 3 oktober 2017, zoals laatstelijk gewijzigd en vastgesteld op 6 februari 2018, WP251, rev.01 ('WP251 Profilering'), p. 14 en 15.

b. Wanneer de betrokkene in de cookie banner op die link (vaak met een benaming zoals "meer informatie" of "cookie policy") klikt, wordt hij doorgeleid naar een document met, als het goed is, (tevens) informatie over de cookies die via de website van de klanten en/of partner worden geplaatst ("**Partner Cookie Policy**").

c. De Partner Cookie Policy bevat in het optimale scenario informatie over alle cookies, zoals functionele, analytische en advertentie cookies, die via de website geplaatst kunnen worden, waaronder die van Oracle en Salesforce, met daarbij een link naar relevante informatie van Oracle en Salesforce. De klanten en/of partners delegeren de informatievoorziening op hun beurt weer dus aan Oracle en Salesforce. Het op deze manier verwijzen naar de documentatie van Oracle en Salesforce alsmede naar tal van andere partijen voldoet op zichzelf al niet aan het vereiste dat toestemming "geïnformeerd" moet zijn.

382. Dat sprake is van handelen in strijd met dit vereiste, blijkt te meer nu in de documentatie van Oracle en Salesforce slechts enige versnipperde informatie is opgenomen met betrekking tot hun cookies.

383. Oracle geeft in het geheel niet aan voor welke specifieke verwerkingen zij cookies plaatst en gebruikt voor marketingdoeleinden. Oracle vermeldt slechts dat cookies gebruikt worden:

> "to recognize you and/or your device(s) on, off and across different services and devices for the purposes specified in Section 5 above."
>
> En:
>
> "We or our Oracle Marketing & Data Cloud partners may use cookies to, among other things, track user trends and collect information about how you use our customers' sites or interact with advertising."[265]

384. Informatie over de cookienaam, levensduur van de cookie en wie de cookie plaatst ontbreekt.

385. Salesforce vermeldt slechts dat Cookies gebruikt worden en dat daarin een "unique, pseudonymized Audience Studio user ID" (in wezen een Cookie ID) staat opgenomen. Wat er met deze cookies wordt gedaan, vermeldt zij niet.[266] Eveneens ontbreekt informatie over de cookienaam en wie de cookie plaatst. Salesforce vermeldt wel de levensduur van de cookie.

386. Beide partijen vermelden niets over het koppelen van Cookie IDs met andere partijen in het kader van cookie syncing zoals beschreven in het feitelijke deel hierboven.

387. Duidelijk is dat deze wijze van informatieverstrekking zelfs in het meest gunstige geval in het geheel niet duidelijk maakt aan de betrokkene wat hij kan verwachten. De betrokkene zal zich door een eindeloze lijst van technische cookie-informatie van een veelheid aan partijen heen moeten worstelen en steeds door moeten klikken naar de informatie van de betrokken derde partijen. Op deze wijze kan niet inzichtelijk worden welke gegevens precies door welke partijen

[265] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, "12. What cookies, pixel tags and other similar technologies do we use?", geraadpleegd op 24 juli 2020.
[266] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder "HTTP Cookies", geraadpleegd op 27 juli 2020 (tevens **Productie 23.d**).

worden verzameld en waarvoor zij ze gebruiken. De wijze waarop de informatie beschikbaar wordt gemaakt voldoet onder meer niet aan het toegankelijkheidsvereiste.[267]

388. Bovendien bevat de informatie niet alle vereiste elementen. Zo kan de betrokkene niet vaststellen wie de (gezamenlijk) verantwoordelijken zijn en voor welke doeleinden zij de gegevens precies gebruiken.[268]

389. Voorts blijkt uit **Productie 18** dat slechts 7 van de 41 onderzochte websites de mogelijkheid biedt om toestemming per ad tech partij te geven. Voor de overige 34 websites is het alles of niets. Bij veel websites betekent dit ook gelijk dat uitwisseling van persoonsgegevens met schrikbarende hoeveelheden ad tech partners toegestaan wordt. Zo deelt RTL, de beheerder van rtlnieuws, buienradar en videoland, naar eigen zeggen gegevens met 250 ad tech partners.

390. Opvallend is verder dat zelfs na bestudering van alle mogelijk relevante documentatie, waaronder cookie policies van de partners en de beschikbare privacy documentatie van Oracle en Salesforce, onduidelijk blijft hoe de persoonsgegevens in het RTB ecosysteem precies worden verzameld, verrijkt, gecombineerd en gedeeld. Het is daardoor voor betrokkenen niet duidelijk wat de gevolgen van de verwerking (die mede profilering omvat) kunnen zijn.

391. Wanneer we specifiek kijken naar de informatie die Oracle en Salesforce zelf beschikbaar maken, blijkt dat deze moeilijk te begrijpen en onvolledig is (**Productie 22 en Productie 23**). Een gedeelte van de Salesforce informatie is bovendien in zijn geheel niet beschikbaar op de Nederlandse website en zeer moeilijk te vinden voor Nederlandse internetgebruikers (zie paragraaf 4.3.1.2). Zelfs indien betrokkenen de informatie zouden bereiken, hetgeen niet aannemelijk is, dan nog is het niet begrijpelijk wat de consequentie is van het geven van toestemming.

392. In de informatie op Oracle's website, blijven veel aspecten van Oracle's verwerkingsoperatie ongespecificeerd. Zo blijft het onduidelijk dat Oracle niet alleen online maar ook offline gedrag monitort en hoe zij gegevens verrijkt met grote hoeveelheden informatie uit een veelvoud van bronnen. Daarmee maakt zij onder meer niet duidelijk welke (soort) gegevens zij verwerkt.

393. Voor de Salesforce website geldt dat Nederlandse bezoekers automatisch naar de Nederlandse pagina van de website worden geleid. Die bevat zoals hiervoor omschreven nauwelijks informatie over de DMP dienst van Salesforce. Slechts op de Engelstalige versie is enige specifieke informatie over de onderhavige dienstverlening beschikbaar. Ook hieruit blijkt niet welke informatie Salesforce precies verzamelt, uit welke bronnen, met wie zij de gegevens deelt en voor welke doeleinden de gegevens gebruikt worden.

394. Gezien het voorgaande wordt niet aan het vereiste van geïnformeerde toestemming voldaan.

(iv) Ondubbelzinnige wilsuiting

395. Ten vierde is vereist dat toestemming wordt gegeven door middel van een ondubbelzinnige wilsuiting. Het moet gaan om een verklaring van betrokkene of een andere ondubbelzinnige actieve handeling waaruit blijkt dat de betrokkene daarmee zijn toestemming voor een specifieke verwerking wenst te geven. Die handeling moet opzettelijk zijn. Vooraf aangevinkte

[267] EDPB Guidelines 05/2020 Consent, p. 16.
[268] EDPB Guidelines 05/2020 Consent, p. 16, par. 68.

opt-in vakjes zijn onrechtmatig, en ook stilzwijgen, inactiviteit of het doorgaan met het gebruik van een dienst of website zijn onvoldoende.[269] Het kan in die gevallen immers niet worden uitgesloten dat de betrokkene de informatie niet eens heeft opgemerkt of gelezen.[270]

396. Het HvJEU heeft in de zaak *Planet49* benadrukt dat een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting in ieder geval een "ondubbelzinnige actieve handeling" vereist. Een website die gebruik maakt van een vooraf aangevinkte opt-in vakjes voldoet daar niet aan.

> *"62. In verordening 2016/679 wordt nu dus uitdrukkelijk actieve toestemming voorgeschreven. In dit verband moet worden opgemerkt dat volgens overweging 32 van deze verordening de toestemming met name kan worden uitgedrukt door te klikken op een vakje bij een bezoek aan een website. Daarentegen sluit deze overweging uitdrukkelijk uit dat „stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit" als toestemming mogen gelden."*[271]

397. Hetzelfde geldt voor websites die een "cookiewall" hanteren, toestemming afleiden uit het doorgaan met het bezoeken van een website of alleen de mogelijkheid bieden bezwaar te maken. Dergelijke toestemming voldoet niet aan het criterium van de ondubbelzinnige wilsuiting, omdat geen sprake is van een actieve of opzettelijke handeling.[272]

398. **Productie 18** laat een overzicht zien van de websites die, blijkens het onderzoek van dr. Bashir (**Productie 16**), gebruik maken van de cookies van Oracle en/of Salesforce. Het overzicht laat zien dat een groot deel van de websites niet op juiste wijze toestemming vraagt en/of informatie verstrekt over de verwerking van persoonsgegevens door Oracle en Salesforce. Van de 41 websites plaatsen 16 websites cookies direct wanneer de internetgebruiker de website bezoekt, dat wil zeggen: voordat toestemming wordt gegeven. 9 websites maken gebruik van een cookiewall, 32 van een banner. Van de websites die gebruik maken van een banner, leiden 9 toestemming af uit doorgaan met het bezoeken van de website zonder de mogelijkheid te bieden om cookies te weigeren. Daar komt nog bij dat slechts twee websites de mogelijkheid bieden om tracking cookies net zo gemakkelijk te weigeren als toe te staan, namelijk met één klik in de cookiebanner. Op alle andere websites die überhaupt een mogelijkheid bieden om cookies te weigeren, moet de internetgebruiker meerdere keren klikken.

399. Zelfs als de betrokkene daadwerkelijk op "akkoord" of "toestemming" moet klikken, kan niet gezegd worden dat hij daarmee daadwerkelijk zijn wil uit voor een specifieke verwerking gebaseerd op een volledige en specifieke waarschuwing voor de gevolgen van het geven van toestemming. De betrokkene moet zich, zoals hiervoor omschreven, een weg banen door verschillende informatielagen en verschillende documenten van allerlei verschillende partijen (voor zover deze documentatie al daadwerkelijk wordt verstrekt). Oracle en Salesforce hebben de informatieverstrekking hiermee zodanig gestructureerd dat een betrokkene in wezen niet in staat is om ondubbelzinnig aan te geven waarmee hij instemt. Op "akkoord" of

[269] EDPB Guidelines 05/2020 Consent, p. 18, par. 79; zie overweging 32 AVG en tevens HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*), r.o. 44 t/m 64.
[270] HvJEU 1 oktober 2019, C—673/17, ECLI:EU:C:2019:801 (*Planet49*), r.o. 55.
[271] HvJEU 1 oktober 2019, C—673/17, ECLI:EU:C:2019:801 (*Planet49*).
[272] EDPB Guidelines 05/2020 Consent, p. 18.

"toestemming" klikken in relatie tot RTB geeft in feite niet meer aan dat dat de betrokkene zijn wil uit om verder te willen browsen.

Overige eisen voor geldige toestemming

400. De AVG stelt een aantal aanvullende eisen aan toestemming.

401. Ten eerste rust op de verantwoordelijke de plicht om te kunnen aantonen dat de betrokkene toestemming heeft gegeven (artikel 7 lid 1 en overweging 42 AVG). Daarbij moet de verantwoordelijke ook kunnen aantonen dat de betrokkene geïnformeerd is en dat de werkstroom voor het verkrijgen van toestemming voldeed aan alle hiervoor genoemde eisen.[273] De verantwoordelijke zal onder meer moeten kunnen aantonen welke informatie is verstrekt, op welke wijze en hoe de betrokkene zijn wil heeft geuit.

402. Ten tweede stelt de AVG aan toestemming de eis dat betrokkene deze te allen tijde moet kunnen intrekken (artikel 7 lid 3 AVG). Daarbij moet het intrekken van toestemming even eenvoudig zijn als het geven ervan (ook artikel 7 lid 3 AVG). Wanneer toestemming dus door middel van één muisklik wordt verkregen, moet de betrokkene die toestemming dus ook met één muisklik, of in ieder geval even eenvoudig, kunnen intrekken.[274]

403. Na intrekking van de toestemming zal de verantwoordelijke alle gegevensverwerkingen die gebaseerd waren op toestemming moeten stoppen. De persoonsgegevens moeten worden gewist, tenzij ze tevens voor een ander doeleinde met een andere rechtsgrond worden verwerkt. Die rechtsgrond moet er in dat geval al zijn geweest toen de verwerking aanving, en in dit kader is ook van belang dat vanaf het begin duidelijk en transparant is geweest welke gegevens voor welke doeleinden worden verwerkt en welke rechtsgrond daarvoor wordt ingeroepen. De verantwoordelijke kan niet nadat de toestemming wordt ingetrokken of ongeldig blijkt, overstappen op een andere rechtsgrond.[275]

404. Het eenvoudig kunnen intrekken van toestemming is een noodzakelijk aspect van geldige toestemming. Nu Oracle en Salesforce deze mogelijkheid niet bieden, is geen sprake van geldige toestemming.

405. Ten slotte, rust zelfs indien de verantwoordelijke zich beroept op de grondslag toestemming de plicht op de verwerkingsverantwoordelijke om een belangenafweging te maken, waarbij rekening moet worden gehouden met de beginselen van proportionaliteit en subsidiariteit. Het beginsel van proportionaliteit brengt met zich mee dat de inbreuk op de belangen van betrokkene niet onevenredig mag zijn in verhouding tot het doel van de verwerking. Op grond van het beginsel van subsidiariteit is vereist dat het doel niet op andere, voor de betrokkene minder nadelige, wijze kan worden bereikt. Bij de afweging moeten alle omstandigheden van het geval in aanmerking worden genomen.[276]

406. In het onderhavige geval geldt dat Oracle en Salesforce grote hoeveelheden gegevens verzamelen uit verschillende bronnen en deze gegevens combineren, verrijken, analyseren en de gegevens en de daarmee opgestelde profielen delen met een onbepaald aantal derden. Het

[273] EDPB Guidelines 05/2020 Consent, p. 22-23.
[274] EDPB Guidelines 05/2020 Consent, p. 23-24.
[275] EDPB Guidelines 05/2020 Consent, p. 24.
[276] HR 9 september 2011, ECLI:NL:HR:2011:BQ8097 (*Santander*), r.o. 3.3.

doel van die verwerkingen is zuiver commercieel. De inbreuk die hiermee gemaakt wordt is volstrekt onevenredig in verhouding tot dat doel. Ook geldt dat het doel, het succesvol adverteren, ook op andere wijze kan worden bereikt die voor betrokkenen veel minder nadelig is.

4.6.2.4 Conclusie ten aanzien van rechtmatigheid

407. Uit het voorgaande volgt dat Oracle en Salesforce niet voldoen aan de vereisten om een beroep te kunnen doen op toestemming als grondslag voor de verwerking. Daarbij wijst de Stichting er nogmaals op dat de plicht en bewijslast om aan te tonen dat wel aan alle vereisten zou zijn voldaan rust op Oracle en Salesforce.[277] Daarvoor geldt dat het enkel verwijzen naar compliance documentatie op dit punt niet voldoende is. Nu Oracle en Salesforce de cookies plaatsen, zullen zij moeten aantonen dat van de betrokkenen van wie zij daarmee gegevens verzamelen daadwerkelijk toestemming is verkregen en dat deze toestemming voldoet aan alle daarvoor geldende eisen.

408. Oracle en Salesforce handelen hiermee in strijd met het rechtmatigheidsbeginsel van de AVG (artikel 5 lid 1 sub a en 6 AVG), nu zij geen toereikende grondslag voor de verwerking hebben. Voorts handelen zij hiermee in strijd met artikel 11.7a Tw. Zij plaatsen immers cookies op de apparatuur van eindgebruikers en lezen informatie uit, en verkrijgen daar geen geldige toestemming voor. Het handelen in strijd met de AVG en Tw, kwalificeert (tevens) als handelen in strijd met een wettelijke verplichting en levert daarom jegens betrokkenen een onrechtmatige daad op.

*4.6.3 Verwerking niet transparant*

409. Oracle en Salesforce verstrekken voorts onvoldoende informatie over hun verwerkingen om aan de vereisten van de AVG te voldoen. Ook daarmee handelen zij in strijd met de AVG en Tw.

410. Transparantie is als fundamenteel beginsel voor de bescherming van persoonsgegevens opgenomen in artikel 5 lid 1 sub a AVG.[278] Het transparantievereiste ligt ook ten grondslag aan de hierboven besproken eisen voor geïnformeerde toestemming, maar heeft een bredere toepassing. Het geldt voor iedere verwerking, onafhankelijk van de grondslag. Ook geldt het vereiste om bij gebruik van cookies in overeenstemming met de AVG informatie te verstrekken op grond van artikel 11.7a lid 1 sub a Tw.

411. Transparantie is al heel lang een kernbeginsel van het EU-recht.[279] Transparantie moet ervoor zorgen dat burgers vertrouwen hebben in de processen die hen raken, helpt hen die processen te begrijpen en stelt hen, indien nodig, in staat bezwaar te maken. Ook is transparantie een

[277] Zie EDPB Guidelines 05/2020 Consent, par. 36 en 104.

[278] Artikel 29 werkgroep, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/69, 29 november 2017, zoals laatstelijk gewijzigd en vastgesteld op 11 april 2018, WP260rev.01 en zoals bekrachtigd door de EDPB op 25 mei 2018 ('WP260 Transparantie'), p.5, par. 2.

[279] In artikel 1 van het Verdrag betreffende de Europese Unie ("VEU")**)** wordt bepaald dat besluiten "in zo groot mogelijke openheid en zo dicht mogelijk bij de burger worden genomen"; Artikel 11, lid 2, van het VEU luidt als volgt: "De instellingen voeren een open, transparante en regelmatige dialoog met representatieve organisaties en met het maatschappelijk middenveld"; en in artikel 15 van het Verdrag betreffende de werking van de Europese Unie ("VWEU)" wordt onder meer bepaald dat burgers van de Unie recht hebben op toegang tot documenten van de instellingen, organen en instanties van de Unie, met als doel dat deze instellingen, organen en instanties van de Unie zorgen voor transparantie in hun werkzaamheden.

uitdrukking van het beginsel van eerlijkheid in verband met de verwerking van persoonsgegevens zoals vervat in artikel 8 van het Handvest en is het derhalve een essentieel grondrechtelijk beginsel. Aan de bepaling in artikel 5 lid 1 sub a AVG dat gegevens op een rechtmatige en behoorlijke wijze moeten worden verwerkt, is daarom transparantie toegevoegd als fundamenteel aspect van de beginselen.[280]

412. Transparantie is intrinsiek verbonden aan de behoorlijkheid en de verantwoordingsplicht van artikel 5 lid 2 AVG. De verwerkingsverantwoordelijke moet daarom onder meer kunnen aantonen dat persoonsgegevens ten aanzien van de betrokkene op een transparante manier worden verwerkt.[281]

413. Het transparantievereiste heeft meerdere aspecten, waaronder het verstrekken van informatie over de verwerking van persoonsgegevens, het geven van uitvoering aan de rechten van betrokkenen en de meldplicht datalekken. Voor de onderhavige zaak is met name het eerste aspect van belang, het verstrekken van informatie over de verwerking van persoonsgegevens. De verplichtingen in dat kader worden nader uitgewerkt in onder meer artikel 12, 13 en 14 en overweging 39 AVG.

414. Overweging 39 luidt:

> *"Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Voor natuurlijke personen dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt. Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt. Dat beginsel betreft met name het informeren van de betrokkenen over de identiteit van de verwerkingsverantwoordelijke en de doeleinden van de verwerking, alsook verdere informatie om te zorgen voor behoorlijke en transparante verwerking met betrekking tot de natuurlijke personen in kwestie en hun recht om bevestiging en mededeling te krijgen van hun persoonsgegevens die worden verwerkt. Natuurlijke personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens, alsook van de wijze waarop zij hun rechten met betrekking tot deze verwerking kunnen uitoefenen. […]"*

4.6.3.1 Algemene eisen transparantie

415. Artikel 12 AVG bevat een aantal algemene regels voor het verstrekken van informatie aan de betrokkene. Zo moet de informatie onder meer beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn en in duidelijke en eenvoudige taal zijn opgesteld, en kan elektronisch worden verstrekt. Dit geldt volgens overweging 58 in het bijzonder voor situaties, waarin het vanwege het grote aantal actoren en de technologische complexiteit voor een

[280] In de Databeschermingsrichtlijn (Richtlijn 95/46/EG) werd transparantie alleen genoemd in overweging 38, als onderdeel van de vereiste om gegevens op een behoorlijke wijze te verwerken, maar niet uitdrukkelijk in het overeenkomstige artikel 6, lid 1, onder a).
[281] Zie tevens WP260 Transparantie, p. 5.

betrokkene moeilijk is om te begrijpen of, door wie en met welk doel zijn persoonsgegevens worden verzameld. Online advertenties worden hier specifiek als voorbeeld genoemd van een dergelijke situatie.

416. De verantwoordelijke moet passende maatregelen nemen om ervoor te zorgen dat de betrokkene de informatie ontvangt (artikel 12 lid 1 AVG).

417. Hiervoor is reeds behandeld (zie onder meer randnummer 380) dat Oracle en Salesforce er bij het plaatsen van cookies op randapparatuur van Nederlandse internetgebruikers niet voor zorgen dat betrokkene de relevante informatie ontvangt. In veel gevallen wordt op de websites via welke Oracle en Salesforce hun cookies plaatsen niet verwezen naar Oracle en Salesforce of hun documentatie over de verwerking van persoonsgegevens. De toepasselijkheid van de beschikbare privacy documentatie van Oracle en Salesforce is daarmee op zichzelf al onduidelijk.

418. In dit verband zij opgemerkt dat Oracle de informatie over haar DMP activiteiten met name geeft in het Privacybeleid voor Oracle Data Cloud[282] en het Privacybeleid voor AddThis[283] (zie paragraaf 4.3.1.1).

419. Voor Salesforce geldt dat de privacy documentatie op de Nederlandstalige website van Salesforce nauwelijks informatie bevat over de DMP activiteiten (zie paragraaf 4.3.1.2). De Engelstalige versie van de website bevat de Salesforce Audience Studio Privacy Policy,[284] waarin meer informatie wordt verstrekt. Een Nederlandse internetgebruiker wordt wanneer hij de website van Salesforce bezoekt echter niet doorgeleid naar de Engelstalige pagina van de website. Een Nederlandse internetgebruiker zal de Audience Studio Privacy Policy dus nooit te zien krijgen, terwijl Salesforce in het kader van haar DMP dienst wel degelijk gegevens verzamelt via websites die op Nederlandse internetgebruikers gericht zijn en in de Nederlandse taal zijn opgesteld.

Niet beknopt, transparant en begrijpelijk

420. De door Oracle en Salesforce verstrekte informatie is niet beknopt, transparant en begrijpelijk. WG29 verduidelijkt in de richtsnoeren met betrekking tot transparantie dat dit onder meer inhoudt dat verwerkingsverantwoordelijken de informatie op een efficiënte en bondige wijze moeten weergeven om informatiemoeheid te voorkomen.[285] Aan deze vereisten wordt niet voldaan.

421. De verwerking van persoonsgegevens in het online advertentieproces wordt gekenmerkt door onoverzichtelijkheid en onduidelijkheid door de veelheid aan betrokken partijen, doeleinden waarvoor gegevens worden verwerkt en de onverwachte combinatie van een groot aantal persoonsgegevens uit verschillende bronnen. Deze onoverzichtelijkheid en onduidelijkheid kenmerkt ook de informatie die in dit kader aan betrokkenen wordt verstrekt. In het beste geval worden internetgebruikers eerst door middel van een cookie banner op de website

[282] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).
[283] https://www.oracle.com/legal/privacy/addthis-privacy-policy.html, geraadpleegd op 23 april 2020.
[284] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, geraadpleegd op 23 april 2020 (tevens **Productie 23.d**).
[285] WP260 Transparantie, p. 7, par. 8.

geïnformeerd, om vervolgens via de Partner Cookie Policy's door te kunnen klikken naar de privacy documentatie van Oracle en Salesforce (randnummer 381). Van beknoptheid is daarbij geen sprake alleen al omdat het om meerdere lagen gaat waarin een veelheid aan informatie wordt verstrekt.

422. Zowel Oracle als Salesforce geven bijvoorbeeld aan gebruik te maken van datapartner ShareThis. ShareThis levert sociale media deelknoppen en verzamelt tegelijkertijd persoonsgegevens die gebruikt worden voor gepersonaliseerde advertenties. Als een betrokkene op een website komt die ShareThis knoppen gebruikt, dan moet de betrokkene op die website naar het privacybeleid of cookiebeleid navigeren. Daar staat dan in sommige gevallen een hyperlink naar het uitgebreide privacy statement van ShareThis.[286] In het privacy statement van ShareThis staat onder het kopje "Data Sharing or Disclosure, Recipients of Your Data", aangegeven dat de klanten onder meer Advertisers, Publishers, Data management platforms, advertising technology partners en data brokers zijn. ShareThis vermeldt vervolgens dat deze partijen zelfstandig verwerkingsverantwoordelijke zijn en verwijst ter illustratie naar de privacy statements van enkele van haar klanten:

> Where the GDPR applies to Usage Data and Profile Information and we share this data with our Customers, our Customers are independent controllers in relation to their processing of such data and they process it in accordance with their own privacy policies.
>
> Customers may share the data which they process with other third parties who are not mentioned in this Privacy Notice, in accordance with their own privacy policies. As an example, they may use third party service providers to display advertising or other content on their behalf.
>
> Please review some of our Customer's privacy policies for more information:
>
> LiveRamp: https://liveramp.com/privacy/
> AppNexus: https://www.appnexus.com/platform-privacy-policy
> Eyeota : https://www.eyeota.com/privacy-policy
> Oracle: https://www.oracle.com/legal/privacy/privacy-policy.html
> Lotame: https://www.lotame.com/about-lotame/privacy/
> Nielsen: https://www.nielsen.com/ssa/en/legal/privacy-policy/

423. Oracle staat hier wel genoemd, Salesforce niet.[287] De betrokkene heeft op dit moment geen volledig beeld meer van de partijen die beschikking krijgen over zijn persoonsgegevens. Als de betrokkene vervolgens wil weten hoe Oracle zijn persoonsgegevens verwerkt, dan kan hij op de link achter Oracle klikken. Deze link leidt echter naar het verkeerde privacybeleid, namelijk het Algemeen privacybeleid van Oracle. In het Algemeen privacybeleid van Oracle staan niet de verwerkingen beschreven waar het hier om gaat. Die staan beschreven in het Privacybeleid voor Oracle Data Cloud. De betrokkene kan dat zelf niet of nauwelijks ontdekken en komt

[286] Sharethis, *Privacy,* 28 juli 2020, te raadplegen via: https://sharethis.com/privacy/.
[287] Uit onderzoek van Cookiebot blijkt het aantal partijen waarmee ShareThis gegevens deelt aanmerkelijk groter; zie hiervoor Cookiebot, "Ad Tech Surveillance on the Public Sector Web", 2019, te raadplegen via: https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf.

daarmee nooit op de juiste informatie terecht over de verwerking van zijn persoonsgegevens door Oracle.

424. Opvallend is verder dat ShareThis Salesforce niet noemt, terwijl Salesforce aangeeft gebruik te maken van SharisThis als partner. Verder is opvallend dat ShareThis haar klanten (waaronder dus in ieder geval Oracle) aanmerkt als zelfstandige verwerkingsverantwoordelijke terwijl Oracle en Salesforce zich op het standpunt proberen te stellen slechts verwerker te zijn.[288]

425. Betrokkenen kunnen door deze wijze van informeren van tevoren de reikwijdte en de gevolgen van de verwerking niet bepalen en worden later verrast door andere manieren waarop hun persoonsgegevens zijn gebruikt. WG29 benadrukt dat waar het complexe, technische of onverwachte gegevensverwerkingen betreft ook afzonderlijk, in ondubbelzinnige taal, moet worden uitgelegd wat de belangrijkste gevolgen van de verwerking zullen zijn. Beschreven moet worden welk effect een specifieke verwerking die in de privacy documentatie wordt beschreven zal hebben op een betrokkene.[289] Dit zou eigenlijk al in de eerste of tweede informatielaag moeten gebeuren.

426. Een ander voorbeeld hiervan is het proces van cookie syncing. Oracle en Salesforce wisselen op grote schaal Cookie IDs uit met andere partijen in de adtech markt, zoals beschreven onder paragraaf 3.2.6. Door het uitwisselen van Cookie IDs kunnen al deze adtech partijen met elkaar communiceren over de betrokkene en waar nodig nog meer persoonsgegevens uitwisselen. Oracle en Salesforce doen dit op grote schaal, als blijkt uit het onderzoek van Dr. Bashir (**Productie 16**).

427. Via de 28 websites (van de 100 geteste websites populaire Nederlandse websites) waarop Oracle cookies aanwezig waren, synchroniseert Oracle cookies met 12 partijen. Als toegelicht in de feiten (randnummer 138) gaat het onder meer om andere datahandelaren en DMPs, waaronder Salesforce, alsook id5 dat gespecialiseerd is in efficiënte cookiesynchronisatie op grote schaal. Van het gebruik van deze, in de RTB markt essentiële, techniek en de partijen waarmee de persoonsgegevens, ten minste Cookie IDs, gedeeld worden vermeldt Oracle niets.

428. Via de 31 websites (van de 100 geteste websites populaire Nederlandse websites) waarop Salesforce cookies aanwezig waren, synchroniseert Salesforce cookies met 23 partijen. Als toegelicht in de feiten (randnummer 140) gaat het hier eveneens om andere datahandelaren en DMPs, waaronder Oracle en Google. Ook Salesforce maakt geen enkele vermelding van het gebruik van deze techniek en de vele partijen waarmee persoonsgegevens uitgewisseld worden.

429. Het effect is voor betrokkenen niet te overzien, met name niet omdat niet duidelijk wordt gemaakt hoe veelomvattend de verwerkingen, datasets en profielen zijn, welke partijen hier allemaal bij betrokken zijn en hoeveel gegevens met elkaar worden gecombineerd. De betrokkene wordt juist misleid doordat een tegenovergestelde indruk wordt gewekt: er worden voorbeelden gegeven die impliceren dat sprake is van voor de hand liggende één op één aanbiedingen die het duidelijke gevolg zijn van een handeling bij de partij die nu een vergelijkbare aanbieding doet. Zo staat in het Privacybeleid voor Oracle Data Cloud:

[288] Sharethis, *Privacy,* 28 juli 2020, te raadplegen via: https://sharethis.com/privacy/.
[289] WP260 Transparantie, p. 8.

> *"iii. Zodat onze Oracle Data Cloud-klanten hun producten en services kunnen personaliseren, waaronder siteoptimalisatie, e-mailpersonalisatie en optimalisatie van dynamische marketing en advertenties.*
>
> *Voorbeeld: Als u eerder interesse hebt getoond in een reis naar Hawaï en u vervolgens de website van een reisbureau bezoekt, kan het reisbureau op maat gesneden aanbiedingen voor vakanties naar Hawaï op de homepage weergeven."*[290]

430. Op geen enkele manier wordt duidelijk dat deze aanbieding het gevolg is van de hiervoor beschreven verwerkingen, die onder meer inhouden dat gegevens uit verschillende bronnen met elkaar worden gecombineerd en dat gegevens met verschillende partijen worden gedeeld. De belangrijkste informatie, namelijk dat gegevens uit verschillende bronnen worden verzameld, gecombineerd en verrijkt, geanalyseerd, en vervolgens worden gedeeld met een onbekend aantal derde partijen voor advertentiedoeleinden, wordt niet beknopt, transparant of begrijpelijk verstrekt.

431. Dat hierbij bovendien sprake is van profilering zou ook uitdrukkelijk kenbaar moeten worden gemaakt moeten worden, zo volgt onder meer uit overweging 60 AVG:

> *[...] "Voorts moet de betrokkene worden geïnformeerd over het bestaan van profilering en de gevolgen daarvan." [...]*

<u>Geen duidelijke en eenvoudige taal</u>

432. Evenmin is sprake van duidelijke en eenvoudige taal. Er wordt gebruik gemaakt van niet-concrete zinsconstructies. WG29 overweegt als volgt ten aanzien van het taalgebruik:

> *"Constructies of woorden als "kan", "zou kunnen", "bepaalde", "vaak" en "mogelijk" zouden eveneens moeten worden vermeden. Wanneer verwerkingsverantwoordelijken ervoor kiezen om onbepaalde taal te gebruiken, zouden ze, in overeenstemming met het beginsel van de verantwoordingsplicht, moeten kunnen aantonen waarom het gebruik van dergelijke taal niet kon worden vermeden en hoe de gebruikte taal de behoorlijkheid van de verwerking niet ondergraaft. Paragrafen en zinnen dienen goed gestructureerd te zijn, waarbij stippen of streepjes worden gebruikt om hiërarchische relaties aan te geven.*
>
> *Werkwoorden zouden in de actieve vorm moeten worden gebruikt, en niet in de passieve vorm, en overbodige zelfstandig naamwoorden zouden moeten worden vermeden. De informatie die aan een betrokkene wordt verstrekt zou geen te juridische, technische of specialistische taal of terminologie moeten bevatten. Wanneer de informatie in een of meer talen wordt vertaald, dient de verwerkingsverantwoordelijke ervoor te zorgen dat alle vertalingen getrouw zijn en dat de woordkeuze en zinsbouw in de andere taal of talen correct zijn, zodat de vertaalde tekst goed is te volgen en te begrijpen. (Wanneer de*

[290] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder '5. Waarom en hoe gebruiken we uw persoonlijke informatie?: A) Om klanten en partners van Oracle Marketing & Data Cloud in staat te stellen producten en services te marketen op basis van uw interesses, I', geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).

*verwerkingsverantwoordelijke zich richt tot betrokkenen die een andere taal spreken, moet een vertaling in die talen worden verstrekt.)"*[291]

433. In de Audience Studio Privacy Policy van Salesforce wordt veel gebruik gemaakt van constructies en woorden die volgens WG29 moeten worden vermeden. Een voorbeeld daarvan is de volgende passage (onderstreping advocaat):

> *"The Customer typically uses this data on our Platform to deliver targeted advertising campaigns both on the Customer Site and App as well as off their sites and apps. For example, Customers may use the Platform to help them find interested users and to deliver ads that attempt to bring those users back to the Customer's Site and App. Where our systems can reasonably infer that a particular computer and/or mobile device belong to the same user or household, we may store such information for use on the Platform. The data stored on our Platform may be combined with third-party data (for example, geolocation data provided by a vendor) in order to better target advertisements, to enable Customers to better understand users across multiple computers and devices, and for ad delivery and reporting purposes."*[292]

434. Ook in het Privacybeleid voor Oracle Data Cloud van Oracle[293] wordt gebruik gemaakt van dermate vage constructies en woorden en technische en specialistische terminologie dat de betrokkene geenszins kan overzien welke van haar gegevens nu precies voor welke doeleinden worden gebruikt en door welke partijen.

435. Een voorbeeld daarvan is de volgende passage (onderstreping advocaat):

> *"iii. Zodat onze Oracle Data Cloud-klanten hun producten en services kunnen personaliseren, waaronder siteoptimalisatie, e-mailpersonalisatie en optimalisatie van dynamische marketing en advertenties.*
>
> *Voorbeeld: Als u eerder interesse hebt getoond in een reis naar Hawaï en u vervolgens de website van een reisbureau bezoekt, kan het reisbureau op maat gesneden aanbiedingen voor vakanties naar Hawaï op de homepage weergeven.*
>
> *iv. Voor het koppelen van profielen en interessesegmenten zodat klanten en partners van Oracle Marketing & Data Cloud uw interessesegmenten kunnen koppelen in de verschillende browsers en/of apparaten die u mogelijk gebruikt voor de doelen die in deze sectie worden beschreven.*
>
> *Voorbeeld: U bent geïnteresseerd in vakanties die worden aangeboden door een reisbureau en hebt op hun online reclame geklikt. U bent aangemeld bij meerdere apparaten (uw desktopcomputer, smartphone en tablet) met dezelfde aanmelding. Oracle-partners hebben vastgesteld dat u waarschijnlijk dezelfde gebruiker op deze*

[291] WP260 Transparantie, p. 10-11.
[292] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder 'How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform', geraadpleegd op 21 juli 2020 (tevens **Productie 23.d**).
[293] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).

*apparaten bent. Het reisbureau kan vakantieaanbiedingen aan u tonen op deze verschillende apparaten (via een onidenticeerbaar gemaakte cookie-id).”*[294]

Niet gemakkelijk toegankelijk

436. Het vereiste dat de informatie gemakkelijk toegankelijk moet zijn, houdt in dat de betrokkene niet zelf op zoek hoeft te gaan naar de informatie. Het moet voor betrokkene onmiddellijk duidelijk zijn waar en hoe hij de informatie kan vinden.[295] Uit artikel 13 en 14 AVG blijkt voorts dat de verantwoordelijke de daar genoemde informatie moet *verstrekken*. Dat betekent dat de verantwoordelijke actief stappen moet nemen om de informatie aan de betrokkene te bezorgen of de betrokkene actief naar de locatie van de informatie moet dirigeren. Het mag niet zo zijn dat de betrokkene zelf op zoek moet gaan naar de relevante informatie.[296]

437. Zoals hiervoor in het kader van toestemming al uiteen is gezet, is de informatie van Oracle en Salesforce niet gemakkelijk toegankelijk.

438. Dat komt om te beginnen doordat Oracle en Salesforce de verplichting om te informeren van internetgebruikers over de verwerkingen door Oracle, Salesforce en alle andere betrokken adtech primair delegeren aan hun klanten.

439. Salesforce doet dat als volgt::

*“**Notice to Customer’s Users***

*Customer is required to clearly and conspicuously post notice (e.g., in its privacy policy) to customer’s users regarding customer’s relationship with Salesforce and other third-party advertising technology companies. Such notice must contain a link to the consumer opt-out mechanism relevant in each jurisdiction, such as the applicable NAI- or DAA-compliant consumer opt-out mechanism.”*[297]

440. Voorts worden betrokkenen in het beste geval via een cookie banner en de Partner Cookie Policy naar de privacy documentatie van een groot aantal betrokken derde partijen, waaronder Oracle en/of Salesforce, gestuurd. Daar moeten zij vervolgens op zoek naar de voor hen relevante informatie (randnummers 381 e.v.). Voor zover een dergelijke structuur al zou voldoen aan het vereiste van toegankelijkheid, geldt dat bij een gelaagde structuur reeds in de eerste informatielaag – in dit geval dus de cookie banner– informatie moet worden verstrekt over de identiteit van alle gezamenlijk verantwoordelijken en alle doeleinden waarvoor zij verwerken.[298]

441. Ook zal de cookie banner informatie moeten bevatten over het verrijken, combineren, profileren, delen en verstrekken van de gegevens nu de betrokkene dat zonder die informatie niet zal verwachten en juist deze verwerkingen (en hun omvang) het grootste effect op de privacy van betrokkenen hebben. Daarnaast moet de cookie banner informatie bevatten over

[294] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, “5. Waarom en hoe gebruiken we uw persoonlijke informatie?: A) Om klanten en partners van Oracle Marketing & Data Cloud in staat te stellen producten en services te marketen op basis van uw interesses, I”, geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).
[295] WP260 Transparantie, p. 8, par. 11 en p. 21 par. 33.
[296] WP260 Transparantie, p. 21 par. 33.
[297] https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/audience-studio-notices-and-license-information.pdf, p. 4, geraadpleegd op 24 juli 2020.
[298] WP260 Transparantie, p. 22 par. 36.

de rechten van betrokkenen.[299] Dit is niet hoe de informatievoorziening in de praktijk wordt ingericht. De cookie banner bevat dergelijke informatie niet en de betrokkene moet eerst een aantal keer verder klikken voor hij eventueel bij dergelijke informatie terecht komt.

442. Een goed voorbeeld van hoe ontoegankelijk de relevante informatie is, is de informatie over het delen van gegevens door middel van cookie syncing, een essentieel onderdeel van de DMP diensten van Oracle en Salesforce (zie hiervoor paragraaf 3.2.6):

443. Een internetgebruiker die op zoek gaat naar informatie over het delen van gegevens door Salesforce zal waarschijnlijk niets vinden nu de op betrokkenen gerichte privacy documentatie deze informatie niet bevat. Informatie hierover kan slechts gevonden worden in de "Audience Studio Notices and License Information" die gericht op de klanten van Salesforce en slechts op de Engelstalige website van Salesforce beschikbaar is (**Productie 23.e en 23.f**). De Nederlandse internetgebruiker die op zoek gaat naar informatie over de verwerking door Salesforce wordt hier echter niet naartoe geleid (zie hiervoor paragraaf 4.3.1.2).

4.6.3.2 Specifieke informatie die verstrekt moet worden

444. Artikelen 13 en 14 AVG beschrijven welke informatie moet worden verstrekt. Artikel 13 AVG ziet op gevallen waarin de persoonsgegevens direct bij de betrokkene zijn verzameld, artikel 14 AVG op gevallen waarin de gegevens uit een andere bron worden verkregen. Dat deze bepalingen ook van toepassing zijn op het vereiste van geïnformeerde toestemming van artikel 11.7a Tw, blijkt ook uit het voornoemde *Planet49*-arrest van het HvJEU:

> *"76 In dit verband moet worden opgemerkt dat artikel 10 van richtlijn 95/46, waarnaar artikel 5, lid 3, van richtlijn 2002/58 en artikel 13 van verordening 2016/679 verwijzen, een opsomming bevat van de informatie die de voor de verwerking verantwoordelijke moet verstrekken aan de betrokkene bij wie hij de op die betrokkene zelf betrekking hebbende gegevens verkrijgt"*[300]

445. De eerste laag van informatie die wordt gebruikt om betrokkenen te informeren dient volgens de Europese toezichthouders de volgende informatie te bevatten:

a. Details van het doel van de verwerking;

b. De identiteit van de verwerkingsverantwoordelijke; en

c. Een beschrijving van de rechten van betrokkenen.[301]

446. Deze informatie moet bij het verzamelen van de gegevens rechtstreeks onder de aandacht van de betrokkene worden gebracht. Daarnaast moet de eerste laag op grond van het behoorlijkheidsbeginsel informatie bevatten over de verwerkingen met het grootste effect op de betrokkene en die voor de betrokkene onverwacht zou kunnen zijn. De betrokkene zou op basis van die informatie reeds in staat moeten zijn om de gevolgen van de verwerking te begrijpen.[302]

[299] WP260 Transparantie, p. 22 par. 36.
[300] HvJEU 1 oktober 2019, C-673/17, ECLI:EU:C:2019:801 (*Planet49*).
[301] WP260 Transparantie, p. 22 par. 36.
[302] WP260 Transparantie, p. 22 par. 36.

447. Hiervoor kwam al aan de orde dat de cookie banners op de websites via welke Oracle en Salesforce cookies worden geplaatst dergelijke informatie niet bevatten (**Productie 28**).

448. Hieronder wordt, voor zover van belang, besproken welke informatie op grond van artikel 13 en 14 AVG moet worden verstrekt en in hoeverre Oracle en Salesforce deze informatie hebben opgenomen in hun privacy documentatie (**Productie 22** en **Productie 23**). Er is daarvoor met name gekeken naar het Privacybeleid voor Oracle Data Cloud van Oracle (**Productie 22.a**) en de Audience Studio Privacy Policy van Salesforce (**Productie 23.d**), nu deze documenten de meeste informatie bevatten over de DMP activiteiten van Oracle en Salesforce. Opnieuw zij benadrukt dat Nederlandse internetgebruikers de Audience Studio Privacy Policy van Salesforce niet eenvoudig kunnen vinden (zie paragraaf 4.3.1.2). Feitelijk verstrekt Salesforce daarmee *geen* informatie over haar DMP verwerkingen aan Nederlandse internetgebruikers. Het navolgende geldt derhalve alleen voor zover het document Salesforce Audience Studio Privacy Policy op de Engelse pagina toch als privacyinformatie in de zin van artikel 13 en 14 moet worden gezien. Ook voor Oracle geldt het navolgende uitsluitend voor zover zij kan aantonen dat het Privacybeleid voor Oracle Data Cloud daadwerkelijk (bijvoorbeeld door middel van een link) aan betrokkenen is verstrekt.

<u>De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger</u>

449. Informatie over de identiteit van de verwerkingsverantwoordelijke moet worden verstrekt zodanig dat de verwerkingsverantwoordelijke gemakkelijk identificeerbaar is.[303] Oracle en Salesforce zijn niet gemakkelijk identificeerbaar als zodanig. Zij worden doorgaans immers niet genoemd in de eerste informatielaag. Evenmin wordt duidelijk gemaakt dat sprake is van gezamenlijke verantwoordelijkheid, terwijl dat wel een bijzonder groot effect heeft op de ingrijpendheid van de verwerking.[304]

450. Oracle stelt ten aanzien van een deel van haar diensten verwerker te zijn (zie randnummers 272 en 273). Voor welke verwerkingen zij zichzelf als verwerker aanmerkt en voor welke als verantwoordelijke is uit haar privacy documentatie echter niet op te maken. Bovendien is al aangegeven dat Oracle wel verantwoordelijke is. Zij zou zich dus ook als zodanig kenbaar moeten maken aan betrokkenen.

451. In tegenstelling tot haar eigen stellingen, wijst Oracle zichzelf in haar privacy documentatie aan als verwerkingsverantwoordelijke. Zij wijst daarbij verschillende partijen aan (zie ook paragraaf 4.4).[305] Daarbij is niet duidelijk wie verantwoordelijk is voor welke verwerkingen.

452. Salesforce lijkt zichzelf ten onrechte enkel als verwerker aan te merken. Dat volgt slechts uit de omstandigheid dat zij op de Engelstalige privacy pagina (**Productie 23.c**) de Audience Studio Privacy Policy (**Productie 23.d**) (onder de naam Salesforce DMP Privacy Policy) onder de kop “Resources in respect of how we protect our customer's data as a processor” heeft

[303] WP260 Transparantie, p. 41
[304] Vgl. WP260, Transparantie, p. 22, par. 36.
[305] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder “2. Reikwijdte” en “3. Wie is verantwoordelijk voor de verwerking van uw persoonlijke informatie?”, geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).

opgenomen. Dit is dus op een pagina waar een Nederlandse internetgebruiker *niet* naartoe wordt geleid.

453. Voor zover Salesforce zou betogen dat dit tevens volgt uit de aanduiding van de verantwoordelijke in haar algemene privacyverklaring (**Productie 23.b**),[306] geldt dat hetgeen daar is opgenomen veel te vaag is om als een dergelijke aanduiding te gelden (zie hierover randnummers 240 t/m 243). Nu het document bovendien daarna op een aantal punten informatie over de DMP dienst bevat (zie paragraaf 4.3.1.2), wekt Salesforce (terecht) de indruk dat zij zichzelf voor die verwerkingen wel degelijk als verwerkingsverantwoordelijke aanmerkt. Welke Salesforce entiteit de verwerkingsverantwoordelijke is, maakt zij daarbij niet duidelijk.

454. Van duidelijke informatie zodanig dat de verwerkingsverantwoordelijke gemakkelijk identificeerbaar is, is geen sprake, zelfs niet wanneer de betrokkene de privacy documentatie van Salesforce daadwerkelijk bereikt.

<u>De contactgegevens van de functionaris gegevensbescherming, indien van toepassing;</u>

455. Salesforce verstrekt in haar Audience Studio Privacy Policy geen informatie over een functionaris gegevensbescherming, terwijl deze gezien haar activiteiten verplicht is op grond van artikel 37 AVG. Uit haar algemene privacyverklaring lijkt overigens te volgen dat Salesforce wel een functionaris heeft aangewezen.[307] Het is opvallend dat zij die in het Audience Studio Privacy Policy niet noemt.

<u>De verwerkingsdoeleinden en grondslag van de verwerking en, indien een beroep wordt gedaan op de grondslag gerechtvaardigd belang, de gerechtvaardigde belangen waarop verantwoordelijke zich beroept;</u>

456. Oracle verstrekt slechts zeer algemene informatie over de doeleinden.

457. In het geval van Oracle werd het doeleinde van de DMP-verwerking (voor zover relevant) tot 11 juni 2020 in respectievelijk de Nederlandse en Engelse versie als volgt beschreven:

> *"We gebruiken uw persoonlijke informatie voor de volgende doeleinden:*
>
> *a) zodat klanten en partners van Oracle Marketing & Data Cloud hun producten en services aan u kunnen aanbieden op basis van uw interesses"*[308] **(Productie 22.a)**
>
> *"We use personal information for the following commercial purposes:*
>
> *a) to help enable Oracle Marketing & Data Cloud customers and partners to market products and services toyou based on your interests"*[309] (**Productie 22.d**)

[306] https://www.salesforce.com/nl/company/privacy/full_privacy/, geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).
[307] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder "13. Contact met ons opnemen' wordt de "Salesforce Data Protection Officer" genoemd., geraadpleegd op 22 juli 2020.
[308] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder "5. Waarom en hoe gebruiken we uw persoonlijke informatie?" bij "a) Om klanten en partners van Oracle Marketing & Data Cloud in staat te stellen producten en services te marketen op basis van uw interesses", tekst tot 11 juni 2020. , geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).
[309] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder "5. For what commercial or business purpose do we use your personal information?", tekst tot 11 juni 2020. , geraadpleegd op 23 aril 2020.

458. Wie de “klanten en partners” zijn, welke gegevens worden gebruikt, hoe gegevens worden gebruikt en of deze verwerking gelimiteerd is tot het gebruik van “uw interesses”, is niet duidelijk.

459. Oracle heeft de Engelse versie op 11 juni 2020, na het ontvangen van de sommatiebrief van de Stichting, aangepast.[310] De wijziging betreft met name een specificatie van het marketing doeleinde. Het doeleinde is echter nog steeds erg vaag omschreven. Zo kunnen de door Oracle verwerkte gegevens in dit kader bijvoorbeeld gebruikt worden:

> *“to create, communicate, deliver, and exchange offerings that have value for customers, clients, partners and society at large”*
>
> of
>
> *“to encourage safe practices and trends and the provision of factual information, including, by way of example, providing product or automotive recall notices”*[311]
> **(Productie 22.c)**

460. Opvallend is dat de Nederlandse versie deze wijziging (nog) niet bevat.[312]

461. In zowel de Engelse als de Nederlandse versie van het Privacybeleid voor Oracle Data Cloud volgt daarna een geheel andere opsomming van doeleinden die lijken te zien op marketing.[313] De privacy documentatie vermeldt niet welke gegevens voor welk doeleinde worden gebruikt.

462. Salesforce verstrekt in haar Audience Studio Privacy Policy in het geheel geen informatie over doeleinden, maar geeft enkel voorbeelden van doeleinden waarvoor haar klanten gegevens zouden kunnen gebruiken:

> *“The Customer typically uses this data on our Platform to deliver targeted advertising campaigns both on the Customer Site and App as well as off their sites and apps. For example, Customers may use the Platform to help them find interested users and to deliver ads that attempt to bring those users back to the Customer’s Site and App. Where our systems can reasonably infer that a particular computer and/or mobile device belong to the same user or household, we may store such information for use on the Platform. The data stored on our Platform may be combined with third-party data (for example, geolocation data provided by a vendor) in order to better target advertisements, to enable Customers to better*

[310] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html , onder “5. For what commercial or business purpose do we use your personal information?”, geraadpleegd op 21 juli 2020.
[311] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#scope, onder “5. For what commercial or business purpose do we use your personal information?” bij “a) To help enable Oracle Marketing & Data Cloud customers and partners to market products and services to you based on your interests”, geraadpleegd op 23 juli 2020.
[312] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).
[313] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder “5. For what commercial or business purpose do we use your personal information?” na “More specifically, Oracle can process information about you:”; https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder “5. Waarom en hoe gebruiken we uw persoonlijke informatie?”, na “In het bijzonder verwerkt Oracle mogelijk informatie over u:”, geraadpleegd op 23 juli 2017 (tevens **Productie 22.a**).

> *understand users across multiple computers and devices, and for ad delivery and reporting purposes."*[314]

463. De beschrijving van de kern van de dienst blijft dus gelimiteerd tot de opmerking dat klanten de dienst *meestal* gebruiken voor gepersonaliseerde reclame. Dit doeleinde is te algemeen geformuleerd en laat ruimte open voor andere doeleinden die niet genoemd worden.

464. Voorts geeft Salesforce geen enkele informatie over profilering, terwijl zij dat wel zou moeten doen (overweging 60 AVG).

465. Ook over de grondslag zijn Oracle en Salesforce niet duidelijk.

466. Voor zover Oracle zichzelf aanmerkt als verantwoordelijke, geeft zij aan dat toestemming de grondslag is en dat deze namens Oracle wordt verkregen.[315] Oracle geeft echter aan dat de partners van wie zij gegevens verkrijgt, niet altijd een relatie hebben met de betrokkenen.[316] Zonder nadere toelichting, die ontbreekt, is onbegrijpelijk hoe deze partners die geen relatie hebben met de betrokkenen toestemming kunnen verkrijgen.

467. Salesforce verstrekt in haar Audience Studio Privacy Policy ten aanzien van de DMP-verwerkingen geen informatie over de grondslag(en).[317] Ook in haar algemene privacybeleid is geen duidelijke informatie op dit punt opgenomen. Voor zover dat beleid informatie bevat over de grondslag van het tonen van gepersonaliseerde advertenties en inhoud, ziet deze slechts op gepersonaliseerde informatie over Salesforce ("gepersonaliseerde informatie over ons") niet op gepersonaliseerde informatie over derden zoals waarvoor de DMP-gegevens worden gebruikt.[318]

<u>De feitelijke ontvangers van de persoonsgegevens, waaronder (gezamenlijke) verantwoordelijken, verwerkers en derden aan wie de gegevens zullen worden verstrekt (artikel 4 sub 9 AVG);</u>

468. Oracle heeft slechts een algemene opmerking opgenomen over de potentiële ontvangers van persoonsgegevens:

> *"Klanten en partners van Oracle Data Cloud, met inbegrip van aanbieders van digitale marketing, reclamebureaus, online uitgevers, aangesloten tv-aanbieders, platforms aan de vraagzijde, gegevensbeheerplatforms, platforms aan de aanbodzijde en sociale-medianetwerken."*[319]

---

[314] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder "How we Collect and Use De-identified and/or Pseudonymized Personal Data via our Platform", geraadpleegd op 21 juli 2017 (tevens **Productie 22.a**).
[315] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder 6 "Wat is onze wettelijke basis voor informatie over u verzameld in de EU/EER?", geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).
[316] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder 4 "Welke soorten persoonlijke informatie verwerken we en uit welke bronnen?", bij "Offline informatie" "alsmede derde partijen die mogelijk geen relatie met u hebben", voor het laatst geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).
[317] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, geraadpleegd op 21 juli 2020 (tevens **Productie 23.d**).
[318] https://www.salesforce.com/nl/company/privacy/full_privacy/, onder "5. Doeleinden waarvoor we Persoonsgegevens verwerken en de rechtsgrondslagen waarop we ons baseren", geraadpleegd op 21 juli 2020.
[319] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, onder "8. Wanneer en hoe kunnen we u persoonlijke informatie delen?" bij "Delen met derde partijen", geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).

469. Deze opsomming betreft in wezen de gehele *adtech* markt en alle websitehouders. Het aantal potentiële ontvangers is daarmee praktisch ongelimiteerd. Voorts is ook niet duidelijk welke rol deze partijen hebben. Mogelijk kan Oracle met meerdere van deze partijen aangemerkt worden als gezamenlijke verwerkingsverantwoordelijken (zie tevens randnummer 284).

470. Salesforce verstrekt wel informatie over het delen van persoonsgegevens.[320] In deze informatie doet Salesforce het echter voorkomen alsof zij uitsluitend gepseudonimiseerde gegevens verwerkt en die alleen in uitzonderlijke gevallen met partijen deelt. Dit staat haaks op wat haar DMP dienst feitelijk inhoud: het verzamelen van zoveel mogelijk herleidbare informatie om deze beschikbaar te maken voor een groot aantal partijen. Salesforce noemt in haar privacy documentatie geen ontvangers bij naam en verstrekt geen specifieke informatie over het delen van persoonsgegevens in het kader van marketingactiviteiten.

471. Gedaagden voldoen daarmee niet aan het vereiste om informatie te verstrekken over de feitelijke ontvangers van de gegevens. Dit klemt eens te meer nu juist dit aspect een enorm groot effect op de privacy van betrokkenen heeft.

De bewaartermijn;

472. Oracle bewaart de gegevens die online verkregen zijn, bijvoorbeeld door middel van cookies, 13 maanden na verkrijging. De “offline gegevens”, waaronder dus naam, adres, e-mailadres, telefoonnummer, demografische gegevens, aankoopgegevens, bedrijfsgegevens en “publicly available information” bewaart Oracle tot 5 jaar na verkrijging. Deze lange termijn is niet te rechtvaardigen.

473. Oracle somt in haar privacy documentatie enkele bewaartermijnen op.[321] Geen bewaartermijn wordt echter genoemd van de gegevens die via Publishers worden verkregen.

474. Salesforce vermeldt slechts dat de third party cookies van Salesforce een levensduur hebben van zes maanden.[322] Over de bewaartermijn van de gegevens die met cookies verkregen worden of die via de DMP dienst verhandeld worden staat niets vermeld.

475. Daarmee voldoen partijen ook niet aan het vereiste om informatie te verstrekken over bewaartermijnen. Gezien de algehele doelstelling van de DMP diensten van Oracle en Salesforce, het verzamelen, combineren en beschikbaar maken van zoveel mogelijk informatie, is het bovendien aannemelijk dat de gecreëerde datasets onbeperkt worden bewaard, waarmee Oracle en Salesforce tevens in strijd met het beginsel van dataminimalisatie handelen (zie daarover paragraaf 4.6.4).

De categorieën van persoonsgegevens die worden verwerkt; en

476. Voor zover Oracle en Salesforce de gegevens niet direct bij betrokkenen maar via een andere bron verzamelen, moet informatie worden opgenomen over de categorieën persoonsgegevens die worden verwerkt. Hiervan is in ieder geval voor een gedeelte van de verwerking sprake, nu Oracle en Salesforce niet enkel via door hen zelf geplaatste cookies gegevens verkrijgen, maar

[320] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder ‘How we Use and Share Personal Data’, geraadpleegd op 22 juli 2020.
[321] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, onder “7. Hoe lang bewaren we informatie over u?”, geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).
[322] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder “HTTP Cookies”, geraadpleegd op 22 juli 2020 (tevens **Productie 23.d**).

onder meer ook gegevens verkrijgen van leveranciers en door middel van cookie syncing koppelingen kunnen maken met gegevens verzameld door andere partijen (paragraaf 3.2.4 t/m 3.2.6).

477. Oracle somt een groot aantal categorieën persoonsgegevens op, die dermate breed zijn geformuleerd dat vrijwel alle gegevens daaronder kunnen vallen.[323]

478. Salesforce beschrijft in haar privacy documentatie beperkt welke gegevens zij verzamelt. Aandacht wordt onder andere besteed aan IP-adressen, device IDs en video's die de betrokkene bekeken heeft.[324]

479. Salesforce gaat echter nauwelijks in op de kern van haar diensten, te weten het verzamelen van gegevens over internetgebruik, het tracken van betrokkenen en het verkrijgen van gegevens van data partners. Het is op basis van deze privacy documentatie voor de betrokkene onmogelijk om een inschatting te maken van welke gegevens Salesforce van de betrokkene verwerkt.

480. Salesforce beschrijft voorts niet in heldere taal dat het met deze gegevens nieuwe persoonsgegevens creëert zoals profielen en interessesegmenten.

De bron van de persoonsgegevens

481. Nu Oracle en Salesforce ook niet direct bij betrokkenen maar via een andere bron persoonsgegevens verzamelen, moet tevens informatie worden opgenomen over de bron van de gegevens.

482. De informatie van Oracle hierover in haar privacy documentatie verstrekt, kan gezien haar werkwijze niet volledig zijn. In haar privacy documentatie heeft Oracle een hyperlink geplaatst naar een lijst van circa 75 datapartners.[325] De in het document genoemde partijen zouden de enige gegevensleveranciers in de EU/EER zijn.[326] In een persbericht geeft Oracle echter onder meer aan met 1500 datapartners te werken (**Productie 15**). Uit onderzoek blijkt verder dat Oracle haar cookies koppelt aan de cookies van andere partijen, ook wanneer deze geplaatst zijn bij Nederlandse gebruikers (**Productie 16**) (zoals eerder aangegeven, wordt dit "cookie syncing" genoemd). Met deze koppeling worden persoonsgegevens uitgewisseld, ten minste het Cookie ID. Verder wordt het ook mogelijk om meer gegevens uit te wisselen (zie tevens paragraaf 3.2.6). De vele partijen waarmee Oracle cookies koppelt worden echter niet genoemd in de privacy documentatie en de meesten staan niet in de lijst van gegevenspartners.

483. Salesforce verschaft in haar privacydocumentatie geen informatie over de leveranciers van gegevens. Zoals hiervoor omschreven (randnummers 379 e.v.), moet de betrokkene een omslachtige route afleggen om bij de uitgebreide lijst van datapartners te komen. Daarnaast

[323] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#3, onderdeel 4, geraadpleegd op 22 juli 2020 (tevens **Productie 22.a**).
[324] https://www.salesforce.com/products/marketing-cloud/sfmc/audience-studio-privacy/, onder 'Statistical Identifier', 'Mobile Device Identifiers', 'Viewed Content Data', geraadpleegd op 22 juli 2020.
[325] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html (tevens **Productie 22.a**); https://www.oracle.com/nl/data-cloud/solutions/data-as-a-service/data-providers.html, geraadpleegd op 21 juli 2020.
[326] https://www.oracle.com/nl/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, geraadpleegd op 21 juli 2020 (tevens **Productie 22.a**).

zijn verschillende, deels overlappende en deels afwijkende lijsten van datapartners te vinden op de website (zie randnummers 117 en 118).[327]

484. Salesforce verstrekt ook geen informatie over het koppelen van persoonsgegevens (waaronder Cookie IDs) aan de gegevens van andere *ad-tech* partijen door middel van cookie syncing. Zoals blijkt uit onderzoek maakt ook Salesforce hier gebruik van (**Productie 16**).

485. Het is voor de betrokkene niet mogelijk om een duidelijk en volledig beeld te krijgen van de bronnen waaruit Oracle en Salesforce persoonsgegevens verkrijgen.

486. Uit bovenstaande blijkt dat Oracle en Salesforce niet de op grond van artikel 13 en 14 AVG vereiste informatie verstrekken.

4.6.3.3 Transparantie en gezamenlijke verantwoordelijkheid

487. Wanneer sprake is van gezamenlijke verantwoordelijkheid moeten de verwerkingsverantwoordelijken bovendien op transparante wijze de verantwoordelijkheid van ieder van hen voor nakoming van de verplichtingen uit de AVG vaststellen (artikel 26 lid 1 AVG). Dat moet "met name" met betrekking tot de rechten van betrokkenen en de informatieverplichtingen uit artikel 13 en 14. Duidelijk moet zijn welke rol ieder van hen vervult en welke verhouding zij hebben met betrokkenen. De "wezenlijke inhoud" van de afspraken tussen de verantwoordelijken moet aan betrokkenen ter beschikking worden gesteld (artikel 26 lid 2 AVG).

488. Iedere verwerkingsverantwoordelijke moet passende maatregelen nemen om ervoor te zorgen dat betrokkenen op beknopte, transparante, begrijpelijke, toegankelijke wijze en in duidelijke en eenvoudige taal zijn geïnformeerd (artikel 12 lid 1 AVG). Oracle en Salesforce voldoen niet aan deze verplichting. Zoals hiervoor reeds toegelicht geven zij niet aan dat er sprake is van gezamenlijke verantwoordelijkheid (binnen hun concern, zie randnummer 283), wie de gezamenlijk verantwoordelijken zijn, laat staan dat zij inzicht geven in de rolverdeling. Ook nemen zij geen passende maatregelen om ervoor te zorgen dat de partijen van wie zij gegevens verkrijgen deze informatie verstrekken.

489. Ten aanzien van Oracle geldt dat zij zich in haar brief op het standpunt stelt dat zij slechts met vier zorgvuldig geselecteerde leveranciers van gegevens werkt en dat zij stelt zorgvuldig te controleren of deze wel aan de AVG voldoen. Zoals hiervoor al aangegeven, is een van deze leveranciers ShareThis (zie randnummers 113.b en 422 e.v.). Zoals blijkt uit onderzoek is ShareThis een partij die op intransparante wijze op grote schaal gegevens verzamelt.[328] Het is daarom onmogelijk om adequaat te informeren over alle partijen met wie de gegevens via ShareThis gedeeld worden, laat staan dat het mogelijk is om aangeven hoe de (gezamenlijke) verantwoordelijkheid georganiseerd is.

[327] https://konsole.zendesk.com/hc/en-us/sections/206625468-Salesforce-DMP-Ecosystem-Partners, geraadpleegd op 29 april 2020, en https://www.salesforce.com/products/commerce-cloud/partner-marketplace/, geraadpleegd op 29 april 2020.
[328] Ad Tech Surveillance on the Public Sector Web, Report by Cookiebot, aanbevolen door EDRi, maart 2019, te raadplegen via: https://www.cookiebot.com/en/cookiebot-report/.

4.6.3.4 Wijzigingen in privacy policies

490. Uit artikel 12 AVG volgt dat de transparantievereisten van de AVG van toepassing zijn gedurende de hele levenscyclus van de verwerking. Betrokkenen moeten dus ook op de hoogte worden gesteld van veranderingen in de informatie van de artikelen 13 en 14 AVG. Volgens WG29 betekent dit dat betrokkenen ook moeten worden geïnformeerd over veranderingen in de privacyverklaringen.

491. Veranderingen die "substantieel of wezenlijk" zijn moeten actief ter kennis worden gebracht van de betrokkene, namelijk "op een zodanige wijze worden meegedeeld dat de meeste ontvangers er feitelijk acht op zullen slaan".[329] Een verandering in het doel van de verwerking moet in ieder geval als substantieel en wezenlijk worden aangemerkt volgens WG29. Kennisgeving daarvan moet plaatsvinden via een geschikt medium, zoals e-mail, een papieren brief of een pop-up op een webpagina.[330]

492. Oracle heeft haar (Engelstalige) Oracle Data Cloud Privacy Policy laatstelijk gewijzigd op 11 juni 2020, na het ontvangen van de sommatiebrief van de Stichting (zie randnummer 459). Het doeleinde werd tot dat moment omschreven als "to help enable Oracle Marketing & Data Cloud customers and partners to market products and services to you via online and offline marketing activities based on your interests".[331] In de aangepaste documentatie is een aantal specificaties toegevoegd, zoals "to create, communicate, deliver, and exchange offerings that have value for customers, clients, partners and society at large" en "to encourage safe practices and trends and the provision of factual information, including, by way of example, providing product or automotive recall notices".[332] Het Nederlandstalige Privacybeleid voor Oracle Data Cloud is niet meer gewijzigd sinds 26 juli 2019.

493. De wijzingen die Oracle in haar privacy documentatie heeft doorgevoerd zijn van wezenlijke aard en moeten daarom via een geschikt medium gecommuniceerd worden aan de betrokkenen. Niets wijst erop dat Oracle dat gedaan heeft. In de nieuwe privacy documentatie wordt bovendien niet duidelijk benadrukt welke wijzigingen zijn doorgevoerd. Ook hiermee schendt Oracle de transparantievereisten zoals opgenomen in de artikelen 12, 13 en 14 AVG.

4.6.3.5 Conclusie ten aanzien van transparantie

494. Gezien het voorgaande voldoen Oracle en Salesforce niet aan de transparantievereisten van de AVG. Zij overtreden daarmee artikel 5 lid 1 sub a, 12, 13 en 14 AVG. Deze overtreding levert tevens een overtreding van artikel 11.7a Tw, nu Oracle en Salesforce ook op grond van dat artikel verplicht zijn om in overeenstemming met de AVG te informeren over de cookies die zij plaatsen. Het handelen in strijd met de AVG en Tw kwalificeert (tevens) als handelen in strijd met een wettelijke verplichting en levert daarom jegens betrokkenen een onrechtmatige daad op.

[329] WP260 Transparantie, p. 19
[330] Ibidem.
[331] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder "5. For what commercial or business purpose do we use your personal information?", tekst tot 11 juni 2020, geraadpleegd op 23 april 2020.
[332] https://www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html, onder "5. For what commercial or business purpose do we use your personal information?", tekst vanaf 11 juni 2020, geraadpleegd op 10 juli 2020.

*4.6.4 Verwerking in strijd met dataminimalisatie*

495. Uit het feitelijk kader volgt dat het handelen van Oracle en Salesforce gericht is op big data (zie paragraaf 3.2). Zij plaatsen cookies, verzamelen daarmee gegevens over vrijwel iedere Nederlandse internetgebruiker, evalueren en verrijken de gegevens, creëren en delen profielen en koppelen de gegevenssets met andere gegevenssets door middel van cookies syncing. Alles is gericht op het verzamelen van zoveel mogelijk informatie over zoveel mogelijk internetgebruikers om op basis daarvan gerichte advertenties te tonen.

496. Dat handelen staat haaks op het beginsel van dataminimalisatie en is daarom in strijd met de AVG zoals in het navolgende zal worden toegelicht.

497. Het beginsel van dataminimalisatie, ook wel minimale gegevensverwerking genoemd, is opgenomen in artikel 5 lid 1 sub c AVG:

> *"Persoonsgegevens moeten:*
>
> *c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");"*

498. Het beginsel van dataminimalisatie omvat:

a. een verplichting tot minimale gegevensverwerking; en

b. een verplichting tot toepassing van gegevensbescherming door ontwerp en standaardinstellingen.

499. Het beginsel van dataminimalisatie is afgeleid uit het vereiste van proportionaliteit, dat rechtstreeks verband houdt met de in het kader van artikel 8 EVRM uit te voeren toets of de inbreuk op het door deze bepaling beschermde grondrecht noodzakelijk is in een democratische samenleving.[333]

500. Dat er met name op het gebied van profilering risico's op schending van het dataminimalisatie beginsel bestaan, wordt door WG29 benadrukt:

> *"De kansen die profilering voor het bedrijfsleven biedt, goedkopere opslagkosten en de mogelijkheid om grote hoeveelheden gegevens te verwerken kunnen organisaties aanmoedigen meer persoonsgegevens te verzamelen dan ze eigenlijk nodig hebben, voor het geval dit in de toekomst van pas komt. Verwerkingsverantwoordelijken moeten ervoor zorgen dat zij aan het beginsel van minimale gegevensverwerking voldoen, alsook aan de vereisten van doelbinding en opslagbeperking.*
>
> *Verwerkingsverantwoordelijken moeten duidelijk kunnen uitleggen en rechtvaardigen waarom zij persoonsgegevens moeten verzamelen en bewaren, of overwegen samengevoegde, geanonimiseerde of (wanneer dit voldoende*

[333] Conclusie AG, Parket bij de Hoge Raad 23 juni 2017, ECLI:NL:PHR:2017:553 (*Vereniging Praktijkhoudende Huisartsen/Vereniging van Zorgaanbieders voor Zorgcommunicatie*).

*bescherming biedt) gepseudonimiseerde gegevens te gebruiken voor profilering."* [334]

4.6.4.1 Minimale gegevensverwerking

501. Het beginsel van dataminimalisatie komt terug in een aantal overwegingen bij de AVG, zoals overweging 39:

> *"De persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit vereist met name dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt. Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt. Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan. (...)"*

502. Het beginsel van dataminimalisatie bevat dus een proportionaliteitstoets. Als de verwerking niet proportioneel is en/of hetzelfde doel redelijkerwijs op een andere manier kan worden bereikt, is niet voldaan aan het vereiste van dataminimalisatie. Dat zelfs indien er sprake is van een rechtmatige grondslag, hetgeen in de onderhavige zaak niet het geval is, de verwerking nog noodzakelijk moet zijn voor het beoogde doel, blijkt ook uit een arrest van de Hoge Raad met betrekking tot het toen geldende artikel 8 Wet bescherming persoonsgegevens, het equivalent van artikel 6 AVG:

> *"3.3. (c) Ook als de gegevensverwerking in beginsel is toegestaan op een van de in art. 8 Wbp limitatief opgesomde gronden, blijft de eis gelden dat de verwerking in het concrete geval noodzakelijk moet zijn met het oog op het omschreven doel van de verwerking. De aanwezigheid van een wettelijke rechtvaardigingsgrond maakt derhalve een belangenafweging aan de hand van de hiervoor onder (a) vermelde beginselen niet overbodig. Bij deze afweging moeten de omstandigheden van het geval in aanmerking worden genomen."*[335]

503. Zoals hiervoor uitgebreid uiteen is gezet, is bij de verwerking door Oracle en Salesforce sprake van:

a. Verwerking van grote hoeveelheden persoonsgegevens per persoon (Oracle heeft het over 30.000 datapunten, zie randnummer 121);

b. Een enorme groep bijdragers c.q. bronnen van persoonsgegevens, bestaande uit Publishers en leveranciers van gegevens;

c. Een voortdurende verwerking waarbij onduidelijk is in hoeverre de opslag door alle partijen wordt beperkt, zeer waarschijnlijk zullen de gegevens door sommige partijen niet actief worden verwijderd;

[334] WP251 Profilering, p. 13
[335] HR 9 september 2011, ECLI:NL:HR:2011:BQ8097 (*Santander*).

d. Een enorme groep betrokkenen, te weten: iedereen die gebruik maakt van het internet;

e. Een grote en onbeperkte groep gebruikers van de gegevens, bestaande uit Publishers die de gegevens gebruiken om hun advertentieruimte beter te vermarkten, adverteerders die de gegevens gebruiken om hun biedingen te bepalen, en tussenpersonen zoals ad exchanges, SSPs en DSPs (zie randnummer 123);

f. Verwerking van persoonsgegevens die naar hun aard gevoelig zijn nu zij een zeer gedetailleerd beeld van (het gedrag van) de betrokkenen scheppen.

504. Er is derhalve sprake van *datamaximalisatie* in plaats van *dataminimalisatie*. Gedaagden verzamelen en combineren zoveel mogelijk gegevens, uit zoveel mogelijk bronnen van zoveel mogelijk betrokkenen en, in het kader van winstmaximalisatie, door zoveel mogelijk verschillende partijen.

505. De verwerking levert daarmee inherent een inbreuk op het beginsel van dataminimalisatie op. Daarbij staat de inbreuk niet in verhouding tot het – zuiver commerciële – doel van Oracle en Salesforce en de andere betrokkenen partijen. In tegenstelling tot sommige andere big data toepassingen (zoals bijvoorbeeld in de wetenschap) is hier geen maatschappelijk belang bij gebaat. Ook hebben betrokken zelf geen voordeel bij de verwerkingen. De belangen van betrokkenen bij bescherming van hun fundamentele rechten en vrijheden wegen dan ook zwaarder dan de belangen van Oracle en Salesforce.

506. Over het algemeen wordt betoogd dat big data toepassingen zich moeilijk laten verenigen met het beginsel van dataminimalisatie.[336] Immers big data gaat uit van datamaximalisatie. Doorgaans worden zoveel mogelijk gegevens verzameld en met nieuwe technologie geautomatiseerd gecombineerd en geanalyseerd om daaraan bepaalde conclusies te kunnen verbinden of tot bepaalde inzichten te komen. Zoals ook de Europese toezichthouders onderkennen, zijn de beginselen voor de bescherming van persoonsgegevens, zoals dataminimalisatie, onverkort van toepassing op big data.[337]

507. Bovendien kan het doeleinde van effectief adverteren ook eenvoudig op andere wijze bereikt worden, met minder negatieve gevolgen voor de rechten en vrijheden van betrokkenen. De effectiviteit van op gedrag afgestemde advertenties en andere uitingen is immers al enige tijd onderwerp van discussie. Steeds meer partijen gaan over op advertenties op basis van de context van bijvoorbeeld de nieuwsitems waarbij de advertentie wordt geplaatst (zie paragraaf 186 e.v.).[338] Voor dergelijke vormen van adverteren, zijn in tegenstelling tot de vormen van advertenties waar de DMP dienst op is ingericht, vrijwel geen persoonsgegevens nodig. Het enige verschil is dat het economische belang van Oracle en Salesforce daar niet bij gebaat is, nu dit hun DMP diensten overbodig zou maken.

---

[336] N. Wolters Ruckert & L. van Sloten, 'Big Data: Big Privacy Challenges', *Computerrecht* 2016/82 en L. Viergever & J. Koëter, 'Is onze privacyregelgeving 'Big data proof'?', *Tijdschrift voor Internetrecht*, 6 december 2012, p. 171.
[337] Artikel 29 werkgroep, 'Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU', 14 september 2014, WP221. ('WP221 Big Data')
[338] Zo begon de Ster al in 2018 met zogenaamde "No Consent Advertising", zie Screenforce, *Ster start no consent advertising op online kanalan van NPO'*, 18 december 2018, te raadplegen via: https://screenforce.nl/ster-start-no-consent-advertising-op-online-kanalen-van-npo/.

4.6.4.2 Gegevensbescherming door ontwerp en standaardinstellingen

508. Het beginsel van dataminimalisatie is voorts uitgewerkt in onder meer artikel 25 AVG:

> *"Gegevensbescherming door ontwerp en door standaardinstellingen*
>
> *1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.*
>
> *2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.*
>
> *[…]"*

509. Op grond van artikel 25 AVG moeten de verwerkingsverantwoordelijken zogenaamde "gegevensbescherming door ontwerp en standaardinstellingen" toepassen.

a. Gegevensbescherming door ontwerp houdt in dat de verantwoordelijke er bij het bepalen van de middelen voor verwerking en gedurende de verwerking steeds voor moet zorgen dat passende maatregelen en waarborgen in het ontwerp van de verwerking zijn ingebouwd om aan de verordening te voldoen. Die maatregelen en waarborgen dienen erop gericht te zijn dat aan de beginselen van gegevensbescherming wordt voldaan. Daarbij wordt in de tekst van artikel 25 "minimale gegevensverwerking" uitdrukkelijk genoemd. De waarborgen en maatregelen die in het ontwerp van de verwerking moeten worden meegenomen, moeten dus onder meer gericht zijn op het verzekeren van een minimale gegevensverwerking.[339]

b. Gegevensbescherming door standaardinstellingen houdt in dat de verantwoordelijke maatregelen moet nemen om ervoor te zorgen dat de standaardinstelling zo zijn dat alleen gegevens worden verwerkt die noodzakelijk zijn. De maatregelen dienen de hoeveelheid gegevens die wordt verzameld, de omvang van de verwerking van die

[339] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 13 november 2019, ("EDPB 4/2019 DPbDD") p. 6, par. 7-8.

gegevens, de duur van de opslag en de toegankelijkheid tot de gegevens waar mogelijk te beperken. Standaard dienen dus zo min mogelijk gegevens verwerkt te worden, zo kort mogelijk, etc. terwijl de betrokkene wel de keuze mag hebben een uitgebreidere verwerking actief toe te staan.[340]

510. Overweging 78 bepaalt (onderstreping advocaat):

> *"Ter bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens zijn passende technische en organisatorische maatregelen nodig om te waarborgen dat aan de voorschriften van deze verordening wordt voldaan. Om de naleving van deze verordening aan te kunnen tonen, moet de verwerkingsverantwoordelijke interne beleidsmaatregelen nemen en maatregelen toepassen die voldoen aan met name de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen.*
>
> *Dergelijke maatregelen kunnen onder meer bestaan in het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, transparantie met betrekking tot de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en uit het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren. Bij de ontwikkeling, de uitwerking, de keuze en het gebruik van toepassingen, diensten en producten die zijn gebaseerd op de verwerking van persoonsgegevens, of die persoonsgegevens verwerken bij de uitvoering van hun opdracht, dienen de producenten van de producten, diensten en toepassingen te worden gestimuleerd om bij de ontwikkeling en de uitwerking van dergelijke producten, diensten en toepassingen rekening te houden met het recht op bescherming van persoonsgegevens en, met inachtneming van de stand van de techniek, erop toe te zien dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming. […]"*

511. Volgens de Europese toezichthouders moeten verantwoordelijken in dit kader ten eerste beoordelen of het überhaupt noodzakelijk is om persoonsgegevens te verwerken. Ze hebben de plicht om te controleren of er technologie, processen of methodes bestaan die de verwerking van persoonsgegevens overbodig maken.[341]

512. Belangrijke elementen om te implementeren in het ontwerp en standaardinstellingen zijn volgens de Europese toezichthouders onder meer:

a. Data avoidance: het überhaupt vermijden van het verwerken van persoonsgegevens wanneer dit mogelijk is voor het doeleinde van de verwerking.

b. Relevantie: het beperken van de verwerking tot de gegevens die relevant zijn voor de verwerking. De verantwoordelijke moet dit kunnen aantonen.

[340] Vgl. Autoriteit Persoonsgegevens, 'Microsoft Windows 10 – De verwerking van persoonsgegevens via telemetrie', 29 augustus 2017.
[341] EDPB 4/2019 DPbDD, p. 19, par. 69.

c. Noodzakelijkheid: elk onderdeel van de dataset moet nodig zijn voor de gespecificeerde doeleinden van de verwerking en gegevens mogen niet worden verwerkt als het doeleinde ook op andere wijze kan worden bereikt.

d. Beperking: het beperken van de hoeveelheid verzamelde gegevens tot dat wat nodig is.

e. Data flow: de gegevensstromen moeten efficiënt zijn zodat geen onnodige kopieën van de gegevens worden gemaakt en niet meer punten van data collectie worden gebruikt dan nodig.[342]

513. Door op de hiervoor omschreven wijze handelen Oracle en Salesforce in strijd met de verplichtingen van artikel 25 AVG. Zij zouden bij het inrichten van het DMP en het verzamelen van de gegevens al moeten meenemen of en zo ja welke persoonsgegevens nodig zijn en de verzameling daartoe moeten beperken. Dat doen zij niet, zoals ook uit de feiten blijkt. Zij hebben hun DMP zo ingericht dat maximaal gegevens worden verzameld. Bij het plaatsen en uitlezen van cookies, cookie syncing, en het verzamelen uit andere bronnen wordt geen moment de vraag gesteld of dat nodig is. Ook bij de verwerkingen die volgen is dit het geval. Er wordt niet gekeken naar relevantie of noodzakelijkheid, laat staan of de verwerking kan worden vermeden. De gegevens worden op verschillende plekken opgeslagen en gedeeld met een veelvoud aan partijen. Ook het aantal personen met toegang tot de gegevens is daarmee onbeperkt.

514. Voorzover Oracle en Salesforce zich in dit kader beroepen op pseudonimisering geldt het volgende. Van pseudonimisering is sprake wanneer gegevens aan pseudoniem zoals een nummer gekoppeld worden in plaats van bijvoorbeeld aan de naam van betrokkene. Bij pseudonimisering is dat pseudoniem echter nog steeds herleidbaar tot een geïdentificeerde of identificeerbare persoon. Om die reden geldt dat bij het gebruik van pseudonimisering nog steeds sprake is van persoonsgegevens.[343] Wel kan pseudonimisering in het algemeen gezien worden als een verstandige beveiligingsmaatregel, omdat gepseudonimiseerde gegevens door derden minder eenvoudig misbruikt kunnen worden.

515. In het geval van Oracle en Salesforce, en andere partijen in de RTB markt, geldt dat zij in het algemeen een beroep doen op pseudonimisering en vergelijkbare technieken zoals hashing, waarbij bijvoorbeeld een IP- of e-mailadres wordt ongevormd tot een serie getallen, letters en/of andere tekens. Zij trachten hiermee de indruk te wekken dat geen sprake is van persoonsgegevens of dat de privacy hiermee beschermd is. Dat is echter geenszins het geval. Ook bij het gebruik van dit soort technieken is het doel om zoveel mogelijk gegevens te koppelen aan unieke internetgebruikers. Bij hashing wordt daarvoor bijvoorbeeld door verschillende ad tech partijen dezelfde hashing-techniek gebruikt, zodat de gegevens van een internetgebruiker die zijn verzameld door hen aan elkaar gekoppeld kunnen worden. Op die wijze worden enorme hoeveelheden gegevens over internetgebruikers verzameld. Het gebruik van een pseudoniem is hier dus niet zozeer een beveiligingsmaatregel, maar juist de identificator op basis waarvan alle gegevens aan elkaar kunnen worden gekoppeld. Het

[342] EDPB 4/2019 DPbDD, p. 19, par. 71.
[343] Zie tevens Artikel 29 werkgroep, Advies 5/2014 over anonimiseringstechnieken, 10 april 2014, WP216 ("WP216 Anonimiseringstechnieken").

presenteren hiervan als beveiligingsmaatregel, of zelfs als “anonieme data” is ojuist en misleidend.

516. Ter toelichting van bovenstaande wordt als **Productie 29** een publicatie van dr. Wolfie Christl in het geding gebracht.[344] In deze publicatie bespreekt hij onder meer hoe pseudonimisering in de online advertentiemarkt wordt gebruikt en hoe Oracle daar in het kader van haar DMP gebruik van maakt.

517. Nergens blijkt uit dat de standaardinstellingen die Oracle en Salesforce toepassen op enig punt gericht zijn op beperking van de verwerking of een privacyvriendelijke benadering. Oracle en Salesforce verzamelen standaard zoveel mogelijk gegevens en gebruiken die standaard voor het opstellen van gedetailleerde profielen. Oracle en Salesforce delen de gegevens standaard met een grote groep gebruikers. Van gegevensbescherming door ontwerp en standaardinstellingen is derhalve geen sprake.

4.6.4.3 Conclusie ten aanzien van dataminimalisatie

518. Gezien het voorgaande voldoen Oracle en Salesforce niet aan het beginsel van datamimalisatie, en de verplichtingen tot minimale gegevensverwerking en gegevensbescherming door ontwerp en standaardinstellingen. Zij overtreden daarmee artikel 5 lid 1 sub c en 25 AVG.

*4.6.5 Verboden doorgifte aan de Verenigde Staten*

519. Oracle en Salesforce leveren hun DMP dienst beide primair vanuit hun hoofdkantoor in de Verenigde Staten, Oracle Corporation en Salesforce.com, Inc. Deze entiteiten zijn tevens de eigenaar van de domeinen die de bku en _kuid_ cookies plaatsen (randnummers 296 en 301). Zij bieden hun DMPs wereldwijd aan. Ook de Nederlandse entiteiten zijn daarbij betrokken (randnummers 300 en 303). In hun privacy documentatie worden verschillende entiteiten in de V.S. aangewezen als verwerkingsverantwoordelijke (randnummers 297 en 302 ). Dit betekent dat de DMP-gegevens door Oracle en Salesforce mede in de V.S. worden verwerkt.

520. De doorgifte van persoonsgegevens vanuit Nederland en andere delen van de EU naar de VS door Oracle en Salesforce, zoals deze sinds 25 mei 2018 plaatsvindt, is onrechtmatig.

521. Oracle geeft in haar privacybeleid aan dat, voor zover zij zichzelf als verantwoordelijke aanmerkt, de gegevens worden doorgegeven aan de V.S. op basis van het Privacyshieldbesluit. Dit besluit is echter recent ongeldig verklaard door het HvJEU in de zaak *Schrems II*.[345]

522. Modelcontracten en bindende bedrijfsvoorschriften van Oracle en Salesforce kunnen hen evenmin soelaas bieden. Deze zijn immers slechts geschikt voorzover zij verwerker zou zijn, terwijl zij voor de DMP activiteiten aangemerkt moet worden als (gezamenlijk) verwerkingsgverantwoordelijke. Salesforce geeft op haar website aan dat zij als gevolg van het *Schrems II*-arrest op basis van modelcontracten en bindende bedrijfsvoorschriften doorgeeft, maar dat maakt de doorgifte niet rechtmatig.[346]

---

[344] Dr. Wolfie Christl is een gerespecteerde technologie expert, onderzoeker en digitale rechten activist, zie https://wolfie.crackedlabs.org/en.
[345] HvJEU 16 juli 2020, C-311/18 (*Schrems II*).
[346] https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/EU-Data-Transfer-Mechanisms-FAQ.pdf, geraadpleegd op 18 juli 2020.

523. Zelfs als Oracle en Salesforce bepaalde handelingen verrichten als verwerker, blijft de doorgifte onrechtmatig. Uit de zaak *Schrems II* blijkt immers dat het beschermingsniveau in de V.S. onvoldoende is. Daarom kunnen de modelcontracten en bindende bedrijfsvoorschriften geen waarborg zijn voor datadoorgifte.

524. In het navolgende zal worden toegelicht waarom Oracle en Salesforce met deze doorgifte in strijd handelen met de AVG. Daarbij zal eerst het algemene verbod op doorgifte worden besproken. Aansluitend zal de recente zaak *Schrems II* worden besproken.

4.6.5.1 Doorgifte in beginsel verboden

525. Op grond van de AVG gelden bijzondere regels voor het verwerken van persoonsgegevens buiten de Europese Economische Ruimte ("**EER**") (artikel 44 e.v. AVG), ook wel "doorgifte". Er sprake van "doorgifte" wanneer persoonsgegevens ter kennis worden gebracht van personen buiten de EER, het betreft dus niet enkel opslag. Doorgifte is verboden tenzij een uitzondering geldt (artikel 44 AVG). De achtergrond hiervan is dat veel landen geen passend beschermingsniveau voor persoonsgegevens bieden en dat de Uniewetgever partijen die gegevens verwerken wilde verplichten om daar rekening mee te houden.

526. De AVG biedt verschillende mechanismes op basis waarvan persoonsgegevens mogen worden doorgegeven. Zo kan de Europese Commissie besluiten dat een derde land, een gebied of een sector in een derde land een "passend beschermingsniveau" waarborgt (artikel 45 AVG) (een zogenaamd "adequaatheidsbesluit"). De Europese Commissie heeft in 2016 bepaald dat de V.S. een passend beschermingsniveau waarborgen voor persoonsgegevens die vanuit de EU aan in de V.S. gevestigde organisaties worden doorgegeven wanneer die organisatie voldoet aan de vereisten van het EU-VS Privacy Shield ("**Privacyshieldbesluit**").[347]

527. Bij gebreke van een adequaatheidsbesluit kan doorgifte plaatsvinden op grond van passende waarborgen (artikel 46 AVG). Een van de "passende waarborgen" zijn door de Europese Commissie goedgekeurde modelcontracten. In 2010 heeft de Europese Commissie bepaalde modelcontractbepalingen goedgekeurd ("**Modelcontractbesluit**").[348] Een andere mogelijkheid is dat de organisatie waaraan wordt doorgegeven beschikt over zogenaamde "bindende bedrijfsvoorschriften" die door de bevoegde Europese privacytoezichthouder zijn goedgekeurd (artikel 47 AVG). Het HvJEU heeft bevestigd dat de artikelen 44 tot en met 47 AVG uitvoering geven aan de uitdrukkelijke verplichting van artikel 8 lid 1 van het Handvest en tot doel hebben het hoge niveau van bescherming waarin de AVG voorziet te continueren bij doorgifte van persoonsgegevens naar een derde land.[349]

[347] Uitvoeringsbesluit (EU) 2016/1250 van de Commissie van 12 juli 2016 overeenkomstig richtlijn 95/46 betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming (PB 2016, L 207, blz. 1, met rectificatie in PB 2018, L 262, blz. 90.)
[348] Besluit 2010/87/EU van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens richtlijn 95/46 (PB 2010, L 39, blz. 5), zoals gewijzigd bij uitvoeringsbesluit (EU) 2016/2297 van de Commissie van 16 december 2016 (PB 2016, L 344, blz. 100).
[349] Zie HvJEU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*), r.o. 72

4.6.5.2 Uitspraak van het HvJEU in *Schrems II*

528. Op 16 juli 2020 heeft het HvJEU in de zaak *Schrems II* uitspraak gedaan over doorgifte van persoonsgegevens van de EU naar de V.S.[350] Het HvJEU heeft daarin het Privacyshieldbesluit ongeldig verklaard.

529. Op grond van artikel 45 lid 2 sub a AVG moet de Europese Commissie in het kader van het nemen van een zogenaamd "adequaatheidsbesluit" zoals het Privacyshieldbesluit onder meer rekening houden met:

> *"de rechtsstatelijkheid, […] onder meer inzake nationale veiligheid (…) en de toegang van overheidsinstanties tot persoonsgegevens, […] alsmede het bestaan van effectieve en afdwingbare rechten van betrokkenen en effectieve mogelijkheden om administratief beroep of beroep in rechte te stellen voor betrokkenen wier persoonsgegevens worden doorgegeven."*

530. Het HvJEU heeft bepaald dat Amerikaanse surveillance-programma's[351] niet voldoen aan het evenredigheidsbeginsel en niet tot het strikt noodzakelijke zijn beperkt.[352] Hiermee is niet voldaan aan de vereisten van artikel 45 lid 2 sub a AVG en artikel 52, lid 1, tweede volzin, Handvest.[353]

531. Wat betreft de toegang tot de rechter heeft het HvJEU bepaald dat regelingen waarop de Amerikaanse surveillance-programma's gebaseerd zijn aan betrokkenen geen rechten verschaffen die zij voor rechtbanken tegenover Amerikaanse overheidsdiensten kunnen afdwingen, zodat geen sprake is van een doeltreffende voorziening in rechte.[354] Het in het Privacyshieldbesluit omschreven ombudsmanmechanisme biedt geen rechtsmiddel met voldoende waarborgen zoals op grond van artikel 47 van het Handvest is vereist.[355]

532. Wat betreft het Modelcontractbesluit oordeelt het HvJEU dat dit wel in stand kan blijven. Echter, de doorgifte van persoonsgegevens mag alleen plaatsvinden indien de doorgevende verwerkingsverantwoordelijke en de invoerende verwerker passende waarborgen bieden, en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken zodat het beschermingsniveau in grote lijnen overeenkomt met dat in de EU.[356] Dit houdt de plicht in aanvullende maatregelen te nemen om het ontoereikende niveau van bescherming in een derde land te verhelpen.[357]

533. Nu het HvJEU in het kader van de beoordeling van het Privacyshieldbesluit heeft bepaald dat het beschermingsniveau in de V.S. niet toereikend is, valt niet in te zien hoe een doorgifte aan de V.S. op basis van passende waarborgen, zoals modelcontracten op grond van artikel 46 lid 2 sub c of bindende bedrijfsvoorschriften op grond van artikel 46 lid 2 sub b, mogelijk is. Immers, het HvJEU heeft bepaald dat, onder meer in het kader van de regelingen waarop

[350] HvJEU 16 juli 2020, C-311/18 (*Schrems II*).
[351] Gebaseerd op section 702 van de Foreign Intelligence Surveillance Act, Executive Order 12333 en Presidential Policy Directive 28.
[352] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 184.
[353] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 185.
[354] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 192.
[355] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 197.
[356] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 197.
[357] HvJEU 16 juli 2020, C-311/18 (*Schrems II*), par. 131.

surveillance-praktijken worden gebaseerd, het beschermingsniveau in de V.S. niet overeenkomt met dat in de EU.

4.6.5.3 Doorgifte door Oracle en Salesforce onrechtmatig

534. Gelet op het voorgaande is de doorgifte van persoonsgegevens door Oracle en Salesforce naar de VS in strijd met de AVG, in het bijzonder overtreden zij daarmee artikel 44 e.v. AVG. Ongeacht de rol van Oracle, blijkt bovendien uit de uitspraak van het HvJEU dat het beschermingsniveau in de V.S. onvoldoende is. Dat betekent dat modelcontracten en bindende bedrijfsvoorschriften geen waarborg kunnen vormen voor datadoorgifte.

*4.6.6 Overige inbreuken*

535. Naast de hierboven besproken beginselen van rechtmatigheid, transparantie en dataminimalisatie, bevat de AVG nog andere beginselen en daarop gebaseerde regels. Oracle en Salesforce handelen gezien het voorgaande tevens in strijd met de hierna besproken beginselen en regels.

4.6.6.1 Het beginsel van behoorlijkheid

536. Artikel 5 lid 1 sub a bepaalt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. In het voorgaande is al gebleken dat de verwerkingen die Oracle en Salesforce uitvoeren niet aan de beginselen van rechtmatigheid en transparantie voldoen. Uit de behandeling van het transparantiebeginsel volgde reeds dat aan het beginsel van behoorlijkheid evenmin wordt voldaan (paragraaf 4.6.3). De beginselen van behoorlijkheid en transparantie zijn immers nauw met elkaar verbonden.

537. Ook overigens is gebleken dat geen sprake is van een behoorlijke gegevensverwerking, nu Oracle en Salesforce niet aan de maatschappelijke zorgvuldigheidseisen voldoen (zie ook paragraaf 5.7.3). Dat bij de maatschappelijk zorgvuldigheid in het kader van de onrechtmatige daad moet worden aangesloten voor de beoordeling van de behoorlijkheid van een verwerking, volgt ook uit de Memorie van Toelichting bij artikel 6 van de Wbp, waarin het vereiste was opgenomen dat persoonsgegevens op een behoorlijke en zorgvuldige wijze moeten worden verwerkt.

> *"Belangrijker is in deze aansluiting te zoeken bij reeds bestaande Nederlandse wetgeving. Het voorschrift dat gegevens op een behoorlijke en zorgvuldige wijze moeten worden verwerkt, sluit beter aan bij de vereiste maatschappelijke zorgvuldigheid die men in acht heeft te nemen ten einde een onrechtmatige daad te voorkomen."*[358]

4.6.6.2 Het beginsel van doelbinding

538. Artikel 5 lid 1 sub b AVG bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet

[358] *Kamerstukken II* 1997-98, 25 892, nr. 3, p. 78 (MvT).

verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze. Dit is het beginsel van doelbinding. Aan dit beginsel voldoen Oracle en Salesforce niet.

539. Het beginsel van doelbinding bevat twee elementen. In de eerste plaats mogen gegevens alleen worden *verzameld* voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Eerder is al aangegeven dat de doeleinden niet welbepaald en uitdrukkelijk zijn omschreven (randnummers 456 e.v.). Ook is in het voorgaande al besproken dat er geen rechtmatige grondslag bestaat voor de verwerking door Oracle en Salesforce (paragraaf 4.6.2). Alleen al hierom kan dan ook geen sprake zijn van een gerechtvaardigd doel.[359] Hierbij is tevens van belang dat het doeleinde dat Oracle en Salesforce nastreven met de verwerking zuiver commercieel en is er geen sprake is van enig algemeen belang (randnummer 180).

540. In de tweede plaats mogen persoonsgegevens niet verder worden verwerkt op een manier die onverenigbaar is met die doeleinden. Als persoonsgegevens verder worden verwerkt voor andere doeleinden, dan zullen die nieuwe doeleinden allereerst ook weer voldoende specifiek moeten zijn en aan de overige hierboven besproken vereisten moeten voldoen. In de onderhavige zaak worden de verzamelde gegevens verder verwerkt door allerlei andere partijen en is het voor internetgebruikers volstrekt onduidelijk voor welke doeleinden hun persoonsgegevens verder worden verwerkt, of zelfs door welke partijen dit wordt gedaan.

541. Daarnaast kan de verdere verwerking alleen rechtmatig zijn, indien deze onder meer voldoet aan de redelijke verwachtingen die de betrokkene had op het moment dat zijn gegevens werden verzameld, en de context waarin dit gebeurde.[360] De betrokken personen zijn zich in casu in het geheel niet bewust van de grootschaligheid, de hoeveelheid op de achtergrond betrokken spelers en mate van verdere verwerking. Dit valt dus niet binnen hun redelijke verwachting.

542. Ook moeten verschillende andere aspecten bij de beoordeling worden betrokken of sprake is van verenigbaar gebruik (artikel 6 lid 4 AVG). Onder meer moet rekening worden gehouden met de aard van de persoonsgegevens en de gevolgen van de verdere verwerking voor de betrokkene. Het betreft in deze zaak gevoelige persoonsgegevens die worden gebruikt voor het bouwen van zeer uitgebreide profielen waarvan de gevolgen voor de internetgebruiker onverwacht en verstrekkend zijn.

543. Tevens relevant is de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke. Er is geen sprake van een directe relatie tussen Oracle en/of Salesforce en de betrokken internetgebruiker, zoals bijvoorbeeld in het geval waarin de gegevens van een internetgebruiker worden verwerkt door een partij waarbij hij een dienst of product heeft afgenomen, bijvoorbeeld een webshop. Sterker nog, internetgebruikers hebben geen weet van het bestaan van Oracle en Salesforce. Evenmin is sprake van een gelijkwaardige relatie. De internetgebruiker staat weerloos tegenover deze grote spelers in een internationale markt met een omzet van honderden miljarden.

544. Gezien het voorgaande voldoet de verwerking van persoonsgegevens door Oracle en Salesforce niet aan het vereiste van doelbinding, noch ten aanzien van de verzameling, noch ten aanzien van de verdere verwerking daarvan.

[359] Artikel 29 werkgroep, Advies 03/2013 over doelbinding, 2 april 2013, WP203, p. 19 (WP203 Purpose limitation).
[360] WP203 Purpose limitation, p. 12.

4.6.6.3 Het beginsel van juistheid

545. Artikel 5 lid 1 sub d AVG bepaalt dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd. Juist wanneer sprake is van profilering, is van groot belang dat aan het beginsel van juistheid wordt voldaan. De WG29 geeft in dit verband aan:

> *"Indien de gegevens die in een proces van geautomatiseerde besluitvorming of profilering worden gebruikt onjuist zijn, zullen immers ook besluiten of profielen die daaruit voortkomen onjuist zijn. Besluiten zijn mogelijk genomen op basis van verouderde gegevens of de onjuiste interpretatie van externe gegevens. Onjuistheden kunnen leiden tot ondeugdelijke voorspellingen of verklaringen over bijvoorbeeld iemands gezondheid, kredietrisico of verzekeringsrisico. Zelfs wanneer ruwe gegevens correct worden opgeslagen, is de gegevensreeks mogelijk niet geheel representatief of kunnen de analysegegevens ongemerkt vooroordelen bevatten."*[361]

546. In het profileringsproces moet het beginsel van juistheid in alle stappen in het oog worden gehouden, met name het geval bij de volgende stappen zoals ook de WG29 benadrukt:

- het verzamelen van gegevens;
- het analyseren van gegevens;
- het opstellen van een profiel van een persoon;
- het toepassen van een profiel om een besluit met betrekking tot de persoon te nemen.

547. Verwerkingsverantwoordelijken moeten volgens de WG29 krachtige maatregelen invoeren om ervoor te zorgen en erop toe te zien dat hergebruikte of onrechtstreeks verkregen gegevens juist en actueel zijn. Dit maakt het des te belangrijker dat duidelijke informatie wordt verstrekt over de persoonsgegevens die worden verwerkt, zodat de betrokkene onjuistheden kan corrigeren en de kwaliteit van de gegevens kan verbeteren. In het voorgaande is al aangegeven dat er geen duidelijk informatie wordt verstrekt. Het in het feitelijk kader besproken proces voor het verzamelen en (verder) verwerken van persoonsgegevens door Oracle en Salesforce en derde partijen die toegang krijgen tot de gegevens, maakt het onmogelijk om de gegevens juist en actueel te houden. Inherent aan het proces van datamaximalisatie, profilering en het op grote schaal delen van deze gegevens, is immers juist dat er geen invloed meer kan worden uitgevoerd op de juistheid.

548. Aan het beginsel van juistheid wordt door Oracle en Salesforce dan ook niet voldaan.

4.6.6.4 De verantwoordingsplicht

549. Artikel 5 lid 2 AVG bepaalt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen inzake de verwerking van persoonsgegevens die in artikel 5 lid 1 zijn omschreven, te weten de beginselen van:

[361] WP251 Profilering, p. 13-14.

- Rechtmatigheid, behoorlijkheid en transparantie;
- Doelbinding;
- Minimale gegevensverwerking;
- Juistheid;
- Opslagbeperking; en
- Integriteit en vertrouwelijkheid.

550. Aangezien Oracle en Salesforce gezien het voorgaande in strijd met al deze principes handelen, kunnen zij niet aan hun verantwoordingsplicht voldoen.

551. Artikel 24 AVG bepaalt:

> *"1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.*
>
> *2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd."*

552. Overweging 75 AVG verduidelijkt dat het qua waarschijnlijkheid en ernst uiteenlopende risico voor de rechten en vrijheden van natuurlijke personen kan voortvloeien uit een gegevensverwerking die kan resulteren in ernstige lichamelijke, materiële of immateriële schade. Vervolgens wordt een aantal voorbeelden gegeven van situaties waarin een gegevensverwerking in dergelijke schade kan resulteren. Dit is onder meer het geval wanneer betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen, wanneer bijzondere persoonsgegevens worden verwerkt, wanneer sprake is van profilering, wanneer gegevens van kwetsbare personen worden verwerkt en wanneer sprake is van de verwerking van grote hoeveelheden gegevens. Al deze situaties doen zich in de onderhavige zaak voor. Dat betekent dat er een verzwaarde plicht op Oracle en Salesforce rust om passende technische en organisatorische maatregelen te nemen om verwerking in overeenstemming met de AVG te garanderen. Iets wat gezien hun handelwijze onmogelijk is en waarvan ook op geen enkele manier blijkt dat deze zijn genomen.

553. Evenmin voldoen zij aan de specifieke regels die voortvloeien uit dit principe, althans zullen zij moeten aantonen dat zij hieraan voldoen, zoals, voor zover niet eerder in deze dagvaarding al besproken:

- het opstellen en uitvoeren van een passend gegevensbeschermingsbeleid (artikel 24 lid 2 AVG);

- gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 AVG), gebleken is dat dergelijke maatregelen niet danwel onvoldoende zijn getroffen;
- het bijhouden van een verwerkingsregister (artikel 30 AVG);
- het uitvoeren van een gegevensbeschermingseffectbeoordeling (ook wel "DPIA") voor iedere verwerking met een hoog risico voor de rechten en vrijheden van natuurlijke personen (artikel 35 AVG) en het vooraf raadplegen van de toezichthoudende autoriteit voor iedere DPIA waaruit blijkt dat de verwerking een hoog risico zou inhouden indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken (artikel 36 AVG);
- het nemen van extra maatregelen (artikel 24 lid 3 AVG).

4.6.6.5 De voorwaarden voor de verwerking van persoonsgegevens van kinderen

554. Gezien de wijze waarop Oracle en Salesforce persoonsgegevens verzamelen en de omvang van de gegevensverzameling, worden ook persoonsgegevens van kinderen verzameld. Er worden immers van praktisch alle Nederlanders die informatie op het internet lezen of bekijken persoonsgegevens verwerkt. De AVG bevat extra strenge regels voor de verwerking van persoonsgegevens van kinderen.

555. Overweging 38 AVG bepaalt het volgende ten aanzien van de verwerking van persoonsgegevens van kinderen:

> *"Kinderen hebben met betrekking tot hun persoonsgegevens recht op specifieke bescherming, aangezien zij zich allicht minder bewust zijn van de betrokken risico's, gevolgen en waarborgen en van hun rechten in verband met de verwerking van persoonsgegevens. Die specifieke bescherming moet met name gelden voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten." [onderstreping advocaat]*

556. De AVG bevat verschillende specifieke regels om deze bescherming te garanderen.

557. Ten eerste bepaalt artikel 12 AVG dat de informatie die de betrokkene moet ontvangen op basis van het transparantiebeginsel in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal moet worden verstrekt, *in het bijzonder* wanneer de informatie specifiek voor een kind bestemd is. Overweging 58 verduidelijkt:

> *"Aangezien kinderen specifieke bescherming verdienen, dient de informatie en communicatie, wanneer de verwerking specifiek tot een kind is gericht, in een zodanig duidelijke en eenvoudige taal te worden gesteld dat het kind deze makkelijk kan begrijpen."*

558. In randnummers 432 e.v. is gebleken dat de door Oracle en Salesforce verstrekte informatie niet begrijpelijk is voor volwassen, laat staan voor kinderen.

559. Ten tweede bestaat er een recht op vergetelheid wanneer persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij aan een kind (artikel 17 lid 1 sub f AVG). Overweging 65 AVG licht dit als volgt toe:

> *"(…) Meer bepaald moeten betrokkenen het recht hebben hun persoonsgegevens te laten wissen en niet verder te laten verwerken wanneer de persoonsgegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt, wanneer de betrokkenen hun toestemming hebben ingetrokken of bezwaar maken tegen de verwerking van hun persoonsgegevens, of wanneer de verwerking van hun persoonsgegevens op een ander punt niet met deze verordening in overeenstemming is. Dat recht is met name relevant wanneer de betrokkene toestemming heeft gegeven als kind, toen hij zich nog niet volledig bewust was van de verwerkingsrisico's, en hij dergelijke persoonsgegevens later wil verwijderen, met name van het internet. De betrokkene dient dat recht te kunnen uitoefenen niettegenstaande het feit dat hij geen kind meer is. (…)"*

560. Oracle en Salesforce kunnen niet aan deze verplichting voldoen, zoals in het onderstaande ook nog zal blijken.

561. Ten derde is het niet toegestaan geautomatiseerde besluiten als bedoeld in artikel 22 AVG te nemen ten aanzien van kinderen, tenzij hiertoe een noodzaak bestaat (overweging 71 AVG).[362] Dergelijke besluiten worden door Oracle en Salesforce genomen en nergens blijkt dat kinderen hiervan worden uitgesloten. Van een noodzaak hiertoe is geen sprake.

562. Bovendien heeft WG29 aangegeven dat aangezien kinderen een kwetsbaardere groep van de maatschappij vormen, organisaties in het algemeen moeten afzien van profilering van kinderen voor marketingdoeleinden.[363] Ook wanneer artikel 22 AVG volgens uw rechtbank niet van toepassing zou zijn, geldt dus dat het opstellen van profielen van kinderen door Oracle en Salesforce niet is toegestaan.

563. Ten vierde bepaalt artikel 8 AVG dat wanneer een verwerking is gebaseerd op toestemming, in verband met een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind, deze verwerking alleen rechtmatig is als het kind ten minste 16 jaar oud is. Indien het kind jonger is dan 16, is toestemming van de ouders nodig.

564. Dit betekent dat Salesforce en Oracle toestemming nodig hebben van de ouders van kinderen onder de 16 jaar waarvan zij persoonsgegevens verwerken, over welke toestemming zij niet beschikken. Persoonsgegevens worden immers, mede, verzameld in verband met diensten van de informatiemaatschappij, te weten het bezoek aan een website en het in dat verband verstrekken van, niet rechtsgeldige, toestemming voor het verwerken van persoonsgegevens. Tevens zal, in ieder geval in een (aanmerkelijk) deel van de websites, sprake zijn van een rechtsreeks aanbod aan een kind. Dit is slechts anders indien een verlener van diensten van de informatiemaatschappij het in dit verband duidelijk maakt aan potentiële gebruikers dat hij zijn diensten alleen aanbiedt aan personen van 18 jaar of ouder, en dit niet wordt ondermijnd

[362] WP251 Profilering, p. 34.
[363] WP251 Profilering, p. 35.

door ander bewijs.[364] Hiervan is, in ieder geval voor een deel van de websites waarop Oracle en Salesforce persoonsgegevens verzamelen, geen sprake.

a. Het verbod op het verwerken van bijzondere persoonsgegevens en strafrechtelijke gegevens

565. Artikel 9 AVG bepaalt dat het verwerken van bijzondere persoonsgegevens is verboden, tenzij sprake is van een uitzondering. Onder bijzondere persoonsgegevens worden verstaan persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

566. Het verbod is niet alleen van toepassing wanneer direct bijzondere persoonsgegevens worden verzameld, maar ook wanneer profielen worden opgesteld die een combinatie van gegevens bevatten waaruit bijzondere persoonsgegevens kunnen worden afgeleid. WG29 omschrijft dit als volgt:

> *"Via profilering kunnen gegevens van bijzondere categorieën worden gecreëerd op basis van gegevens die zelf niet tot bijzondere categorieën van gegevens behoren maar wel hiertoe gaan behoren wanneer ze met andere gegevens worden gecombineerd. Het kan bijvoorbeeld mogelijk zijn iemands gezondheidstoestand af te leiden uit de geregistreerde gegevens van zijn boodschappen in combinatie met gegevens over de kwaliteit en energie-inhoud van voedingsmiddelen.*
>
> *Zo kunnen verbanden worden ontdekt die een aanwijzing geven over iemands gezondheid, politieke overtuigingen, geloofsovertuigingen of seksuele geaardheid (...)."*[365]

567. Eerder is al het voorbeeld aangehaald van de warenhuisketen die had ontdekt dat een vrouw zwanger was voordat haar eigen vader dit wist (randnummer 55). In dit geval is sprake van de verwerking van bijzondere gegevens, te weten gezondheidsgegevens. Ook is al besproken het onderzoek waaruit bleek dat wanneer simpele Facebook-"likes" werden gecombineerd met gegevens uit andere bronnen, in 88% van de gevallen de seksuele geaardheid van mannelijke gebruikers kon worden vastgesteld, in 95% van de gevallen de etnische afkomst goed was te schatten en in 82% de onderzoekers een juiste voorspelling maakten of de internetgebruiker christen of moslim was. Dit betreft ook allemaal bijzondere gegevens, die werden afgeleid uit een dataset die vele malen minder uitgebreid was dan de datasets waarover Oracle en Salesforce beschikken.

568. Er moet dan ook worden aangenomen dan Oracle en Salesforce niet alleen normale persoonsgegevens, maar ook bijzondere persoonsgegevens verwerken, zonder dat er een uitzondering op het verbod hiertoe van toepassing is. Een van de mogelijke uitzonderingen is uitdrukkelijke toestemming van de betrokkene (artikel 9 lid 2 sub a AVG). Uitdrukkelijke toestemming is een verzwaarde vorm van toestemming, die aan meer vereisten moet voldoen

[364] Artikel 29 Werkgroep, Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679, WP259, p. 29.
[365] WP251 Profilering, p. 17.

dan de toestemming op grond van artikel 6 AVG. Er moet sprake zijn van een uitdrukkelijke verklaring van de betrokkene. Nu niet aan de vereisten voor standaard toestemming op grond van artikel 6 AVG wordt voldaan (paragraaf 4.6.2), kan ook geen sprake zijn van geldige uitdrukkelijke toestemming in de zin van artikel 9 AVG. De overige uitzonderingen van artikel 9 komen evenmin in aanmerking.

569. Bovendien geldt op grond van artikel 22 lid 4 AVG dat geautomatiseerde besluiten als bedoeld in artikel 22 lid 1 AVG niet mogen worden gebaseerd op bijzondere persoonsgegevens, tenzij een uitzondering van toepassing, waarvan in casu geen sprake is.

570. Artikel 10 AVG bepaalt dat persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen op grond van artikel 6 lid 1 alleen mogen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Net als met bijzondere persoonsgegevens, zullen de door Oracle en Salesforce verwerkte profielen strafrechtelijke gegevens bevatten. Zo kan door middel van cookies bijvoorbeeld een beeld worden verkregen over online fraude.

571. De uitzonderingen op het verwerkingsverbod voor strafrechtelijke gegevens zijn opgenomen in artikel 32 en 33 van de Uitvoeringswet Algemene verordening gegevensbescherming ("**UAVG**"). Ook geldt dat een van de uitzonderingen uitdrukkelijk toestemming is, op welke uitzondering zoals hierboven is besproken geen beroep kan worden gedaan. Evenmin komt één van de overige uitzonderingen in aanmerking.

4.6.6.6 <u>De rechten van de betrokkenen</u>

572. De AVG bevat een aantal aanvullende rechten voor betrokkenen, te weten:

a. Het recht om toestemming in te trekken (artikel 7 lid 3 AVG);

b. Het recht op inzage (artikel 15 AVG);

c. Het recht op rectificatie (artikel 16 AVG);

d. Het recht op gegevenswissing (artikel 17 AVG);

e. Het recht op beperking van de verwerking (artikel 18 AVG);

f. De plicht tot kennisgeving van een wissing of beperking door de verwerkingsverantwoordelijke aan iedere ontvanger van de gegevens (artikel 19 AVG);

g. Het recht op overdraagbaarheid (dataportabiliteit, artikel 20 AVG); en

h. Het recht van bezwaar.

573. Betrokkenen moeten actief op deze rechten worden gewezen (artikel 12 lid 1 jo artikel 13 lid 2 sub b en c en artikel 14lid 2 sub c en d AVG). Overweging 59 AVG benadrukt daarnaast dat er regelingen voorhanden dienen te zijn om betrokkenen in staat te stellen hun rechten

*gemakkelijker* uit te oefenen. Ten aanzien van het intrekken van toestemming bepaalt artikel 7 lid 3 AVG dat dit even eenvoudig moet zijn als het geven van toestemming.

574. In paragraaf 4.6.3 is al aangegeven dat de wijze waarop Oracle en Salesforce informatie verstrekken, niet aan de vereisten van de AVG voldoet. Dit geldt ook voor de wijze waarop betrokkenen worden geïnformeerd over hun rechten. De hieronder besproken informatie wordt dus niet op de juiste manier aan betrokkenen kenbaar gemaakt.

575. Inherent aan de manier waarop Oracle en Salesforce persoonsgegevens verwerken, is bovendien dat het niet mogelijk is om (volledig) aan (alle) rechten van betrokkenen te voldoen. Dat blijkt ook wel uit de privacy documentatie van Oracle en Salesforce (**Producties 22 en 23**).

576. In het Privacybeleid voor Oracle Data Cloud (hoofdstuk 12, "Welke keuzes hebt u?") noch in de AddThis Privacy Policy (hoofdstuk 7, "What are your privacy rights?") is enige informatie opgenomen over de rechten genoemd onder a, c en e-h hierboven. Er bestaat kennelijk geen mogelijkheid die rechten uit te oefenen.

577. Wel wordt in beide hoofdstukken melding gemaakt van een zeer gecompliceerde wijze van afmelden en bezwaar maken tegen het gebruik van informatie over een betrokkene. Er worden drie mogelijke afmeldtools beschreven, waarvan één een brancheoplossing betreft die geen specifieke oplossing bevat voor persoonsgegevens die door Oracle worden verwerkt en één een extra app die moet worden gedownload voor een mobiel apparaat. Gezien de schaal waarop gegeven worden gedeeld, zal geen van deze oplossingen de verwerking volledig beëindigen. Bovendien kan van de "afmeldtool voor Oracle Data Cloud" door mensen in Nederland überhaupt geen gebruik worden gemaakt, zoals hieronder zal worden besproken. Daarnaast is aangegeven dat geen van de tools werkt als bepaalde cookies automatisch worden geweigerd. Op geen enkele manier wordt de betrokkenen dan ook een *gemakkelijker* manier geboden om bezwaar te maken. Evenmin wordt de informatie duidelijker gescheiden van andere informatie weergegeven, zoals artikel 21 lid AVG vereist.

578. Er wordt daarnaast melding gemaakt van een manier om gegevens te wissen, door middel van de afmeldtool voor Oracle Data Cloud, één van de tools die ook bij de afmeldmogelijkheden wordt genoemd. Als hierop wordt geklikt, wordt men echter doorverwezen, via nog een andere pagina, naar een scherm waar een veelheid aan informatie moet worden ingevuld en waar via een dropdown menu het land van de betrokkene moet worden geselecteerd. Vervolgens blijkt dat de tool alleen beschikbaar is voor mensen in de Verenigde Staten (**Productie 30**). Er is dus geen afmeld- of verwijdermogelijkheid voor mensen in Nederland. Het scherm geeft aan dat er geen *"offline personal data for interest-based advertising in your region"* zou worden verwerkt, te weten alle landen behalve de Verenigde Staten. Dit is gezien hetgeen hierover eerder besproken is, evident onjuist.

579. Dat mag ook wel blijken uit het feit dat wanneer gebruik wordt gemaakt van de mogelijkheid tot inzage er wel resultaten worden gegeven (**Productie 21**) . Deze zijn echter geenszins volledig, want bij lange na niet alle informatie die op grond van artikel 15 AVG moet worden verstrekt, is hierin opgenomen.

580. Met betrekking tot Salesforce geldt dat in het document "Audience Studio and Data Studio Privacy" (**Productie 23.d**) geen enkele enige informatie is opgenomen over de rechten genoemd onder a en e-g hierboven. Er bestaat kennelijk geen mogelijkheid die rechten uit te oefenen.

581. Er wordt melding gemaakt van een browser opt-out mogelijkheid die werkt door middel van een cookie. Het resultaat hiervan is onder meer dat klanten van Salesforce de internetgebruiker niet meer mogen targeten, maar dit zegt niks over de persoonsgegevens waarover die die klanten al beschikken.

582. Ten aanzien van het recht op inzage, verwijdering en rectificatie zou de betrokkene een mail moeten sturen of een verzoek per post aan een adres in de Verenigde Staten. Wat er in dit verzoek zou moeten worden opgenomen en hoe dit zou kunnen leiden tot het inwilligen van het verzoek is volstrekt onduidelijk, nu Salesforce beweert enkel gepseudonimiseerde informatie te verwerken en de betrokkene dus niet zou moeten kunnen worden herkend door middel van een e-mailadres of naam. Waarschijnlijk is dit de reden dat Salesforce aangeeft dat zij de informatie mogelijk niet kan verstrekken. Bovendien wordt aangegeven dat de verzoeken geen betrekking kunnen hebben op gegevens die voor klanten worden opgeslagen.

583. Gezien het voorgaande voldoen Oracle en Salesforce niet aan de verplichting uitvoering te geven aan de rechten van betrokken.

## 4.7 Oracle beschermt persoonsgegevens onvoldoende, blijkens een datalek in 2020

584. Zoals hiervoor beschreven heeft eerder dit jaar een datalek plaatsgevonden bij Oracle (zie **Productie 12** en randnummer 149.a).[366] Een onderzoeker en journalisten van technologie medium TechCrunch hadden zonder autorisatie toegang tot een server en daarop opgeslagen persoonsgegevens van Oracle. Het ging om de persoonsgegevens zoals naam, adres, emailadres en persoonsgegevens van gevoelige aard zoals gegevens over deelname aan online kansspelen voor e-sports en betaalgegevens. Het betrof gegevens van een enorme groep betrokkenen. Het betreft daarmee enkel vanwege de omvang van de toegankelijke database één van de grootste veiligheidsinbreuken van het jaar. [367]

585. De onderzoeker en TechCrunch konden toegang verkrijgen tot de gegevens omdat de server waarop de gegevens waren opgeslagen niet adequaat beveiligd was en er onder meer geen login met een wachtwoord was vereist.

### *4.7.1 Beveiligingsplicht*

586. Op grond van artikel 32 AVG moeten de verwerkingsverantwoordelijke en verwerker passende maatregelen nemen om de persoonsgegevens die zij verwerken te beschermen.

587. Artikel 32 AVG:

> *"Beveiliging van de verwerking*

[366] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).
[367] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).

> *1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen […]"*

588. Deze verplichting vormt een uitwerking van het beginsel van integriteit en vertrouwelijkheid (artikel 5 lid 1 sub f AVG) en wordt nader uitgewerkt in overweging 39. Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, mede ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt.[368]

589. Wanneer derden zonder bevoegdheid om persoonsgegevens te verwerken eenvoudig toegang kunnen verkrijgen tot persoonsgegevens, zoals hier is gebeurd, zijn kennelijk onvoldoende beveiligingsmaatregelen genomen.[369] Dat geldt eens te meer nu het hier een enorme hoeveelheid aan gegevens betrof, waaronder mede gegevens van gevoelige aard zoals gegevens over deelname aan kansspelen en betaalgegevens. Het op het risico afgestemde beveiligingsniveau had derhalve relatief hoog moeten zijn. Dat een dergelijke database zonder login met wachtwoord beschikbaar is, is in dit verband onbegrijpelijk. Dat sprake is van een inbreuk op de beveiliging impliceert bovendien dat de beveiligingsplicht is geschonden.

590. Dat Oracle naar eigen zeggen door het nemen van aanvullende maatregelen heeft kunnen voorkomen dat het incident zich herhaalt, [370] demonstreert bovendien dat Oracle in staat is om maatregelen te nemen die het incident hadden kunnen voorkomen. Oracle had die maatregelen simpelweg al vooraf moeten nemen.

591. Oracle heeft daarmee niet voldaan aan haar verplichting om de persoonsgegevens die zij verwerkt adequaat te beveiligen. Dit levert een overtreding van artikel 5 lid 1 sub f en 32 AVG op.

*4.7.2 Datalek is inbreuk in verband met beveiliging*

592. Het incident levert bovendien een inbreuk in verband met persoonsgegevens zoals bedoeld in artikel 4 lid 12 en 33 en 34 AVG op.

593. Artikel 4 lid 12 AVG:

> *„inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging*

[368] Artikel 5 lid 1 sub f AVG en overweging 39 AVG.
[369] Vgl. Autoriteit Persoonsgegevens, *HagaZiekenhuis - Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom*, 18 juni 2020, p. 16, te raadplegen via; https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf; Autoriteit Persoonsgegevens, *UWV – Last onder dwangsom*, 31 juli 2018, te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/last_onder_dwangsom_uwv_werkgeversportaal.pdf.
[370] Techcrunch, *Oracle's Bluekai tracks you across the web. That data spilled online,* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).

> *of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;"*

594. In het onderhavige geval is sprake geweest van ongeoorloofde toegang tot opgeslagen gegevens. Daarmee kwalificeert het incident als inbreuk. Op grond van artikel 33 en 34 AVG moet een dergelijke inbreuk gemeld worden:

a. Aan de toezichthoudende autoriteit tenzij niet waarschijnlijk is dat de inbreuk risico's voor betrokkenen met zich meebrengt (artikel 33 lid 1 AVG); en

b. Aan de betrokkenen indien de inbreuk waarschijnlijk een hoog risico voor betrokkene met zich meebrengt (artikel 34 lid 1 AVG).

595. Nu het in het onderhavige geval om veel gegevens gaat waaronder bovendien gegevens van gevoelige aard lijkt het waarschijnlijk dat de inbreuk risico's voor betrokkenen met zich mee heeft gebracht, en had Oracle het incident aan de relevante toezichthouders moeten melden. Voor de personen van wie de database gegevens van gevoelige aard bevatte, geldt bovendien dat de inbreuk waarschijnlijk een hoog risico heeft opgeleverd. Deze betrokkenen hadden derhalve ook geïnformeerd moeten worden.[371] Het lijkt er niet op dat Oracle dat heeft gedaan.

*4.7.3 Conclusie ten aanzien van beveiliging*

596. Uit voorgaande volgt dat Oracle de beveiligingsplicht van artikel 32 AVG geschonden heeft. Derden hebben immers ongeautoriseerd toegang kunnen verkrijgen tot de persoonsgegevens die zij verwerkt. Dit geldt zelfs wanneer zij, zoals zij ten onrechte stelt, slechts verwerker voor een deel van de verwerking zou zijn. De inbreuk op de beveiliging had voorts gemeld moeten worden bij de autoriteiten en betrokkenen.

597. Gezien het voorgaande voldoet Oracle niet aan het beginsel van integriteit en vertrouwelijkheid en de verplichtingen ten aanzien van beveiliging en datalekken. Zij overtreedt daarmee artikel 5 lid 1 sub f, 32, 33 en 34 AVG.

## 5 AANSPRAKELIJKHEID EN SCHADE

### 5.1 Primair: Aansprakelijkheid op grond van de AVG

598. De Uniewetgever beoogt met de AVG burgers een hoog beschermingsniveau te bieden:

> *"Teneinde natuurlijke personen een consistent en hoog beschermingsniveau te bieden en de belemmeringen voor het verkeer van persoonsgegevens binnen de Unie op te heffen, dient het niveau van bescherming van de rechten en vrijheden van natuurlijke personen op het vlak van verwerking van deze gegevens in alle lidstaten gelijkwaardig te zijn."*[372]

599. De keuze voor een direct werkende verordening in plaats van een richtlijn zorgt mede voor gelijkwaardige bevoegdheden op het gebied van toezicht en handhaving en vergelijkbare

[371] Artikel 29 werkgroep, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, 3 oktober 2017, laatstelijk herzien en goedgekeurd op 6 februari 2018, WP250rev.01, en zoals bekrachtigd door de EDPB op 25 mei 2018; Beleidsregels 'De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp)' van 8 december 2015 (*Stcrt*. 2015, nr 46128).
[372] Overweging 10 AVG.

sancties voor overtredingen van de Europese privacywetgeving in de lidstaten (onderstreping advocaat):

> *"Doeltreffende bescherming van persoonsgegevens in de gehele Unie vereist de versterking en nadere omschrijving van de rechten van betrokkenen en van de verplichtingen van degenen die persoonsgegevens verwerken en van degenen die over die verwerking beslissen, alsmede gelijkwaardige bevoegdheden op het gebied van toezicht en handhaving van de regels inzake gegevensbescherming en vergelijkbare sancties voor overtredingen in de lidstaten."*[373]

600. Zo verplicht de AVG alle lidstaten een systeem toe te passen dat zorgt voor "doeltreffende, evenredige en afschrikkende" sancties.[374]

601. Schendingen van de AVG kunnen, afhankelijk van de inbreuk, worden beboet met bedragen tot € 10.000.000 of € 20.000.000 respectievelijk 2 of 4 % van de wereldwijde jaaromzet in het voorgaande boekjaar (artikel 83 AVG). Sinds het van toepassing zijn van de AVG, hebben de nationale privacy toezichthouders binnen de EU al diverse keren van hun boetebevoegdheid gebruik gemaakt. De Franse toezichthouder CNIL legde een boete van € 50 miljoen op aan Google LLC, onder meer vanwege gebrek aan transparantie en ontoereikende informatievoorziening.[375] De Duitse toezichthouder deelde een boete uit van € 14.5 miljoen aan een woningbouwcoöperatie, wegens het op grote schaal opslaan van persoonsgegevens van huurders.[376] Halverwege vorig jaar maakte de Britse toezichthouder, de ICO, haar voornemen bekend om aan de vliegtuigmaatschappij British Airways een boete van € 205 miljoen op te leggen wegens een datalek.[377] In dezelfde week kondigde de ICO een voorgenomen boete van ruim € 110 miljoen voor hotelketen Mariott aan, opnieuw wegens een datalek.[378] De verwachting is dat de komende jaren meerdere hoge boetes zullen volgen.

602. Ook de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens ("**AP**") heeft hoge boetes opgelegd. Het HagaZiekenhuis moest een boete van € 460.000 betalen, omdat de interne beveiliging van de patiëntendossiers niet goed op orde was. Daarnaast legde de AP een last onder dwangsom op, om te zorgen dat de beveiliging alsnog op orde werd gebracht.[379] In maart van dit jaar legde de AP de tennisbond KNLTB een boete op van € 525.000 voor het verkopen

---

[373] Overweging 11 AVG.
[374] Artikel 84 AVG. Vgl. ook overweging 151 en 152 AVG.
[375] Commission nationale de l'informatique et des libertés (CNIL), *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*, te raadplegen via: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
[376] EDPB, *Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company*, 5 november 2019, te raadplegen via: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en
[377] ICO, *Intention to fine British Airways £183.39m under GDPR for data breach*, 9 juli 2019, te raadplegen via: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
[378] ICO, *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*, te raadplegen via: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
[379] Autoriteit Persoonsgegevens, *Haga beboet voor onvoldoende interne beveiliging patiëntendossiers,* 16 juli 2019, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers

van persoonsgegevens.[380] Twee maanden later ontving een onbekend bedrijf een boete van € 725.000 voor het verwerken van vingerafdrukken van werknemers.[381]

603. Toch zijn de serieuze boetes op één hand te tellen. Dat terwijl de AP in 2019 ruim 27.800 privacyklachten ontving, een forse stijging ten opzichte van de jaren ervoor.[382] De AP heeft herhaaldelijk benadrukt dat haar capaciteit onvoldoende is om alle klachten snel af te kunnen handelen.[383] Deze capaciteitsproblemen doen zich ook in de rest van Europa voor. In een recent evaluatierapport over de AVG uit de Europese Commissie haar zorgen over het nadelige effect hiervan op nationale handhaving van de in de AVG opgenomen regels.[384]

604. Het gevolg van het gebrek aan publiekrechtelijke handhaving is dat datahandelaren zoals Oracle en Salesforce de afgelopen jaren producten die gecreëerd zijn om zoveel mogelijk persoonsgegevens over zoveel mogelijk internetgebruikers te exploiteren ongestoord hebben doorontwikkeld. Zoals professor en advocaat Lokke Moerel[385] het treffend formuleert:

> *"Maar het bedrijfsmodel van de grote technologiebedrijven en datahandelaren is grotendeels ongemoeid gebleven. Zij verzamelen via de cookies nog steeds naar hartenlust data, combineren die tot profielen en verkopen die aan derde partijen voor advertenties. De toestemming die burgers moeten geven voor de cookies is een wassen neus volgens Moerel. Zij spreekt van 'wijdverbreide noncompliance met de AVG."*[386]

605. De nationale toezichthouders missen simpelweg de slagkracht om dit soort gedragingen een halt toe te roepen. Een noodzakelijke aanvulling op publiekrechtelijke handhaving is daarom de mogelijkheid om privacyschendingen op grond van civiele handhaving aan te pakken. De AVG voorziet ruimschoots in die mogelijkheid. Artikel 80 AVG geeft betrokkenen de mogelijkheid zich te laten vertegenwoordigen door een stichting die namens hen bepaalde rechten uitoefent en het recht op schadevergoeding uitoefent. Artikel 82 AVG geeft eenieder die schade heeft geleden door een schending van de AVG het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen.

606. Op deze manier komt zogenoemde strooischade ook voor vergoeding in aanmerking.[387] Bij dit type schade is de schade per individueel geval te beperkt in verhouding tot de kosten van een procedure.[388]

---

[380] Autoriteit Persoonsgegevens, *Boete voor tennisbond vanwege verkoop van persoonsgegevens*, 3 maart 2020, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-tennisbond-vanwege-verkoop-van-persoonsgegevens
[381] Autoriteit Persoonsgegevens, *Boete voor bedrijf voor verwerken vingerafdrukken werknemers*, 30 april 2020, te raadplegen via https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-bedrijf-voor-verwerken-vingerafdrukken-werknemers
[382] Autoriteit Persoonsgegevens, *Forse stijging privacyklachten in 2019, 14 februari 2020*, te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019.
[383] Zie o.a. RTLZ, *Privacyautoriteit kan drukte niet aan: grove privacyschendingen dreigen,* 14 februari 2020, te raadplegen via: https://www.rtlnieuws.nl/tech/artikel/5020511/autoriteit-persoonsgegevens-tekort-drukte-privacyklachten-avg-d66-sp
[384] Europese Commissie, 27 juni 2020, 'Staff Working Document: accompanying the Communication - two years of application of the General Data Protection Regulation (COM(2020) 264 final).
[385] Prof. Mr. Lokke Moerel is verbonden aan Tilburg University, zie https://www.tilburguniversity.edu/nl/medewerkers/e-m-l-moerel en aan internationaal advocatenkantoor Morrisson Foerster zie https://www.mofo.com/people/lokke-moerel.html.
[386] *Privacywet mist na twee jaar nog steeds tanden*, Financieel Dagblad 25 mei 2020, te raadplegen via: https://fd.nl/ondernemen/1345538/privacywet-mist-na-twee-jaar-nog-steeds-tanden.
[387] W.H. van Boom, 'Effectuerend handhaven in het privaatrecht', *NJB* 2007/826, afl. 16, p. 987; I.N. Tzankova, *Strooischade*, Den Haag: Sdu Uitgevers 2006, p. 50.
[388] M. Rottenberg & D. Jacobs, 'Enforcing Privacy Rights: Class Action Litigation and the Challenge of cy pres', in: D. Wright & P. De Hert (ed.), Enforcing Privacy: Regulatory, Legal and Technological Approaches, Springer International Publishing Switzerland 2016, p. 311-312.

607. Op 1 januari 2020 is de Wet afwikkeling massaschade in collectieve actie (WAMCA) in werking getreden. Deze wet maakt het mogelijk om een collectieve vordering tot schadevergoeding in te stellen. Dit is opgenomen in artikel 3:305a BW. Hierop zal hoofdstuk 8 verder ingaan.

## 5.2 Schenden AVG, toerekenbaarheid en relativiteit

608. Zoals in hoofdstuk 4 toegelicht handelen Oracle en Salesforce in strijd met fundamentele rechten van betrokkenen en overtreden zij de AVG en artikel 11.7a Tw. Zij doen dit met name door:

a. Toepassing van geautomatiseerde besluitvorming door profilering (artikel 22 AVG);

b. Zonder verwerkingsgrondslag (in dit geval: toestemming) persoonsgegevens te verwerken door onder meer door cookies te plaatsen (artikel 6 AVG en 11.7a Tw);

c. Niet te voldoen aan de vereisten om de verwerking voor betrokkenen transparant te maken (artikel 12 – 14 AVG en 11.7a Tw);

d. Te doen aan datamaximalisatie in plaats van de vereiste dataminimalisatie (artikel 5 lid 1 sub c en 25 AVG);

e. Op onrechtmatige wijze persoonsgegevens door te geven aan de V.S. (artikel 44 e.v. AVG).

609. Nu Oracle en Salesforce hiervoor de verwerkingsverantwoordelijke zijn, zijn zij op grond van artikel 82 AVG aansprakelijk voor de door de onrechtmatige verwerkingen veroorzaakte schade. In het slot van artikel 82 lid 2 AVG ligt bovendien een relativiteitseis besloten: de AVG strekt tot bescherming tegen de schade zoals die zich heeft voorgedaan. In het navolgende zal een en ander nader worden toegelicht.

### *5.2.1 Uitgangspunt: Oracle en Salesforce worden vermoed persoonsgegevens te verwerken (artikel 11.7a lid 4 Tw)*

610. In artikel 11.7a lid 4 Tw is een bewijsvermoeden opgenomen (paragraaf 4.3.2.2). Dit bewijsvermoeden houdt in dat als cookies worden gebruikt om gegevens over het gebruik van verschillende diensten van de informatiemaatschappij, zoals websites, te verzamelen, te combineren of te analyseren zodat de internetgebruiker anders behandeld kan worden, vermoed wordt dat er sprake is van een verwerking van persoonsgegevens.[389]

611. Dit bewijsvermoeden is opgenomen vanwege zorgen over de privacy-implicaties van 'third party cookies', alsmede over de cookies waarmee surfgedrag, interesses en andere gegevens van gebruikers worden geanalyseerd voor commerciële doeleinden.[390]

612. De Stichting heeft in deze dagvaarding gemotiveerd uiteen gezet dat de bku en _kuid_ cookie van Oracle en Salesforce bij uitstek onder dit bewijsvermoeden vallen (zie paragraaf 4.3.2.2).

[389] *Kamerstukken I* 2011/12, 32549, E; *Kamerstukken II* 2013/14, 33902, 3.
[390] *Kamerstukken II* 2011/12, 32549, 39

Dit betekent dat Oracle en Salesforce op grond van de Tw worden vermoed persoonsgegevens te verwerken.

613. Dit vermoeden zorgt er ook voor dat Oracle en Salesforce naast de regels in artikel 11.7a Tw ook de beginselen van de AVG moeten naleven.[391]

614. Voorts geldt voor de bku en _kuid_ cookies dat uit onderzoek (**Productie 16**) blijkt dat Oracle en Salesforce in ieder geval een gedeelte van de cookies zelf plaatsen. Op grond van artikel 11.7a Tw rust de verplichting om toestemming te verkrijgen en informatie te verstrekken ten aanzien van cookies op degene die de cookies plaatst. Zelfs als Oracle en Salesforce onder de AVG slechts de verwerker zouden zijn en zelfs als geen sprake zou zijn van een verwerking van persoonsgegevens, rust op hen krachtens artikel 11.7a Tw de bewijslast om aan te tonen dat toestemming is verkregen en is geïnformeerd en dat die toestemming en informatie aan de AVG voldoen, omdat zij de cookies plaatsen.

*5.2.2 Uitgangspunt: Oracle en Salesforce zijn verwerkingsverantwoordelijke in de zin van de AVG*

615. Zoals reeds uiteengezet, verwerken Oracle en Salesforce op grote schaal persoonsgegevens voor commerciële doeleinden. Dit heeft tot gevolg dat de persoonlijke eigenschappen en gegevens van iedereen die online is, voortdurend worden verzameld en uitgewisseld door en met medewerking van onder meer Oracle en Salesforce.

616. Als uitgangspunt heeft te gelden dat degene die persoonsgegevens verwerkt verantwoordelijk is voor de verwerking, tenzij deze aantoont dat dat niet het geval is.[392] Sprake is van een bijzondere regel over een bewijsvermoeden waaruit een andere verdeling van de stelplicht, bewijslast en/of bewijsrisico voortvloeit.

617. Nu Oracle en Salesforce persoonsgegevens verwerken, heeft als uitgangspunt te gelden dat zij verwerkingsverantwoordelijke zijn. De Stichting hoeft dit dus niet aan te tonen. In paragraaf 4.4 heeft zij voldoende toegelicht waarom Oracle en Salesforce de verwerkingsverantwoordelijke zijn voor de onderhavige verwerkingen. Indien Oracle en Salesforce menen dat zij geen verwerkingsverantwoordelijke zijn, dienen zij dit aan te tonen.

618. De AVG definieert slechts twee rollen voor partijen die persoonsgegevens verwerken: de verwerkingsverantwoordelijke (artikel 4 sub 7 AVG) en de verwerker (artikel 4 sub 8 AVG). Uit de jurisprudentie van het HvJEU volgt dat het begrip "verwerkingsverantwoordelijke" ruim moet worden uitgelegd, mede gelet op de doelstelling van de AVG om een hoog niveau van gegevensbescherming te waarborgen.[393] De EDPS bevestigt dat die ruime uitleg ook ten doel heeft te voorkomen dat er een gebrek aan verantwoordelijkheid bestaat en zodoende te waarborgen dat betrokkenen de garantie hebben van effectieve en volledige bescherming.[394] Dit brengt met zich mee dat een partij die meent slechts verwerker te zijn dat zal moeten

[391] *Kamerstukken II* 2013/14. 33902, nr. 3
[392] Rechtbank 's-Hertogenbosch 31 januari 2013, ECLI:NL:RBOBR:2013:BZ2126; WG 29 Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", goedgekeurd op 16 februari 2010.
[393] HvJEU 29 juli 2019, C-40/17, ECLI:EU:C:2018:1039 (*Fashion ID*), r.o. 66; HvJEU 10 juli 2018, zaak C 25/17, (*Jehovan todistajat*), r.o. 66; HvJEU 5 juni 2018, C 210/16 (*Wirtschaftsakademie Schleswig-Holstein*), r.o. 28; HvJEU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain en Google*)
[394] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 13.

aantonen. Deze partij kan zich dus niet aan zijn verantwoordingsplicht onttrekken met een enkel verweer dat hij de verwerkingsverantwoordelijke niet is.

*5.2.3 Uitgangspunt: bewijslast naleving beginselen AVG rust op Oracle en Salesforce*

619. Artikel 5 lid 2 van de AVG bepaalt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen uit artikel 5 lid 1 van de AVG, waaronder de in deze dagvaarding uitgebreid behandelde beginselen van rechtmatigheid, transparantie, minimale gegevensverwerking en integriteit en vertrouwelijkheid (zie hoofdstuk 4). De verwerkingsverantwoordelijke moet kunnen aantonen dat hij voldoet aan deze beginselen. Dit wordt ook wel de verantwoordingsplicht of het beginsel van accountability genoemd.[395]

620. De beginselen worden bovendien in de overige artikelen van de AVG uitgewerkt, waarmee de verantwoordingsplicht in wezen voor alle verplichtingen uit de AVG geldt. Dit wordt overigens ook bevestigd in artikel 24 AVG waaruit volgt dat de verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Verwezen wordt in dit kader ook naar overweging 74 en 79 AVG waaruit volgt dat voor iedere verwerking vastgesteld moet worden wie de verwerkingsverantwoordelijke is en dat deze partij moet kunnen aantonen dat hij aan de AVG voldoet.

621. De verantwoordingsplicht c.q. het beginsel van accountability van onder andere artikel 5 lid 2 en 24 AVG brengt een omkering van de bewijslast met zich mee.[396] Dit betekent dat het aan de verwerkingsverantwoordelijken, in dit geval Oracle en Salesforce, is om aan te tonen dat zij hebben voldaan aan de beginselen van de AVG. De Stichting hoeft dus niet aan te tonen dat Oracle en Salesforce de beginselen van de AVG hebben geschonden. De Stichting stelt zich overigens op het standpunt dat zij dit wel al voldoende heeft gesteld en aangetoond in hoofdstuk 4 'Privacyrecht'. Oracle en Salesforce kunnen dus niet volstaan met een betwisting van de stellingen en feiten van de Stichting. Oracle en Salesforce zullen moeten aantonen dat zij aan de beginselen van de AVG hebben voldaan, hetgeen zij, gelet op de stellingen en feiten van de Stichting, niet succesvol zullen kunnen doen.

622. Uit de overwegingen bij de AVG volgt verder dat overeenkomstig de beginselen van behoorlijke en transparante verwerking (artikel 5 lid 1 (a) van de AVG) de betrokkenen op de hoogte moeten worden gesteld van het feit dat er verwerking plaatsvindt en van de doeleinden daarvan. De verwerkingsverantwoordelijke dient de betrokkenen de nadere informatie te verstrekken die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen, met inachtneming van de specifieke omstandigheden en de context waarin de persoonsgegevens worden verwerkt. De bewijslast dat de verantwoordelijke heeft voldaan aan het transparantiebeginsel, en dus dat hij betrokkenen adequaat heeft geïnformeerd, rust op de verwerkingsverantwoordelijke (artikel 5 lid 2 jo lid 1 sub a AVG).[397] Daarbij geldt bovendien dat de transparantieverplichting mede de verplichting behelst om transparant te zijn over wie de verantwoordelijke is en wie overigens (als ontvanger) betrokken zijn bij de verwerking (zie paragraaf 4.6.3 "Verwerking niet transparant"). Ook hieruit volgt dat het Oracle en Salesforce zijn die hierover duidelijkheid moeten verschaffen.

[395] J. Jansen & N.D. Schuitema, 'De AVG en het gebruik van artificial intelligence', *TvCo* 2020/3/4, p. 183.
[396] P.A. Nabben & E.C. Post Uiterweer, 'De AVG: hoe heet wordt de soep gegeten?', *ArbeidsRecht* 2019/24, p. 24.
[397] Zie tevens WP260 Transparantie, o.a. par. 2, 13, 21 en 28.

623. Tenslotte geldt voor de in dit kader vereiste toestemming dat de AVG uitdrukkelijk bepaalt dat op de verwerkingsverantwoordelijke de bewijslast rust om aan te tonen dat hij toestemming heeft verkregen voor de verwerking (artikel 7 lid 1 AVG).[398]

## 5.3 Causaal verband tussen schade en schending van de AVG wordt aangenomen

624. Uit artikel 82 lid 1 en 2 AVG blijkt dat de verwerkingsverantwoordelijke aansprakelijk is tegenover een betrokkene indien een onrechtmatige verwerking van persoonsgegevens plaatsvindt, ongeacht of de verwerkingsverantwoordelijke iets te verwijten valt. Vandaar dat sprake is van een risicoaansprakelijkheid: de verwerkingsverantwoordelijke is tegenover de betrokkene aansprakelijk door het enkele feit dat bij de verwerking van zijn/haar persoonsgegevens de AVG is geschonden, ongeacht of de verwerkingsverantwoordelijke ten aanzien van die schending iets te verwijten valt. Deze lezing van artikel 82 AVG vindt in de literatuur breed bijval (zie bijvoorbeeld Van der Jagt-Vink [399] en Van Schelven[400]). De verwerkingsverantwoordelijke kan alleen gevrijwaard worden van aansprakelijkheid, indien hij kan aantonen dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.[401] Het voorgaande heeft tot gevolg dat de Stichting het causaal verband niet hoeft aan te tonen. Het causaal verband (csqn-verband) wordt reeds aangenomen bij schending van de AVG door Oracle en Salesforce.

## 5.4 Enkele betrokkenheid voldoende voor medeaansprakelijkheid

625. Nieuw ten opzichte van de Privacyrichtlijn is dat de AVG het voor de betrokkene mogelijk maakt om zijn schade te verhalen op elk van de partijen die bij de betreffende verwerking betrokken zijn. Uit artikel 82 lid 2 AVG volgt immers dat *elke* verwerkingsverantwoordelijke die bij de verwerking *betrokken* is, aansprakelijk is voor de schade die wordt veroorzaakt door een schending van de AVG. Dat gekozen is voor de term 'betrokken' (in het Engels 'involved') laat zien dat de drempel voor aansprakelijkheid laag is.

## 5.5 Recht op schadevergoeding op grond van artikel 82 AVG

### *5.5.1 Inleiding*

626. In de vorige hoofdstukken is aangetoond dat Oracle en Salesforce de AVG structureel en op grote schaal schenden. Oracle en Salesforce verzamelen, verrijken en delen op grote schaal persoonsgegevens en profielen met een onbepaalde hoeveelheid commerciële bedrijven, zonder dat zij van de betrokkenen de vereiste toestemming hebben gekregen. Zij voldoen daarbij bovendien niet aan de vereisten van transparantie, dataminimalisatie en doorgifte. Deze gedragingen vinden plaats zonder dat betrokkenen hierover controle kunnen uitoefenen en vaak zonder dat betrokkenen er überhaupt weet van hebben. Het nadelige effect van deze gedragingen op internetgebruikers is evident: hun persoonlijke informatie wordt gebruikt in

[398] Zie tevens EDPB Consent, o.a. par. 36 en 104.
[399] F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming', MvV 2019/7.9, p. 290.
[400] P. van Schelven, 'Aandachtspunten inzake AVG aansprakelijkheid / vrijwaring', te raadplegen via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf.
[401] F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming', MvV 2019/7.9, p. 290; [401] P. van Schelven, 'Aandachtspunten inzake AVG aansprakelijkheid / vrijwaring', te raadplegen via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf.

het RTB-proces. Gegevens die een heel precies beeld scheppen van persoonlijke kenmerken, interesses en voorkeuren worden gebruikt om de internetgebruiker te beïnvloeden. Internetgebruikers lijden door dit proces (een concrete vorm van) schade, namelijk immateriële en materiële schade:

a. **Immateriële schade:** tot op heden is slechts aan de orde gekomen dat een schending van de AVG resulteerde in immateriële schade. De relevante rechtspraak wordt hierna verder toegelicht.

b. **Materiële schade:** hoewel de rechter met name tot vergoeding van immateriële schade is overgegaan bij schendingen van de AVG, kunnen dergelijke schendingen ook resulteren in materiële schade. Daarvan is in het geval van Oracle en Salesforce sprake. De betrokkenen worden door het handelen van Oracle en Salesforce immers in hun vermogen geraakt. De informatie die door deze partijen over internetgebruikers wordt verzameld, heeft economische waarde. Dat dit het geval is volgt uit het enkele feit dat commerciële partijen zoals Oracle en Salesforce bereid zijn kosten te maken en een complexe organisatie in te richten om deze informatie te (doen) verzamelen. De materiële schade wordt nader uitgewerkt in paragraaf 5.5.5.

627. Zowel de immateriële schade als de materiële schade dient door Oracle en Salesforce te worden vergoed. De Stichting baseert haar vordering primair op artikel 82 AVG, subsidiair op artikel 6:162 BW (onrechtmatige daad) c.q. artikel 6:212 BW (ongerechtvaardigde verrijking).

628. Bij schending van de AVG geeft artikel 82 AVG de benadeelde recht op schadevergoeding van de materiële en immateriële schade. Artikel 82 lid 1 AVG luidt als volgt:

> *"Eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade."*

*5.5.2 Schadebegrip in het kader van de AVG*

629. In zijn rechtspraak hanteert het HvJEU de preambule als hulpmiddel bij de uitlegging van de bepalingen uit Europese wetgeving. Overweging 146 van de preambule van de AVG stelt dat "alle schade" dient te worden vergoed en dat het begrip schade ruim moet worden uitgelegd in het licht van de rechtspraak van het HvJEU, "op een wijze die ten volle recht doet aan de doelstellingen" van de AVG.

630. Het HvJEU neemt als uitgangspunt dat de te vergoeden schade reëel en zeker moet zijn. Daarvan is al snel sprake. In *Staelen t. Ombudsman* concludeert de Grote Kamer van het HvJEU dat het "gevoel van psychische schade" als reële en zekere schade is aan te merken.[402] Daarmee wijkt de Grote Kamer nadrukkelijk af van de conclusie van de AG, die meent dat "*de vergoeding niet louter [kan] worden gebaseerd op de subjectieve verklaring van de partij die deze vordert*".[403]

[402] HvJEU 4 april 2017, C-337/15, ECLI:EU:C:2017:256 (*Europese Ombudsman*), r.o. 127-128.
[403] Conclusie AG 27 oktober 2016, C-337/15 (*Europese Ombudsman*), rndnr. 114.

*5.5.3 Immateriële schadevergoeding*

631. Ook in de Nederlandse jurisprudentie wordt het schadebegrip op deze manier uitgelegd. In Nederland is al meerdere malen schadevergoeding toegewezen wegens schending van de AVG. Daarbij wordt aangehaakt bij artikel 6:106, eerste lid, aanhef en onder b, van het BW.[404]

632. Op 1 april 2020 wees de Afdeling bestuursrechtspraak van de Raad van State ("**Afdeling**") een viertal uitspraken, waarin zij oordeelt over schadevergoeding in verband met het verwerken van persoonsgegevens in strijd met de AVG door een bestuursorgaan.[405] De Afdeling bevestigt dat een schending van de AVG onder omstandigheden wordt aangemerkt als een "aantasting in de persoon op andere wijze" als bedoeld in artikel 6:106, eerste lid, aanhef en onder b van het BW, die aanspraak geeft op vergoeding van immateriële schade.[406]

633. Uit de uitspraken van de Afdeling volgt dat de aanspraak op schadevergoeding bij een schending van het gegevensbeschermingsrecht al snel bestaat.

634. In twee van de vier uitspraken komt de Afdeling tot de conclusie dat het recht op gegevensbescherming niet, of slechts zeer beperkt, is geschonden.[407]

635. In een derde uitspraak over een gemeente die een naam had genoemd in reactie op de vraag van andere gemeenten in het kader van een Wob-verzoek, komt de Afdeling indirect tot hetzelfde oordeel. De Afdeling overweegt dat het niet gaat om "*ernstig verwijtbaar gedrag met zo ernstige gevolgen, dat dit als inbreuk op een fundamenteel recht moet worden gekwalificeerd*".[408] Het gegevensbeschermingsrecht is in artikel 8 van het Handvest als fundamenteel recht beschouwd. De Afdeling verwijst in r.o. 31 ook naar die bepaling en stelt in haar beoordeling voorop dat het verlies van controle over persoonsgegevens een aantasting van een persoonlijkheidsrecht vormt.

636. In de zaak waarin de Afdeling concludeert dat het gegevensbeschermingsrecht wél is geschonden, kent zij zonder voorbehoud een schadevergoeding toe. Het betreft de eenmalige verstrekking van medische gegevens door de directeur van het Pieter Baancentrum in een tuchtprocedure die de betrokkene tegen hem was gestart.[409] De gegevens waren opgenomen in het verweerschrift van de directeur. Het tuchtcollege had de betrokkene hiervan in kennis gesteld. Deze heeft het college vervolgens verzocht de gegevens buiten beschouwing te laten, aan welk verzoek het tuchtcollege direct gehoor gaf.

637. De Afdeling overweegt dat in strijd is gehandeld met het gegevensbeschermingsrecht en daardoor met het recht op bescherming van de persoonlijke levenssfeer, hetgeen kan worden aangemerkt als een aantasting in de persoon als bedoeld in artikel 6:106 lid 1 onder b BW.[410] De Afdeling verlangt niet dat de betrokkene zijn immateriële schade met concrete gegevens onderbouwt:

---

[404] Rb Amsterdam, 2 september 2019,ECLI:NL:RBAMS:2019:6490, (*UWV*) (civiel), r.o. 18.
[405] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898; ABRvS 1 april 2020, ECLI:NL:RVS:2020:899; ABRvS 1 april 2020, ECLI:NL:RVS:2020:900; ABRvS 1 april 2020, ECLI:NL:RVS:2020:901.
[406] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36.
[407] ABRvS 1 april 2020, ECLI:NL:RVS:2020:900 en ABRvS 1 april 2020, ECLI:NL:RVS:2020:901.
[408] ABRvS 1 april 2020, ECLI:NL:RVS:2020:899.
[409] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898
[410] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36.

> *"[d]e nadelige gevolgen van de verstrekking van de gevoelige persoonsgegevens liggen voor de hand." (r.o. 36)*

638. De Afdeling rekent het de directeur aan dat het privacygevoelige persoonsgegevens betreft, maar overweegt verder dat de ernst en de duur van de inbreuk beperkt zijn (onderstreping advocaat):

> *"Wat betreft de ernst van de inbreuk overweegt de Afdeling dat de privacygevoelige persoonsgegevens bij een kleine groep professionals terecht zijn gekomen en dat de leden van het tuchtcollege die uit hoofde van hun functie een geheimhoudingsplicht hebben. Wat betreft de duur van de inbreuk is van belang dat het Pieter Baan Centrum na het overleggen van de gevoelige gegevens op 15 januari 2018, actie heeft ondernomen om de gegevensverstrekking ongedaan te maken." (r.o. 36)*

639. Gelet op deze omstandigheden kent de Afdeling de betrokkene een schadevergoeding toe, naar billijkheid vastgesteld op een bedrag van € 500,-.[411] Bij de bepaling van de hoogte betrekt de Afdeling de aard, duur en ernst van de inbreuk. Appellante had zich op het standpunt gesteld dat de rechtbank in eerste aanleg een te laag bedrag had toegekend, namelijk € 300,-. De Afdeling is het daarmee eens en kent een hoger bedrag toe. De Afdeling motiveert niet waarom toekenning van € 500,- schadevergoeding in dit geval billijker is dan € 300,-. Aangenomen mag worden dat in situaties waarin meerdere factoren in het voordeel van toekenning van schadevergoeding wegen dit ook zal resulteren in een hoger bedrag. Hierop zal in paragraaf 5.5.4.1 verder worden ingegaan.

640. De Afdeling volgt met zijn vier uitspraken het EBI-arrest van de Hoge Raad van 15 maart 2019.[412] In dat arrest oordeelde de Hoge Raad dat naast gevallen van geestelijk letsel ook "de aard en ernst van de normschending en van de gevolgen daarvan" een recht op immateriële schadevergoeding kunnen rechtvaardigen.[413] In zijn *NJ*-noot onder het arrest geeft Lindenbergh aan dat de Hoge Raad deze categorie niet als uitzondering op het uitgangspunt van geestelijk letsel formuleert, maar als nevengeschikte grondslag.[414]

641. Dat de Afdeling in de zaak over de gegevensverstrekking door de directeur van het Pieterbaancentrum niet verlangt dat de betrokkene zijn immateriële schade met concrete gegevens onderbouwt, is ook in lijn met het EBI-arrest.[415] De Hoge Raad heeft in het EBI-arrest immers geoordeeld dat in voorkomende gevallen de nadelige gevolgen van de normschending zo voor de hand liggen*, "dat een aantasting in de persoon kan worden aangenomen*".

642. De uitspraken maken duidelijk dat de Afdeling voor het antwoord op de vraag of aanspraak op schadevergoeding bestaat zwaar gewicht toekent aan de aard van het recht: het recht op bescherming van de persoonlijke levenssfeer. Handelen in strijd met het gegevensbeschermingsrecht levert een "persoonsaantasting" op, die de aanspraak op

[411] ABRvS 1 april 2020 ,ECLI:NL:RVS:2020:898.
[412] Hoge Raad 15 maart 2019, ECLI:NL:HR:2019:376 *(*EBI*)*, r.o. 4.2.1.
[413] Hoge Raad 15 maart 2019, ECLI:NL:HR:2019:376 *(EBI)*
[414] Hoge Raad 15 maart 2019, ECLI:NL:HR:2019:376 (*EBI*), NJ 2019/162 met annotatie van S.D. Lindenbergh, par. 11.
[415] Hoge Raad 15 maart 2019, ECLI:NL:HR:2019:376 *(*EBI*)*, r.o. 4.2.1.

immateriële schadevergoeding rechtvaardigt. De Afdeling legt de lat voor het recht op schadevergoeding bij AVG-schendingen daarmee niet bijzonder hoog.

643. Deze ruime interpretatie van artikel 6:106 eerste lid, aanhef en onder b BW, wordt ook gevolgd door lagere rechters. De rechtbank Noord-Nederland oordeelde op 15 januari 2020 dat verstrekking van (slechts) naam en adres aan één derde al resulteerde in een aanspraak op schadevergoeding. [416] De rechtbank kende een bedrag van € 250,- toe en overwoog daartoe het volgende:

> *"De rechtbank is van oordeel dat er sprake is van een schending van een fundamenteel recht, die naar zijn aard en gelet op de ernst daarvan meebrengt dat aanspraak bestaat op vergoeding van schade. Dit laatste volgt ook uit de AVG."*
>
> *[...]*
>
> *"Het enkele feit dat de schade niet exact gepreciseerd kan worden en mogelijk relatief gering van omvang is geen grond kan vormen om elke aanspraak daarop af te wijzen." (r.o. 4.106)*

644. Tot eenzelfde conclusie kwam de rechtbank Amsterdam in een zaak waarin het UWV ten onrechte bijzondere persoonsgegevens met een derde had gedeeld. [417] Het UWV had per abuis aan de nieuwe werkgever van betrokkene medegedeeld dat zij langdurig ziek was geweest. Hoewel de nieuwe werkgever haar arbeidsovereenkomst hierna gewoon verlengde, kent de rechtbank toch een schadevergoeding van € 250,- toe. De rechtbank overweegt daartoe het volgende:

> *"[H]et enkele feit dat de schade (wel reëel maar) relatief gering van omvang is [kan] geen grond vormen om elke aanspraak daarop af te wijzen. Een verordening-conforme uitleg van artikel 6:106 lid 1 BW brengt mee dat [eiseres] recht heeft op een (naar billijkheid vast te stellen) vergoeding van haar schade." (r.o. 18)*

645. Ook in het buitenland wordt een ruime interpretatie van het schadebegrip gehanteerd. De Londense *Court of Appeal* oordeelde in *Lloyd v. Google* zelfs dat naast controleverlies over persoonsgegevens niet (eens) vereist was dat afzonderlijk nog schade werd gesteld en bewezen:[418]

> "*For the reasons, I have given, I would conclude that damages are in principle capable of being awarded for loss of control of data under article 23 and section 13, even if there is no pecuniary loss and no distress*." (r.o. 70)

646. De zaak draait om het verzamelen van surfgegevens van iPhone-gebruikers door Google via Apple's webbrowser Safari. Anders dan de Nederlandse rechter, zoekt de Engelse rechter geen aansluiting bij het nationale rechtsbestel voor de toekenning van schadevergoeding. De Engelse rechter ziet in artikel 82 AVG een zelfstandige grondslag voor een vordering tot schadevergoeding.

---

[416] Rb. Noord-Holland, 15 januari 2020, ECLI:NL:RBNNE:2020:247 (*NDC Mediagroep*).
[417] Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 *(UWV*).
[418] Court of Appeal 2 oktober 2019, EWCA Civ 1599 (*Lloyd v Google*).

*5.5.4 Berekening hoogte immateriële schadevergoeding*

647. De hoogte van de schadevergoeding wordt mede bepaald door de doelstellingen van het recht op schadevergoeding in de AVG. Uit overweging 146 AVG volgt dat betrokkenen een volledige en daadwerkelijke schadevergoeding dienen te ontvangen. Daarnaast volgt uit artikel 84 AVG dat sancties *"doeltreffend, evenredig en afschrikwekkend"* moeten zijn.[419] Dat is een kwalificatie die vaker in Uniewetgeving wordt gebruikt (zie bijvoorbeeld richtlijn 2004/48 en richtlijn 2006/54). Het HvJEU bepaalde in het arrest *Manfredi* dat toekenning van niet-compensatoire schadevergoeding mogelijk is, voor zover daarbij het doeltreffendheidsbeginsel en het gelijkwaardigheidsbeginsel in acht worden genomen.[420]

648. Wanneer schadevergoeding (mede) de bescherming van het gegevensbeschermingsrecht in het algemeen als doel heeft, brengt dat met zich mee dat ook rekening gehouden moet worden met de sanctionerende werking van die schadevergoeding. Ook Hartlief benadrukt in zijn conclusie bij het eerdergenoemde EBI-arrest dat rechtshandhaving van rechten en plichten één van de functies is van het schadevergoedingsrecht. Juist wanneer er geen sprake is van aantoonbare immateriële schade of deze moeilijk aantoonbaar is, kan de sanctionering van rechten en plichten een belangrijke rol spelen bij het bepalen van schadevergoeding, aldus Hartlief.[421]

5.5.4.1 Relevante factoren hoogte immateriële schadevergoeding

649. Bij de beoordeling van de hoogte van de immateriële schadevergoeding hanteren de rechters verschillende factoren. Daarbij lijkt de algemene regel dat een weging van meerdere factoren in het voordeel van toekenning van schadevergoeding, zal resulteren in de toewijzing van een hoger bedrag.

650. De Afdeling en lagere rechters hebben de volgende factoren toegepast bij de beoordeling van de hoogte van de schadevergoeding:

a. **Aard van de gegevens**: de Afdeling nam in aanmerking de bijzondere gevoeligheid van de aard van de persoonsgegevens die zonder toestemming van de betrokkene waren verwerkt.[422]

b. **Ernst van de inbreuk/aantal ontvangers**: de Afdeling achtte het relevant dat de privacygevoelige persoonsgegevens bij een kleine groep professionals terecht waren gekomen.[423]

c. **Duur van de inbreuk:** de Afdeling achtte het relevant dat de verwerkingsverantwoordelijke direct actie had ondernomen om de gegevensverstrekking ongedaan te maken.[424]

[419] Vgl. ook overweging 151 en 152 AVG.
[420] HvJEU 13 juli 2006, C-295/04 - 298/04 *(Manfredi)*.
[421] Conclusie Advocaat-Generaal Hartlief 16 oktober 2018, ECLI:NL:PHR:2018:1295, par. 4.4.
[422] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36.
[423] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36.
[424] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 36.

d. **Aantal betrokkenen:** de rechtbank Noord-Nederland achtte het relevant dat het verlies van controle van persoonsgegevens zich maar tot één persoon beperkte.[425]

e. **Onomkeerbaarheid schade:** de rechtbank Noord-Nederland en Amsterdam achtten het relevant dat het verlies van controle van de betrokkenen over de persoonsgegevens blijvend was.[426]

651. Voor zover bij de vaststelling van de omvang van de schadevergoeding aanknoping gezocht moet worden bij artikel 6:106 BW, geldt bovendien dat rekening moet worden gehouden met alle omstandigheden van het geval. Naast bovengenoemde factoren, kunnen bijvoorbeeld worden meegenomen:

a. de **mate van verwijtbaarheid**; en

b. de **economische verhoudingen** tussen beide partijen.[427]

652. Zo zal een schadevergoeding hoger uitvallen wanneer sprake is van ernstige onachtzaamheid en/of wanneer er een economisch ongelijkwaardige verhouding bestaat tussen (grote) professionele marktpartijen enerzijds en internetgebruikers (consumenten) anderzijds.

653. De genoemde factoren sluiten aan bij de indeling van de boetecategorieën in de AVG (artikel 83 lid 4 en 5 AVG) en de beleidsregels van de AP.[428] De AP heeft voor een systeem gekozen waarbij de boete afhankelijk is gemaakt van de zwaarte en ernst van de geschonden norm en de verhouding tot andere normen in het gegevensbeschermingsrecht:

a. Hoge boetes gelden onder meer voor inbreuken die verband houden met bijzondere persoonsgegevens, de rechten van betrokkenen en (verboden) doorgifte van persoonsgegevens aan derde landen.

b. Lagere boetes worden uitgedeeld bij schending van formele verplichtingen, zoals het sluiten van een verwerkingsovereenkomst en het bijhouden van een register met persoonsgegevens.

654. Bij het vaststellen van de hoogte van de boete houdt de AP ook rekening met andere factoren, zoals de duur van de overtreding, het aantal betrokkenen en de omvang van de schade.

5.5.4.2 Forfaitaire bedragen/tarifering van schade

655. De Stichting vordert in deze zaak toewijzing van een forfaitair bedrag van €500 aan schadevergoeding per Gedupeerde. Hoewel dit niet uitdrukkelijk wordt overwogen, lijkt het erop dat de Afdeling en rechtbanken in de hiervoor aangehaalde AVG-jurisprudentie een forfaitaire vergoeding voor schade hebben toegewezen.

656. In beginsel strookt een forfaitaire vergoeding voor schade niet met het uitgangspunt van het Nederlandse schadevergoedingsrecht: de daadwerkelijke schade dient volledig vergoed te

[425] Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247, r.o. 4.107.
[426] Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490, r.o. 18.
[427] TM en EV I, Parlementaire Geschiedenis BW Boek 6, respectievelijk p. 377 en 388.
[428] Zie Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019).

worden en concreet begroot te worden met inachtneming van alle omstandigheden van het geval.[429] Op dit uitgangspunt zijn in de rechtspraak echter, zowel op praktische gronden als om redenen van billijkheid, uitzonderingen aanvaard.[430] De Stichting zal hierna toelichten dat ook in onderhavige zaak van dit uitgangspunt moet worden afgeweken en een forfaitaire vergoeding op zijn plaats is.

657. In de procedure over de Groningse aardbevingsschade vorderen twee eisers (onder andere) een veroordeling van (onder meer) de NAM en de Staat tot vergoeding van immateriële schade. In deze procedure heeft de rechtbank Noord-Nederland[431] prejudiciële vragen aan de Hoge Raad gesteld, waaronder de vraag of de schadevergoeding forfaitair vastgesteld kan worden. De Hoge Raad formuleert deze vraag als volgt:[432]

> *"Met prejudiciële vraag 9c wenst de rechtbank te vernemen in hoeverre het hoogst persoonlijke karakter van immateriële schadevergoeding zich verdraagt met het min of meer 'forfaitair' vaststellen van schadevergoeding."*

658. Ten aanzien van deze vraag overweegt de Hoge Raad als volgt (onderstreping advocaat):

> *"De omvang van een verplichting tot vergoeding van schade die bestaat in een aantasting in de persoon op andere wijze, laat zich niet 'min of meer forfaitair' vaststellen nu dat niet verenigbaar is met het hoogst persoonlijke karakter van de vordering tot vergoeding van deze schade.[433] <u>Dat laat onverlet dat de rechter kan oordelen dat de aard en de ernst van de aansprakelijkheidvestigende gebeurtenis meebrengen dat de in dit verband relevante nadelige gevolgen daarvan [...] zo voor de hand liggen, dat een aantasting in de persoon kan worden aangenomen en dat de rechter daarbij aannemelijk kan achten dat de door deze aantasting in de persoon geleden schade [...] ten minste een bepaald bedrag beloopt</u>."[434]*

659. De Hoge Raad geeft hiermee een vingerwijzing dat onder omstandigheden de schadevergoeding ten minste een bepaald bedrag kan belopen: een minimaal 'forfaitair' bedrag.

660. Een dergelijk minimaal 'forfaitair bedrag' kan worden toegewezen indien gelet op de aard en ernst van de 'aansprakelijkheidvestigende gebeurtenis' de nadelige gevolgen daarvan voor de hand liggen.

661. Ook in onderhavige zaak liggen de nadelige gevolgen zo voor hand dat een aantasting in de persoon kan worden aangenomen en de schade tenminste een bepaald bedrag dient te belopen per Gedupeerde. Oracle en Salesforce verwerken op grote schaal, langdurig en om commerciële redenen grote hoeveelheden gevoelige gegevens van de Gedupeerden. Daarbij schenden zij onder meer de AVG en artikel 11.7a Tw, het recht op bescherming van de

[429] HR 5 december 2008, ECLI:NL:HR:2008:BE9998, r.o. 3.3.
[430] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 208.
[431] Rb. Noord-Nederland 10 oktober 2018, ECLI:NL:RBNNE:2018:4009.
[432] HR 19 juli 2019, ECLI:NL:HR:2019:1278, r.o. 2.13.1.
[433] EHRM 10 februari 2011, nr. 30499/03 (*Dubetska e.a./Oekraine*), rov. 105.
[434] HR 19 juli 2019, ECLI:NL:HR:2019:1278, r.o. 2.13.7.

persoonlijke levenssfeer, het recht op privacy[435] en het gegevensbeschermingsrecht[436] (aard en ernst van de 'aansprakelijkheidvestigende gebeurtenis'). Er is sprake van massale, langdurige en ernstige inbreuken op fundamentele rechten,[437] waarvan de nadelige gevolgen verondersteld kunnen worden.

662. Lindenbergh benadrukt in zijn noot bij het EBI-arrest[438] dat bij schending van fundamentele rechten het nog meer voor de hand ligt om voor de omvang van de schadevergoeding aan te sluiten bij de aard en ernst van de normschending. Afhankelijk van het type geval kan tarifering van schadebedragen worden toegepast, waarbij het voor de hand ligt om aan alle benadeelden hetzelfde schadebedrag toe te kennen. Lindenbergh geeft als voorbeeld de massale inbreuk op de persoonlijke levenssfeer een datalek van belangrijke privégegevens:[439]

> *"Bij — kort gezegd — schending van fundamentele rechten ligt het evenwel veel meer voor de hand om de omvang van de vergoeding te relateren aan de aard en ernst van de normschending. Daarbij gaat het immers veeleer om veronderstelde gevolgen. Dat laat, afhankelijk van het type geval, ook vrij goed tarifering (categoriebedragen) van bedragen toe: bij massale inbreuk op de persoonlijke levenssfeer door een datalek van belangrijke privégegevens ligt het voor de hand om aan alle benadeelden eenzelfde bedrag toe te wijzen."*

663. De Stichting stelt zich op het standpunt dat het ook in onderhavige zaak voor de hand ligt om dergelijke tarifering toe te passen. Aan de Gedupeerden dient eenzelfde minimaal schadebedrag te worden toegekend.

664. Ook op praktische gronden dient een forfaitaire schadeberekening te worden gehanteerd. Sprake is immers van massale schendingen van fundamentele rechten. De afwikkeling van dergelijke (massa)schade wordt bevorderd door het hanteren van een forfaitaire schadeberekening. In de toelichting op de nieuwe wet Afwikkeling Massaschade in collectieve acties (WAMCA) wordt hierover opgemerkt dat het gebruik van een onderverdeling in vaste categorie(bedragen) ervoor zorgt dat de massaschade collectief kan worden afgewikkeld.[440] Door zo veel mogelijk met categorieën te werken[441] wordt er als het ware geabstraheerd van de individuele gevallen. Voor een efficiënte en effectieve massaschaderegeling is het aldus onvermijdelijk om te abstraheren van individuele omstandigheden.[442]

665. Daarnaast bepaalt artikel 6:97 BW dat de rechter de schade begroot op de wijze die het meest met de aard ervan in overeenstemming is. Hiermee ontstaat ruimte om de schade te begroten aan de hand van tarifering/schadecategorieën.[443]

---

435 Artikel 7 van het Handvest.
436 Artikel 8 van het Handvest en de AVG.
437 Schending van een fundamenteel recht lijkt geen separaat criterium te zijn, nu de Hoge Raad spreekt over een 'aansprakelijkheidvestigende gebeurtenis'. Anders: conclusie A-G Hartlief, ECLI:NL:PHR:2018:1295, r.o. 5.4 e.v., maar hij wordt daarin niet gevolgd door de Hoge Raad. In de literatuur wordt soms ook anders bepleit. Zie hierover: Janssen en Bloo-Kroes, 'De jurisprudentiële ontwikkelingen van immateriële schadevergoeding bij een bijzondere normschending', *MvV* 2019, nummer 10.
438 HR 15 maart 2019, ECLI:NL:HR:2019:376 (*EBI*), *NJ* 2019/162 met annotatie van S.D. Lindenbergh, par. 18.
439 HR 15 maart 2019, ECLI:NL:HR:2019:376 (*EBI*), *NJ* 2019/162 met annotatie van S.D. Lindenbergh, par. 18.
440 Kamerstukken II, vergaderjaar 2016–2017, 34 608, nr. 3 5 pagina's 5 en 6.
441 Kamerstukken II, vergaderjaar 2016–2017, 34 608, nr. 3 5 pagina 52.
442 T. Hartlief, Massaschade en de regelende rechter, Blog NJB 13 november 2017.
443 Kamerstukken II, vergaderjaar 2016–2017, 34 608, nr. 3 5 pagina 52.

666. Gelet op het voorgaande vordert de Stichting in onderhavige zaak toewijzing van een forfaitair bedrag aan schadevergoeding per Gedupeerde.

5.5.4.3 Toepassing op onderhavige zaak

667. De Stichting meent dat de door de achterban van de Stichting geleden schade zich leent voor forfaitaire begroting, aan de hand van de door de Afdeling en lagere rechters geformuleerde factoren (zie paragraaf 5.5.4.1):

a. **Aard van de gegevens**: Oracle en Salesforce verwerken grote hoeveelheden persoonlijke gegevens per betrokkene. Met deze gegevens worden profielen gemaakt van de internetgebruiker die op grote schaal ingezet worden voor het personaliseren van advertenties. Die profielen bevatten informatie, zoals geslacht, woonplaats, leeftijd, aantal apparaten in gebruik, etc., maar ook gevoeligere informatie zoals de informatie waar iemand naar zoekt en heeft gezocht, de websites die iemand bezoekt en heeft bezocht, de artikelen die iemand leest en heeft gelezen en koopgedrag. Uit die gegevens worden voorkeuren en interesses afgeleid. Zeker is dat de verzamelde gegevens een zeer nauwkeurig en indringend beeld geven van de levens van de betrokkenen. De aard van de gegevens is daarom gevoelig te noemen, anders dan het geval is bij bijvoorbeeld enkel een naam en adres. Bovendien is inherent aan de handelwijze van Oracle en Salesforce dat ook bijzondere persoonsgegevens worden verwerkt.

b. **Ernst van de inbreuk/aantal ontvangers**: Oracle en Salesforce schenden de AVG op grove wijze. Zij delen de volmaakte profielen waarin ook gevoeligere gegevens zijn opgenomen, enkel voor commercieel gewin. Dat sprake is van profilering maakt dat de schending als bijzonder ernstig moet worden aangemerkt en dat er sprake is van een verhoogd risico voor de rechten van de betrokken. Hetzelfde geldt voor de hoeveelheid gegevens die worden verwerkt. Dat alles blijkt ook uit overweging 75 AVG. Oracle en Salesforce schenden bovendien niet één bepaling van de AVG en Tw maar een veelheid. Deze verwerking van persoonsgegevens vindt plaats zonder dat Oracle en Salesforce daarvoor een geldige grondslag hebben. Daarbij overtreden zij bovendien de fundamentele beginselen van transparantie en dataminimalisatie en het verbod op doorgifte. In tegenstelling tot voornoemde uitspraken, waar de gegevens slechts met één of enkele partijen werden gedeeld, delen Oracle en Salesforce de persoonlijke gegevens met een zeer grote en onbepaalde groep ontvangers, mogelijk duizenden partijen per veiling.

c. **Duur van de inbreuk:** Oracle en Salesforce schenden de AVG al sinds de toepasselijkheid ervan. De inbreuken vinden op dit moment nog steeds plaats en blijven – indien niet wordt ingegrepen – voortduren. In tegenstelling tot voornoemde uitspraken, waar de inbreuk steeds van korte duur was, is in dit geval de inbreuk voortdurend.

d. **Aantal betrokkenen:** de schendingen hebben een industriële omvang en raken elke internetgebruiker, waar ook ter wereld en in ieder geval in Nederland. Onderzoek toont aan dat de cookies van Oracle en Salesforce via een groot deel van Nederlands meest populaire websites worden geplaatst (zie **Productie 16** en paragraaf 3.3.1). Het is zeer

waarschijnlijk dat iedere Nederlandse ingezetene die regelmatig het internet gebruikt deze websites wel eens heeft bezocht.

e. **Onomkeerbaarheid schade:** Oracle en Salesforce hebben persoonsgegevens (onrechtmatig) bekend gemaakt aan derden, waardoor het verlies van controle over de persoonsgegevens blijvend is. Er is immers niet meer te achterhalen in wiens handen persoonsgegevens zijn gevallen, nu de gegevens zijn verhandeld en doorverhandeld tussen honderden partijen waarvan de Stichting (en vermoedelijk ook Oracle en Salesforce) de identiteit niet kennen. Aangenomen moet worden dat deze informatie voor eeuwig beschikbaar zal blijven aan commerciële partijen. De schade is daarmee onomkeerbaar geworden. Een verzwarende omstandigheid is verder dat Oracle en Salesforce de persoonsgegevens hebben doorgegeven aan de Verenigde Staten, terwijl niet gezegd kan worden dat dat land een passend beschermingsniveau biedt (zie hierover paragraaf 4.6.5).

668. De Stichting meent dan ook dat, gelet op de omstandigheden van dit geval en net als in het geval van de recente uitspraak van de Afdeling,[444] een forfaitaire vergoeding van minimaal € 500 per betrokkene meer dan redelijk is. In vergelijking met de zaak waar de Afdeling dat bedrag op zijn plaats vond, gaat het in casu om veel ernstiger schendingen en gevolgen. De Afdeling vond een bedrag van € 500 billijk, terwijl het ging om één betrokkene, een beperkt aantal persoonsgegevens, gedeeld in de besloten kring van een tuchtprocedure, gedurende korte periode, waarbij direct maatregelen zijn genomen om de rechten van de betrokkene te waarborgen.

669. Dit geldt te meer, nu op grond van artikel 6:106 BW gekeken moet worden naar alle omstandigheden van het geval, waaronder de economische verhoudingen.[445] Kenmerkend in onderhavig geval is dat Oracle en Salesforce – twee beursgenoteerde tech giganten – jarenlang, structureel onrechtmatig persoonsgegevens hebben verwerkt en winsten hebben genoten ten koste van consumenten, te weten Nederlandse internetgebruikers. Die internetgebruikers hebben amper mogelijkheden om tegen het onrechtmatige gedrag van Gedaagden op te treden. Ook dat dient mee te wegen in de beoordeling.

670. Een vergoeding van (minimaal) een bedrag van € 500 komt evenzeer juist voor als wordt gekeken naar de boetecategorieën van de AP (zie randnummer 653 hiervoor). De schendingen die in deze dagvaarding zijn genoemd, vallen onder de hoogste boetecategorie, nu het mede gaat om gevoelige persoonsgegevens en de doorgifte daarvan.

671. Ook in vergelijking met de Verenigde Staten – het thuisland van Oracle en Salesforce – is een vergoeding van (minimaal) € 500 gerechtvaardigd, nu dit bedrag valt binnen de bandbreedte waarin de wet voorziet.[446]

[444] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898.
[445] TM en EV I, Parlementaire Geschiedenis BW Boek 6, respectievelijk p. 377 en 388.
[446] Section 11 (179.150) van de CCPA; DataGuide 2018, p. 39-40.

*5.5.5 Materiële schadevergoeding*

5.5.5.1 Inleiding

672. Zoals eerder toegelicht, geeft artikel 82 AVG de grondslag voor immateriële én materiële schadevergoeding ten gevolge van een inbreuk op de AVG.

673. Overweging 7 AVG bepaalt dat natuurlijke personen controle over hun eigen persoonsgegevens dienen te hebben. Overweging 85 AVG bepaalt verder dat een inbreuk in verband met persoonsgegevens kan resulteren in lichamelijke, materiële of immateriële schade voor natuurlijke personen, zoals verlies van controle over hun persoonsgegevens.

674. De Stichting zal hierna toelichten dat persoonsgegevens economische waarde vertegenwoordigen. Gedupeerden zijn de controle over hun persoonsgegevens verloren door de handelwijze van Oracle en Salesforce. De daaraan gekoppelde economische waarde is hen ontnomen. Zij hebben aldus materiële schade geleden. Deze schade dient door Oracle en Salesforce vergoed te worden.

675. De Stichting zal in dat verband toelichten dat voor de vergoeding van de materiële schade aangesloten kan worden bij de marktwaarde van de persoonsgegevens. De Stichting zal tevens toelichten dat zij een vordering jegens Oracle en Salesforce tot het verstrekken van informatie instelt nu niet de Stichting, maar Oracle en Salesforce over de relevante gegevens beschikken om deze marktwaarde te begroten. De Stichting zal tevens een verzoek doen tot het benoemen van een deskundige die onderzoek kan doen naar de marktwaarde van de persoonsgegevens in het geval Oracle en Salesforce niet vrijwillig deze gegevens overhandigen/inzichtelijk maken.

5.5.5.2 Economische waarde van persoonsgegevens

676. Aan elk van de door Oracle en Saleforce onrechtmatig verwerkte persoonsgegevens kan een waarde worden toegekend. Bedrijven hebben immers geld over voor de gegevens, omdat de gegevens hen onder meer in staat stellen om gepersonaliseerde advertenties aan te bieden op websites en daarmee hun bedrijfsbelangen te bevorderen.[447]

677. Het verzamelen en verwerken van (persoons)gegevens wordt al geruime tijd omschreven als de meest waardevolle bron van inkomsten of 'the new oil'.[448] Het wordt omschreven als de belangrijkste aanjager van de wereldwijde economie.[449]

> *"The world's most valuable resource is no longer oil, but data."*[450]

[447] Competition and Markets Authority, *The commercial use of consumer data, Report on the CMA's call for information*, juni 2015, 61-63; United Nations, Department of Economic and Social Affairs, *Data Economy: Radical transformation or dystopia?*, Frontier Technology Quarterly.
[448] Zie toespraak voormalig EU Commissaris Kroes: http://europa.eu/rapid/pressrelease_SPEECH-12-149_en.htm.
[449] Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (6 mei 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; S.A. Elvy, *Paying for privacy and the personal data economy,* Columbia law review, oktober 2017, vol. 117, nr. 6, p. 1371-1372.
[450] Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (6 mei 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

678. Persoonsgegevens vertegenwoordigen materiële, economische waarde. Dit wordt ook bevestigd in de rechtspraak in het Verenigd Koninkrijk en onderzoeksrapporten in de ons omringende landen.

679. Zo oordeelde het gerechtshof in het Verenigd Koninkrijk dat zeggenschap over persoonsgegevens een waardevol goed is en dat het duidelijk is dat de persoonsgegevens economische waarde hebben.[451]

> *"It is also clear that a person's BGI has economic value: for example, it can be sold. It is commonplace for EU citizens to obtain free wifi at an airport in exchange for providing their personal data. If they decline to do so, they have to pay for their wifi usage. The underlying reality of this case is that Google was able to sell BGI collected from numerous individuals to advertisers who wished to target them with their advertising. That confirms that such data, and consent to its use, has an economic value. Accordingly, in my judgment, a person's control over data or over their BGI does have a value, so that the loss of that control must also have a value."*[452]

680. De Boston Consulting Group bevestigde in 2012 reeds dat de waarde van persoonsgegevens gelijk gesteld kan worden aan andere betaalmiddelen en dat deze gegevens van groot belang zijn voor de wereldwijde economie.

> *"In an increasingly digital society, personal data has become a new form of currency."*[453]
>
> *(...)*
>
> *"From a macroeconomic perspective, it becomes clear that digital data is already a growth driver in an otherwise flagging economy."*[454]

681. Verder voorspelde de Boston Consulting Group dat de waarde die door persoonsgegevens wordt gecreëerd elk jaar aanzienlijk oploopt binnen Europa.[455] De Franse instelling CIGREF heeft de bevindingen uit het rapport van Boston Consulting Group onderschreven.[456]

682. Een onderzoeksrapport van het Deutsches Institut für Vertrauen und Sicherheit im Internet bevestigt niet alleen dat persoonsgegevens waarde in geld vertegenwoordigen, maar wijst er ook op dat het burgerlijk recht aldus voldoende bescherming moet bieden om deze waarde te beschermen.[457]

[451] Court of Appeal 2 oktober 2019, EWCA Civ 1599 (*Lloyd v Google*).
[452] Court of Appeal 2 oktober 2019, EWCA Civ 1599 (*Lloyd v Google*), r.o. 46.
[453] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[454] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[455] Boston Consulting Group, The value of our digital identity, 2012, p. 3.
[456] CIGFREF, L'économie des données personnelles, oktober 2015, p. 8.
[457] Deutsches Institut für Vertrauen und Sicherheit im Internet, Daten als Handelsware, 2016, p. 18, 66-67.

683. Ook volgt uit een onderzoek van Tim Morey, verricht onder internetgebruikers, dat persoonsgegevens een waarde in geld vertegenwoordigen. Uit dit onderzoek komt het volgende beeld naar voren ten aanzien van de waarde van persoonsgegevens:[458]

The three tiers of value

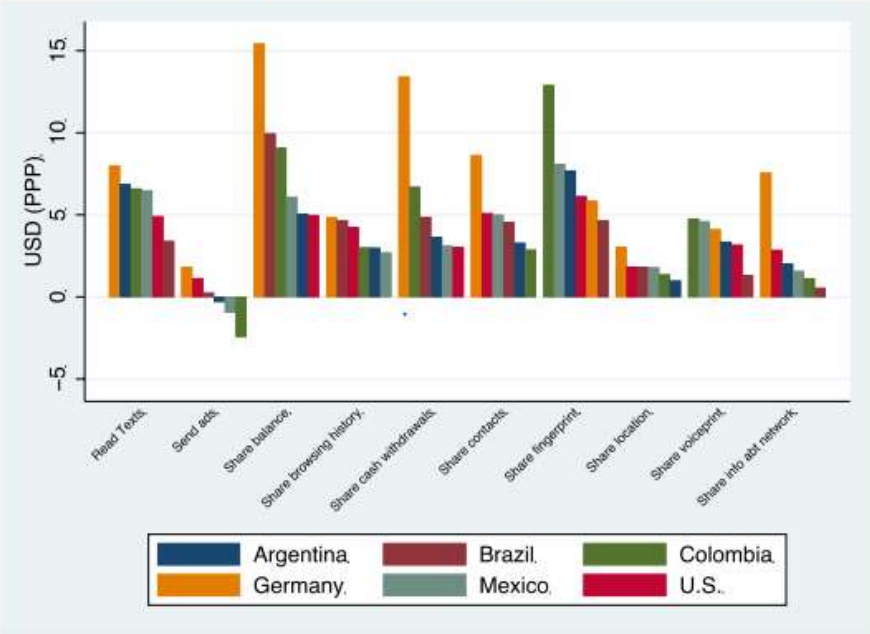
684. Uit het bovenstaande overzicht is af te leiden dat aan de persoonsgegevens een individuele waarde kan worden toegekend en dat de waarde van deze gegevens mogelijk afhangt van het type informatie. De deelnemers van het onderzoek gaven bijvoorbeeld aan een burgerservice nummer van een gebruiker waardevoller te vinden dan de demografische gegevens van een gebruiker.

685. Het onderzoek van Tim Morey werd ook aangehaald in het kader van het bepalen van de economische waarde van persoonsgegevens door de eisers in de zaak Brown et al v Google in de Verenigde Staten. De zaak Brown et al v Google is een collectieve actie zaak tegen Google,[459] waarin Google er onder meer van wordt beschuldigd onrechtmatig te handelen door persoonsgegevens te verzamelen van personen die gebruikmaken van de privémodus van de Chrome internetbrowser.

686. Recent onderzoek bevestigt dat persoonsgegevens waarde in geld vertegenwoordigen, maar onderkent dat het lastig is om de exacte waarde van persoonsgegevens te bepalen.[460] Het onderzoek dat is uitgevoerd door Jeffrey Prince en Scott Wallsten[461] onder internetgebruikers in de Verenigde Staten, Mexico, Brazilië, Colombia, Argentinië en Duitsland, laat het volgende beeld zien omtrent de uiteenlopende waarden van (persoons)gegevens:[462]

[458] T. Morey, What's Your Personal Data Worth?, *DESIGN MIND* (18 januari 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039syour-personal-data-worth.html.
[459] Brown et al v Google LLC et al, U.S. District Court, Northern District of California, No. 20-03664, par. 70.
[460] Zie onder meer R. Jia , What is My Data Worth?, *Berkeley Artificial Intelligence Research*, 2019; J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*.
[461] Scott Wallsten is President en Senior Fellow bij het Technology Policy Institute. Jeff Prince is hoogleraar bedrijfseconomie aan de Kelley School of Business, Indiana University.
[462] J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*, p. 6.

**Figure 2: Average Payment Consumers Would Demand for Permission to Share Data to Share Data Across Countries by Feature**




687. Uit het bovenstaande overzicht is af te leiden dat de waarde van persoonsgegevens niet alleen mogelijk afhangt van de categorie gegevens, maar mogelijk ook per land verschilt. Uit het onderzoek komt aanvullend naar voren dat de leeftijd en geslacht van een deelnemer mogelijke factoren zijn die tevens van invloed kunnen zijn op het bepalen van de waarde van persoonsgegevens.[463]

688. Verder bevestigt de Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten de economische waarde van data.[464] De Richtlijn (EU) 2019/770 ziet op overeenkomsten waarbij een handelaar aan de consument digitale inhoud of een digitale dienst levert of zich daartoe verbindt (artikel 3 lid 1). De consument dient in ruil daarvoor een prijs te betalen of een andere tegenprestatie dan geld te leveren, in de vorm van persoonlijke gegevens of andere data.[465] Hiermee krijgt het betalen in de vorm van persoonsgegevens een met geld te vergelijken waarde en erkent de Richtlijn (EU) 2019/770 de economische waarde van persoonsgegevens. In het voorstel voor de Richtlijn (EU) 2019/770 wordt dit ook bevestigd:

> *"In de digitale economie heeft informatie over natuurlijke personen voor marktdeelnemers vaak en in toenemende mate een met geld te vergelijken waarde. Digitale inhoud wordt dikwijls niet tegen betaling van een prijs, maar tegen een*

[463] J. Prince & S. Wallsten, How Much is Privacy Worth Around the World and Across Platforms?, January 2020, *Technology Policy Institute*, p. 1.
[464] Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten, PbEU 22 mei 2019. De richtlijn is op 11 juni 2019 in werking getreden en moet uiterlijk op 1 juli 2021 zijn omgezet in nationale regelgeving. De nieuwe regels in het nationaal recht dienen dan vanaf 1 januari 2022 in werking te treden.
[465] Mr. dr. C. Spierings, 'Het nieuwe goud: betalen met data', *MvV* 2019, p. 207-214; Mr. dr. M.Y. Schaub, 'Nieuwe regels voor de consumentenkoop en overeenkomsten met betrekking tot digitale inhoud', *NtER* 2019-9-10, p. 243-249.

*andere tegenprestatie dan geld geleverd, bijvoorbeeld in ruil voor het verlenen van toegang tot persoons- of andere gegevens".*[466]

689. Uit het voorgaande volgt dat persoonsgegevens economische waarde vertegenwoordigen.

5.5.5.3 Het bepalen van de omvang van de materiële schade

690. Oracle en Salesforce hebben op grote schaal, langdurig en voor commerciële doeleinden de persoonsgegevens van de Gedupeerden verzameld en verwerkt. Hiermee hebben zij onder meer inbreuk gemaakt op de AVG en de Tw, hebben zij onrechtmatig gehandeld, dan wel zijn zij ongerechtvaardigd verrijkt. Gedupeerden zijn de controle over hun persoonsgegevens verloren en zijn in hun privacybelangen geschaad. Gedupeerden hebben schade geleden (artikel 6:96 BW). Gedupeerden kunnen niet langer de controle uitoefenen op en beslissen over het gebruik van hun persoonsgegevens. Deze schade moet vergoed worden.

691. In geval er een verplichting tot vergoeding van schade bestaat, is het uitgangspunt dat volledige (concrete) schadevergoeding plaatsvindt (artikel 6:95 BW). Op het uitgangspunt van concrete schadeberekening zijn in de rechtspraak, zowel op praktische gronden als om redenen van billijkheid, in bijzondere gevallen uitzonderingen aanvaard.[467]

692. Onderhavige zaak betreft een bijzonder geval. Het gaat hier om persoonsgegevens die op grote schaal, langdurig en voor commerciële doeleinden zijn verzameld en verwerkt. De Gedupeerden zijn de controle over hun persoonsgegevens verloren en in hun privacybelangen geschaad door de handelwijze van Oracle en Salesforce. De schade laat zich echter niet eenvoudig begroten of bewijzen, maar heeft zich wel veelvuldig en op grote schaal voorgedaan bij Nederlandse internetgebruikers. Gelet op een doelmatige schadeafwikkeling en billijkheidsoverwegingen is een snelle afwikkeling naar objectieve maatstaven onder deze omstandigheden zeer wenselijk.

693. Bij de berekening van de materiële schade dient als uitgangspunt te worden genomen dat persoonsgegevens een economische waarde vertegenwoordigen, zo ook de persoonsgegevens die Oracle en Salesforce van de Gedupeerden buit hebben gemaakt. De omvang van de waarde van het verlies van de controle over de persoonsgegevens zou gelijk gesteld kunnen worden aan de waarde die de persoonsgegevens in het normaal economisch verkeer hebben[468] of de waarde die daaraan in het economisch verkeer wordt toegekend.

694. Oracle en Salesforce zouden in dat geval de (objectieve) marktwaarde van (het gebruik van de) persoonsgegevens dienen te vergoeden aan de Gedupeerden.[469] De Stichting stelt zich op het standpunt dat de omvang van de marktwaarde moet worden begroot op de waarde die het gebruik van de persoonsgegevens op de RTB markt heeft. Deze waarde kan bijvoorbeeld volgen uit de prijs die door alle partijen wordt betaald op de RTB markt om van de persoonsgegevens gebruik te mogen maken. Dit is immers de prijs die Gedupeerden aldus hadden kunnen

[466] Zie overweging 13 in het Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud, Brussel, 9 december 2015, COM(2015) 634 final, 2015/0287 (COD).
[467] HR 5 december 2008, ECLI:NL:HR:2008:BE9998, *NJ* 2009/387 (*Rijnstate/R.*); Groene Serie Schadevergoeding, artikel 6:98 BW, par. 4.3.
[468] Parlementaire Geschiedenis, BW Boek 6, p. 818-819.
[469] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par 4.6.2 en 5.6.5.

bedingen voor het gebruik van hun persoonsgegevens vanaf het van toepassing zijn van de AVG, te weten 25 mei 2018.

5.5.5.4 Informatieverzoek en aanwijzen deskundige

695. De Stichting beschikt niet over deze informatie. De door Oracle en Salesforce gepubliceerde (jaar)cijfers laten weliswaar miljarden Euro's aan inkomsten zien, maar geven onvoldoende inzicht in de revenuen die specifiek worden gegenereerd en de onderlinge marktprijzen die worden gehanteerd voor het gebruik van de persoonsgegevens van Nederlandse internetgebruikers.

696. De enige manier om deze gegevens boven tafel te krijgen, is via de betrokken marktpartijen. In hoofdstuk 7 "Bewijs" zal de Stichting uiteenzetten van welke juridische middelen gebruik kan worden gemaakt om deze informatie boven tafel te krijgen. De Stichting zal in dat hoofdstuk tevens de ingestelde vordering jegens Oracle en Salesforce tot het verstrekken van informatie nader toelichten.

697. Onderzoek door een deskundige naar de marktwaarde van (het gebruik van) de persoonsgegevens van de Gedupeerden vanaf 25 mei 2018, waarbij Oracle en Salesforce worden bevolen om aan dat onderzoek volledige medewerking te verlenen, kan in dat kader uitkomst bieden. De Stichting verzoekt de rechtbank dan ook om een deskundige aan te wijzen ex. artikel 194 Rv.

## 5.6 Aansprakelijkheid van Oracle vanwege Datalek

698. Eerder dit jaar heeft een datalek plaatsgevonden in verband met Oracle's DMP. Dat betekent dat Oracle niet heeft voldaan aan haar verplichting om de persoonsgegevens die zij verwerkt adequaat te beveiligen. Dit levert een overtreding van artikel 5 lid 1 sub f en 32 AVG op. Het incident levert bovendien een inbreuk in verband met persoonsgegevens zoals bedoeld in artikel 4 lid 12 en 33 en 34 AVG op. Oracle had het incident daarom moeten melden bij de toezichthoudende autoriteit(en) en betrokkenen. Dat heeft zij niet gedaan. Zie hierover paragraaf 4.7.

699. Uit overweging 85 AVG volgt dat een datalek kan leiden tot materiële of immateriële schade. Als voorbeelden van schade worden onder meer genoemd: financiële verliezen, reputatieschade en verlies van controle over persoonsgegevens.[470]

700. Die schade heeft zich hier voorgedaan. Door de schendingen is er op detailniveau informatie van een enorm aantal internetgebruikers verspreid. Het gaat vermoedelijk mede om persoonsgegevens van de Gedupeerden die worden vertegenwoordigd door de Stichting en zeer waarschijnlijk om de gegevens van een nog veel grotere groep. Zeker is dat miljarden persoonsgegevens op straat zijn komen te liggen. Betrokkenen hebben immateriële schade geleden onder meer als gevolg van het verlies van controle dat zij hebben geleden door het handelen van Oracle.

701. De Stichting meent dat voor de schade die is ontstaan als gevolg van het datalek een forfaitaire vergoeding van minimaal € 100,- per betrokkene redelijk is. De Stichting verlangt daarnaast

[470] Deze voorbeelden worden ook genoemd in overweging 75.

dat Oracle informatie verstrekt over de aard en oorzaak van het datalek, alsmede over de omvang daarvan, de gecompromitteerde gegevens en de groep van gedupeerde betrokkenen.

## 5.7 Subsidiair: Overige aansprakelijkheidsgronden

### *5.7.1 Aansprakelijkheid op grond van de onrechtmatige daad*

702. De Stichting baseert haar vorderingen primair op aansprakelijkheid op grond van de AVG. Aansprakelijkheid kan echter evenzeer worden vastgesteld op grond van artikel 6:162 BW. Subsidiair baseert de Stichting haar vorderingen dan ook op de onrechtmatige daad (artikel 6:162 BW).

703. In overweging 146 AVG is bepaald dat de verordening eventuele eisen tot schadeloosstelling wegens inbreuken op andere regels in het EU-recht of het nationale recht onverlet laat. De mogelijkheid om een vordering op grond van artikel 6:162 BW in te stellen, is aldus parallel mogelijk naast een vordering op grond van de AVG.[471]

704. De Stichting zal hierna toelichten dat bij de beoordeling van haar vorderingen op grond van de onrechtmatige daad de uitgangspunten van de AVG dienen te worden meegenomen. Artikel 6:162 BW dient aldus, voor zover nodig, conform de AVG te worden uitgelegd.

705. De Stichting zal tevens toelichten dat aan de vereisten voor een succesvol beroep op artikel 6:162 BW (onrechtmatige daad, toerekenbaarheid, relativiteit, causaal verband en schade) is voldaan.

### *5.7.2 Artikel 6:162 BW dient AVG-conform te worden uitgelegd*

706. Binnen het EU-recht is het leerstuk van de EU-conforme interpretatie belangrijk om zeker te stellen dat het EU-recht goed doordringt tot in de verschillende lagen van de nationale wetgeving. Volgens dit leerstuk zijn de nationale rechter en nationale uitvoeringsorganen gehouden het van toepassing zijnde nationale recht zoveel mogelijk op die manier te interpreteren dat de nakoming van de verplichtingen die uit het Europese recht voortvloeien, wordt verzekerd.[472] De nationale norm dient zoveel mogelijk te worden uitgelegd in het licht van de bewoordingen en het doel van de betrokken Europeesrechtelijke bepaling om de daarmee beoogde doelstellingen te bereiken. Het leerstuk van de EU-conforme interpretatie geldt onder meer voor richtlijnen, verdragsbepalingen, verordeningen en beginselen.[473]

707. De Stichting stelt zich op het standpunt dat in de onderhavige zaak het leerstuk van de EU-conforme interpretatie ertoe dient te leiden dat artikel 6:162 BW, voor zover nodig, conform de AVG dient te worden uitgelegd op een wijze die ten volle recht doet aan de doelstellingen van de AVG. Dat wil zeggen dat bij de beoordeling van de vorderingen op basis van de onrechtmatige daad van de Stichting de uitgangspunten van de AVG ten aanzien van de

---

[471] Groene Serie Onrechtmatige daad, par. 12.4.7.3 Verhouding van art. 82 van Verordening 2016/679 tot de onrechtmatige daad. Dit wordt ook bevestigd door de Afdeling in onder meer ABRvS 1 april 2020, ECLI:NL:RVS:2020:900, r.o. 25 op basis van het implementatietabel bij artikel 82 AVG in de *Kamerstukken II* 2017/18, 34851 nr. 3.
[472] HvJEG 10 april 1984, 14/83 (*Von Colson en Kamann*), r.o. 26; HvJEG 13 november 1990, C-106/89 (*Marleasing*), r.o. 8; J.R. van den Brink, De uitvoering van Europese subsidieregelingen in Nederland (*R&P* nr. SB6) 2012/3.2.2.3.
[473] J.R. van den Brink, De uitvoering van Europese subsidieregelingen in Nederland (*R&P* nr. SB6) 2012/3.2.2.3; HvJEG 7 januari 2004, C-60/02, (*Rolex*), r.o. 59; HvJEG 13 maart 2008, gevoegde zaken C-383/06-C-385/06 (*ESF-arrest*); HvJEG 17 januari 2008, C-246/06 (*Velasco Navarro*), r.o. 35; HvJEG 5 oktober 1994, C-165/91 (*Van Munster*).

beoordeling van de schendingen, de schade en het causaal verband dienen te worden meegenomen.[474]

708. In dat verband wijst de Stichting ook naar een uitspraak van de rechtbank Amsterdam van 2 september 2019 over de uitleg van artikel 6:106 lid 1 BW (onderstreping advocaat):[475]

> *"Daarnaast dient als uitgangspunt te gelden dat in de AVG zelf uitgangspunten zijn geformuleerd voor de beoordeling van de schending, de schade en het causaal verband daartussen. Daarbij heeft de AVG als uitgangspunt (paragraaf 146 Considerans) dat het begrip „schade" ruim moet worden uitgelegd in het licht van de rechtspraak van het Hof van Justitie, op een wijze die ten volle recht doet aan de doelstellingen van die verordening. Artikel 6:106 lid 1 BW zal voor zover nodig verordening-conform dienen te worden uitgelegd."*

*5.7.3 Onrechtmatige daad, relativiteit en toerekenbaarheid*

709. Volgens artikel 6:162 BW is voor een vordering tot schadevergoeding een onrechtmatige daad vereist. Dit kan zijn een inbreuk op een recht, een doen of nalaten in strijd met een wettelijke plicht en een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt.

710. In hoofdstuk 4 heeft de Stichting de schendingen van de AVG, de Tw en relevante grondrechten door Oracle en Salesforce toegelicht.

711. De AVG is een Europese verordening. Europese verordeningen zijn verbindend in al hun onderdelen en rechtstreeks toepasselijk in elke lidstaat (artikel 288 VWEU). Overeenkomstig artikel 93 van de Grondwet kunnen direct werkende bepalingen uit de Europese verordeningen eveneens gekwalificeerd worden als (equivalent van) wettelijke plichten in de zin van artikel 6:162 lid 2 BW.[476] Hieruit volgt dat de schendingen van de AVG door Oracle en Salesforce gekwalificeerd kunnen worden als een schending van een wettelijke plicht. Dit levert dus een onrechtmatige daad op.

712. De inbreuk op de Tw levert ook zonder meer een onrechtmatige daad op nu er in strijd met een wettelijke plicht (artikel 11.7a Tw) is gehandeld.

713. Daarnaast kunnen de handelingen van Oracle en Salesforce gekwalificeerd worden als een handelen in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. De Stichting heeft in hoofdstuk 3 gemotiveerd uiteengezet dat Oracle en Salesforce een onmisbare rol spelen in de handel in persoonsgegevens in het kader van het RTB systeem onder meer door middel van cookie syncing en de overige in paragraaf 3.2 beschreven handelingen. Als DMPs vormen zij de centrale datahubs in de advertentiemarkt. Oracle en Salesforce handelen in strijd met een maatschappelijke zorgvuldigheidsnorm door zich aldus

[474] M. Wissink, 2014, *The influence of EU law on national private law*, Deventer: Kluwer, p. 119 e.v.; J.R. van den Brink, De uitvoering van Europese subsidieregelingen in Nederland (*R&P* nr. SB6) 2012/3.2.2.3.
[475] Rb Amsterdam, 2 september 2019,ECLI:NL:RBAMS:2019:6490, (UWV) (civiel), r.o. 18.
[476] Groene Serie Onrechtmatige daad, par. 5.2.3 Verdragsbepalingen en Unierecht als wettelijke plichten; A.S. Hartkamp & C.H. Sieburgh, Asser/Hartkamp & Sieburgh 6-IV 2015/16.

op te stellen als gevolg waarvan de Gedupeerden de controle over hun persoonsgegevens zijn verloren, in hun privacybelangen zijn geschaad en schade hebben geleden.

714. Daarnaast dient aan het relativiteitsvereiste te worden voldaan. Het relativiteitsvereiste houdt in dat de norm moet strekken tot de bescherming van de benadeelde in het geschonden belang.[477] Aan het relativiteitsvereiste is zonder meer voldaan nu Oracle en Salesforce onrechtmatig persoonsgegevens verwerken en de AVG strekt tot bescherming van de persoonsgegevens van de Gedupeerden.[478] Aan het relativiteitsvereiste is ook zonder meer voldaan bij schending van artikel 11.7a Tw door Oracle en Salesforce. Artikel 11.7a Tw strekt immers specifiek tot bescherming van de persoonsgegevens en de persoonlijke levenssfeer van gebruikers van de openbare telecommunicatienetwerken en telecommunicatiediensten bij het gebruik van cookies.[479] Door zonder aan de vereisten van artikel 11.7a Tw te voldoen en cookies te plaatsen op de randapparatuur van internetgebruikers schenden Oracle en Salesforce derhalve het specifieke belang dat de bepaling tracht te beschermen.

715. Aan het relativiteitsvereiste is aldus voldaan: alle geschonden wetten (AVG en Tw) strekken naar hun aard ter bescherming van de belangen van de Nederlandse internetgebruikers. Bij een handelen in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, is het relativiteitsvereiste reeds "ingebakken" in de ongeschreven zorgvuldigheidsnorm.[480]

*5.7.4 Toerekening*

716. Vervolgens dient gekeken te worden naar de vraag of aan het vereiste van de toerekening is voldaan. De onrechtmatige gedraging moet aan de dader toegerekend kunnen worden krachtens schuld, wet of verkeersopvatting.[481] Het uitgangspunt bij de AVG is dat de mate van schuld er in beginsel niet toe doet, aangezien het een risicoaansprakelijkheid betreft (zie paragraaf 5.3). Dit heeft tot gevolg dat aan het vereiste van toerekening is voldaan nu artikel 6:162 BW (en artikel 6:163 BW) zoveel mogelijk conform de AVG dient te worden uitgelegd.

717. Tevens is aan het vereiste van toerekening voldaan nu de schendingen van de AVG aan Oracle en Salesforce kunnen worden toegerekend krachtens schuld. Ook zijn de handelingen van Oracle en Salesforce in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt, kunnen worden toegerekend krachtens schuld. Het is immers aan hen te wijten dat de Gedupeerden de controle over de persoonsgegevens zijn verloren en in hun privacybelangen zijn geschaad.

*5.7.5 Causaal verband*

718. Aangezien artikel 6:162 BW (en artikel 6:98 BW) conform de AVG dient te worden uitgelegd, geldt ook bij de onrechtmatige daad dat het causaal verband (csqn-verband) reeds aangenomen wordt (zie paragraaf 5.3). In de literatuur wordt breed aangenomen dat in het

[477] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, p. 29.
[478] Overweging 2 AVG.
[479] Memorie van Toelichting, *Kamerstukken II*, 1996/97, 25 533, nr. 3, p. 4, 7 en 38-39.
[480] Groene Serie Onrechtmatige daad, art. 6:163 BW, par. 4.3.1; I. Giesen, Toezicht en aansprakelijkheid, Deventer: Kluwer 2005, p. 169; S.D. Lindenbergh, *Alles is betrekkelijk* (oratie Rotterdam), Den Haag: Boom Juridische uitgevers 2007, p. 13.
[481] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, p. 25.

kader van de AVG is gekozen voor een risicoaansprakelijkheid: het enkele feit dat door een verwerking de AVG wordt geschonden, is voldoende om aansprakelijk te worden gehouden voor de schade die het gevolg is van die schending.[482]

719. Indien artikel 6:162 BW (en artikel 6:98 BW) door uw rechtbank onverhoopt niet conform de AVG wordt uitgelegd, stelt de Stichting zich (subsidiair) op het standpunt dat in dat geval een vermoeden van causaal verband (csqn-verband) dient te worden aangenomen tussen de onrechtmatige daad van Oracle en Salesforce en de schade die de Gedupeerden hebben geleden. Volgens de Hoge Raad[483] is hiervoor plaats indien het gaat om schending van een norm die ertoe strekt een specifiek gevaar ter zake van het ontstaan van schade bij een ander te voorkomen en dit specifieke gevaar zich heeft verwezenlijkt. In onderhavig geval is sprake van schending van (een) dergelijke norm(en).

720. De normen die zijn opgenomen in de AVG hebben als voornaamste doel de bescherming van persoonsgegevens te verhogen en rechten van betrokkenen te verstevigen. De AVG sterkt tot bescherming van persoonsgegevens onder meer om te voorkomen dat natuurlijke personen de controle over hun persoonsgegevens verliezen en schade lijden. Hetzelfde geldt zoals hiervoor aangegeven voor artikel 11.7a Tw. Oracle en Salesforce hebben echter op grote schaal en langdurig de normen uit de AVG en artikel 11.7a Tw geschonden (zie hoofdstuk 4).

721. De Gedupeerden hebben als gevolg van deze schendingen de controle over hun persoonsgegevens verloren en schade geleden. Het specifieke gevaar waartegen de normen die zijn opgenomen in de AVG en artikel 11.7a Tw beogen te beschermen, heeft zich aldus verwezenlijkt. In dat geval is het redelijk ervan uit te gaan dat causaal verband (csqn-verband) bestaat tussen de onrechtmatige daad van Oracle en Salesforce en de schade, zoals door Gedupeerden geleden.

722. Indien het causaal verband niet op voorhand wordt aangenomen bij de onrechtmatige daad, geldt dat er evengoed een causaal verband bestaat tussen de schade en het onrechtmatig handelen van Oracle en Salesforce. De schade die de Gedupeerden, de Nederlandse internetgebruikers, hebben geleden, wordt immers veroorzaakt door de inbreukmakende handelingen van Oracle en Salesforce, dan wel doordat Oracle en Salesforce hebben gehandeld in strijd met een maatschappelijke zorgvuldigheidsnorm, zoals hiervoor geformuleerd.

723. Artikel 6:99 BW kan worden toegepast in gevallen waarin het volgende vaststaat:[484]

a. de aangesprokene is aansprakelijk voor een gebeurtenis die de gehele schade van de benadeelde kan hebben veroorzaakt;

b. ook een of meer anderen zijn aansprakelijk voor gebeurtenissen die de schade van de benadeelde geheel of gedeeltelijk kunnen hebben veroorzaakt; en

---

[482] F.C. van der Jagt-Vink, 'Schadevergoeding onder de Algemene Verordening Gegevensbescherming', *MvV* 2019/7.9, p. 290; P. van Schelven, '*Aandachtspunten inzake AVG aansprakelijkheid / vrijwaring*', te raadplegen via: https://www.lrgd.nl/Portals/1/Symp_2019_materiaal/4c%20Schelven%20Aandachtspunten%20aansprakelijkheid%20en%20vrijwaring%20AVG%20en%20verwerkersovereenkomst%20-%20LRGD.pdf.

[483] HR 29 november 2002, *NJ* 2004/304 en 305.

[484] Tekst & Commentaar, Schade gevolg van meer gebeurtenissen; alternatieve causaliteit bij: Burgerlijk Wetboek Boek 6, Artikel 99.

c. de schade van de benadeelde is het gevolg van ten minste één van deze gebeurtenissen.

724. De Hoge Raad heeft in dit kader geoordeeld dat uit het vereiste onder c niet kan worden afgeleid dat de benadeelde moet stellen — en dat moet komen vast te staan — wie tot de kring van aansprakelijke personen behoren, omdat het stellen van deze eis tot een onredelijk resultaat zou leiden.[485]

725. Mocht tijdens de procedure blijken dat andere partijen mede verantwoordelijk zijn voor de schade van de Gedupeerden, dan zijn Oracle en Salesforce alsnog aansprakelijk voor de schade op grond van artikel 6:99 BW. Iedere partij die de schade zou hebben kunnen veroorzaakt, is in dat geval immers aansprakelijk.[486]

*5.7.6 Schade*

726. Zoals reeds uiteengezet in paragrafen 5.5.3 en 5.5.5 hebben de Gedupeerden (enige vorm van) schade geleden. Deze schade zal door Oracle en Salesforce vergoed dienen te worden.

5.7.6.1 Winstafdracht (artikel 6:104 BW)

727. Op grond van artikel 6:104 BW kan degene die (i) een onrechtmatige daad heeft gepleegd en (ii) daardoor winst heeft genoten, veroordeeld worden tot afdracht van de winst of een deel ervan.[487] Winst dient daarbij ruim te worden opgevat: het beperken van verliezen valt er ook onder.[488] Verder is voldoende voor toepassing van het artikel dat (iii) de aanwezigheid van enige (vorm van) schade aannemelijk is.[489]

728. Alleen als de gedaagde echter kan aantonen dat geen schade kan zijn ontstaan, is voor toepassing van artikel 6:104 BW geen plaats.[490]

729. Artikel 6:104 BW is door de wetgever ingevoerd met het oog op, onder meer, het kunnen tegengaan van inbreuken op intellectuele eigendomsrechten en mededingingsrechten.[491] Tevens heeft de wetgever aangegeven dat artikel 6:104 BW ook kan dienen voor gevallen waarin de benadeelde vermoedelijk schade heeft geleden, maar schade niet of moeilijk bewijsbaar is.[492]

730. De gedachte achter de bepaling is dat het onredelijk werd geacht om ongeoorloofd ten koste van een ander verkregen winst aan de verkrijger te laten, waar door die ander vermoedelijk

[485] HR 9 oktober 1992, ECLI:NL:HR:1992:ZC0706, *NJ* 1994/535 (*DES-dochters*).
[486] Tekst & Commentaar, Schade gevolg van meer gebeurtenissen; alternatieve causaliteit bij: Burgerlijk Wetboek Boek 6, Artikel 99; T.F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens', *WPNR* 25 november 2017/7172, p. 923.
[487] Schadevergoeding voor de benadeelde is dan uitgesloten, want anders zou dubbel herstel plaatsvinden, de benadeelde meer krijgen dan waar hij recht op heeft en de laedens twee keer een sanctie opgelegd krijgen, zie Rb. Rotterdam 17 oktober 2012, ECLI:NL:RBROT:2012:BY1147, r.o. 5.8.
[488] HR 18 juni 2010, ECLI:NL:HR:2010:BL9662, *NJ* 2015, 33, r.o. 3.3.3 (*Setel/AVR Holding*); J. Spier, *Schadevergoeding: algemeen, deel 3* (Monografieën Nieuw BW, deel B36). Deventer: Kluwer 1992., nr. 39.
[489] Tekst & Commentaar Burgerlijk Wetboek, Begroting van de schade; winstafdracht bij: Burgerlijk Wetboek Boek 6, Artikel 104; Schadevergoeding algemeen 2 (Mon. BW nr. B35) 2017/12.
[490] Groene Serie Schadevergoeding, 2 Aard van vordering tot winstafdracht en vereiste schade bij: Burgerlijk Wetboek Boek 6, Artikel 104.
[491] Parlementaire Geschiedenis, BW Boek 6, p. 1266-67 (MvA II).
[492] Parlementaire Geschiedenis, Boek 6, p. 1269 (MvA II); HR 16 juni 2006, ECLI:NL:HR:2006:AU8940, *NJ* 2006, 585, r.o. 3.5.2 (*Kecofa/Lancôme*): J. Spier, T. Hartlief, S.D. Lindenbergh, A.L.M. Keirse, R.D. Vriesendorp & G. van Maanen, *Verbintenissen uit de wet en Schadevergoeding*, Wolters Kluwer: 2015, Studiereeks Burgerlijk recht, Vol. 5, p. 266.

wel schade is geleden, maar deze naar haar aard niet goed bewijsbaar is.[493] De bepaling geeft niet een recht op winstafdracht, maar geeft de rechter een discretionaire bevoegdheid de schade te begroten op het bedrag van de winst of een gedeelte daarvan en vormt daarmee een wettelijke basis voor een vorm van abstracte schadeberekening, zodat concreet nadeel bij onzekerheid niet door eiser behoeft te worden aangetoond.[494]

731. Uit de jurisprudentie volgt verder dat de op te leggen schadevergoeding niet in een reële verhouding hoeft te staan tot de schade die de benadeelde daadwerkelijk heeft geleden. Ook dient de schade te worden begroot op enkel een deel van de winst als het financiële voordeel dat de schuldenaar heeft behaald de vermoedelijke omvang van de schade aanmerkelijk te boven gaat.[495]

732. Wat de hoogte van de winstafdracht betreft, heeft de rechter veel vrijheid. Het vaststellen van de schade is vooral een kwestie van waardering waar qua bewijs[496] en motivering[497] geen hoge eisen aan worden gesteld. Het is voldoende dat de aanwezigheid van enige (vorm van) schade aannemelijk is.

733. Ook mag de rechter bij beantwoording van de vraag of hij de schade al dan niet op het volledige bedrag van de winst zal begroten, aan de mate van verwijtbaarheid gewicht toekennen.[498]

734. De Stichting beschikt niet over informatie omtrent de winstgevendheid van de DMP diensten van Oracle en Salesforce. Door Oracle en Salesforce gepubliceerde (jaar)cijfers laten weliswaar miljarden Euro's aan inkomsten zien, maar geven onvoldoende inzicht in de revenuen die specifiek in Nederland gedurende de relevante periode – van toepassing zijn van de AVG (25 mei 2018) tot en met datum vonniswijzing – worden gegenereerd. Een aanwijzing voor de waarde van de inkomsten, is de door Oracle en Salesforce betaalde prijs bij overname van vennootschappen die actief zijn in het RTB systeem (randnummers 50 en 52). De totaalsom daarvan bedraagt meer dan € 5 miljard. De Stichting is niet in staat te onderscheiden in welke mate deze waarde is bepaald door activiteiten op de Nederlandse markt.

735. Het ligt op de weg van Oracle en Salesforce om, indien uw rechtbank voor bepaling van de schade zou willen aangrijpen bij het door Oracle en Salesforce genoten voordeel gedurende de periode vanaf de toepasselijkheid van de AVG, daarover duidelijkheid te verschaffen.[499] Daarom verzoekt de Stichting uw rechtbank ook om Oracle en Salesforce te bevelen concrete informatie over te leggen die ten minste een schatting van de winst mogelijk maakt van hun genoten voordeel gedurende de periode vanaf het van toepassing zijn van de AVG tot en met

---

[493] Antwoorden II, Parlementaire Geschiedenis, BW Boek 6, p. 1269.
[494] HR 24 december 1993, ECLI:NL:HR:1993:ZC1202, *NJ* 1995/421 (*W./N.),* HR 24 juni 2016, ECLI:NL:HR:2016:1309, *NJ* 2016/300 (*Vitesse/Gelderland*); HR 18 juni 2010, *NJ* 2015, 32 (*Stichting Ymere*), r.o. 3.2.3, 3.7.
[495] HR 18 juni 2010, *NJ* 2015, 32 (*Stichting Ymere*), r.o. 3.7; HR 18 juni 2010, ECLI:NL:HR:2010:BL9662,*NJ* 2015/33 (*Setel/AVR*) r.o. 3.3.2.; Groene Serie Schadevergoeding, 2 Aard van vordering tot winstafdracht en vereiste schade bij: Burgerlijk Wetboek Boek 6, Artikel 104.
[496] HR 12 maart 2010, ECLI:NLIHR:ZOlOZBK9ISS (*X-lnterpolis en Achmea*), *RvdW* 2010, 416, r.o. 3.4; W. Dijkshoorn & S.D. Lindenbergh, 'Schadebegroting, bewijs en waardering', *Ars Aequi* 2010, p. 541.
[497] HR 17 februari 2006, ECLI:NL:PHR:2006:AU9717 (*Royal & Sun Alliance/Polygram*) *NJ* 2006, 378, r.o. 4.8; P.A. Fruytier, 'De ruime benadering van de Hoge Raad bij schadebegroting op winst: een stap te ver?', *MvV* 2010, p. 274.
[498] Tekst & Commentaar Burgerlijk Wetboek, Begroting van de schade; winstafdracht bij: Burgerlijk Wetboek Boek 6, Artikel 104; HR 18 juni 2010, ECLI:NL:HR:2010:BL9662, NJ 2015/33 (*Setel/AVR Holding*).
[499] Zie onder meer Rb. Amsterdam 22 januari 2018, ECLI:NL:RBAMS:2018:275, r.o. 2 en 22; HR 14 november 2014, ECLI:NL:HR:2014:3241, r.o. 4.2.3 en 4.10, Rb. Den Haag, ECLI:NL:RBDHA:2017:1418, r.o. 4.1.

de dag van vonniswijzing. Vooralsnog neemt de Stichting aan dat het genoten voordeel van Oracle en Salesforce (ieder) in die periode ten minste € 500 per Gedupeerde bedraagt.

736. Tenslotte merkt de Stichting op dat zij de mening is toegedaan dat uw rechtbank van haar discretionaire bevoegdheid gebruik kan maken en de schade op het volledige bedrag van de winst kan worden begroot, gelet op de mate van verwijtbaarheid van de gedragingen van Oracle en Salesforce (aard gegevens, ernst van de inbreuk, duur van de inbreuk, aantal betrokkenen en onomkeerbaarheid van de schade). De Stichting heeft dat hiervoor in paragraaf 5.5.4.3 'Toepassing op onderhavige zaak' nader toegelicht.

5.7.6.2 Abstracte schadebegroting alternatieve wijze van schadebegroting

737. Op het uitgangspunt van concrete schadeberekening worden slechts in bijzondere gevallen, zowel op praktische gronden als om redenen van billijkheid, uitzonderingen aanvaard.[500] Artikel 6:97 BW vormt de wettelijke basis voor de zogenoemde abstracte schadebegroting of abstracte schadeberekening. 'Abstract' wil zeggen dat geabstraheerd wordt van de concrete omstandigheden van het geval.[501]

738. Bij een abstracte schadebegroting vormen niet de omstandigheden van het geval het uitgangspunt bij de schadeberekening, maar wordt er gekeken naar de schade bij vergelijkbare posities van de benadeelde. De vaststelling geschiedt dan volgens objectieve maatstaven. Bij de abstracte methode gaat de rechter na hoe groot in het algemeen de schade is van een schuldeiser die in een gelijksoortige positie verkeert als de eiser in het geding.[502] Aanknopingspunten voor een abstracte benadering kunnen gevonden worden in de aard van de schade, eisen van doelmatigheid en in de redelijkheid van het resultaat.[503]

739. De rechter krijgt daartoe de vrijheid, mits deze wijze van begroting in overeenstemming is met de aard van de schade. Of dat het geval is, wordt met inachtneming van genoemd uitgangspunt aan de rechter overgelaten, uiteraard behalve daar waar de wet op dit punt een bijzondere, de rechter bindende, regel geeft.[504]

740. Het onderhavige geval wordt hierdoor getypeerd dat de Gedupeerden de controle over hun persoonsgegevens zijn verloren. Zonder hun toestemming is gebruik, genot of exploitatie door Oracle en Salesforce niet toegestaan. Dat is wel wat er is gebeurd. Oracle en Salesforce hebben op grote schaal, langdurig en voor commerciële doeleinden de persoonsgegevens van de Gedupeerden verzameld en verwerkt. Zij hebben onder meer inbreuk gemaakt op de AVG en de Tw. Gedupeerden zijn de controle over hun persoonsgegevens verloren en zijn in hun privacybelangen geschaad.

741. Oracle en Salesforce hebben de persoonsgegevens van Gedupeerden zonder hun toestemming gebruikt, zonder daarvoor toestemming te vragen of een vergoeding te betalen. In de bestaande praktijk vragen internetgebruikers (Gedupeerden in dit geval) vooralsnog geen gebruiksvergoeding voor het gebruik van hun persoonsgegevens, door partijen zoals Oracle en

[500] J. Spier, *Verbintenissen uit de wet en schadevergoedin*g (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 208.
[501] A.J. Verheij, *Onrechtmatige daad* (Monografieën Privaatrecht nr. 4), 48 Schadebegroting.
[502] Asser/Sieburgh 6-II 2017/35; Tekst & Commentaar Burgerlijk Wetboek, Begroting van de schade bij: Burgerlijk Wetboek Boek 6, Artikel 97.
[503] S.D. Lindenbergh, *Schadevergoeding: algemeen, deel* 1 (Monografieën BW B34) 2014, p. 53.
[504] Parlementaire Geschiedenis BW Boek 6, p. 339 (MvA II).

Salesforce. Zij zijn vaak niet eens op de hoogte dat hun persoonsgegevens worden gebruikt en door wie.

742. Door het handelen van Oracle en Salesforce hebben de Gedupeerden schade geleden. Deze schade laat zich niet eenvoudig begroten of bewijzen. Een abstracte wijze van schadebegroting kan in dit geval uitkomst bieden. Gelet op aard van de inbreuken (het gaat hier om persoonsgegevens en de privacy van Nederlandse internetgebruikers) en de ernst van de inbreuken (op grote schaal en voor commerciële doeleinden wordt op ernstige wijze langdurig inbreuk gemaakt) stelt de Stichting zich op het standpunt dat een vergoeding van € 500 per persoon een billijke vergoeding is.

## 5.8 Ongerechtvaardigde verrijking

### *5.8.1 Inleiding*

743. Meer subsidiair baseert de Stichting haar vordering tot schadevergoeding op ongerechtvaardigde verrijking (artikel 6:212 BW). In de volgende paragrafen zullen de vier vereisten van een dergelijke vordering nader worden besproken en worden toegelicht dat hieraan is voldaan. De vier vereisten zijn: (i) er is sprake van een verrijking; (ii) de verrijking is ontstaan ten koste van een ander, die verarmd is; (iii) de verrijking en verarming staan in voldoende verband met elkaar en (iv) de verrijking is ongerechtvaardigd.[505]

744. De formulering van artikel 6:212 BW laat veel ruimte voor interpretatie.[506] De wetgever heeft artikel 6:212 BW bewust in abstracte bewoordingen geformuleerd om de vordering een ruim toepassingsbereik te geven.[507] Met zijn keuze voor een algemene, abstract geformuleerde bepaling heeft de wetgever het aan de rechtspraak en literatuur overgelaten om artikel 6:212 BW te omlijnen en de vereisten van dit artikel nader in te vullen.[508] Aan de hand van de literatuur en rechtspraak zal steeds per vereiste een wettelijk kader worden geschetst, waarna deze wordt toegepast op de zaak.

### *5.8.2 Verrijking*

745. Allereerst is er voor de vergoeding van schade uit hoofde van artikel 6:212 BW het bestaan van een verrijking vereist. Het begrip verrijking omvat zowel behaald voordeel als afgewend nadeel.[509] Verrijkingen hebben een gevarieerd voorkomen en dienen ruim te worden uitgelegd.[510]

746. Bij verrijkingen dient sprake te zijn van een 'vermogensverschuiving van vermogensbestanddelen'.[511] Linssen betoogt dat artikel 6:212 BW ook van toepassing is

[505] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par. 1.1.1.
[506] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par. 1.1.1.
[507] Parlementaire Geschiedenis, BW Boek 6, p. 829.
[508] Parlementaire Geschiedenis, BW Boek 6, p. 831.
[509] Groene Serie Verbintenissenrecht, artikel 6:212 BW, aant. 4.2.1; Zie HR 24 mei 2013, ECLI:NL:HR:2013:BZ1782, *NJ* 2013/540 (*Credit Suisse/SuBWay Rotterdam*).
[510] Groene Serie Verbintenissenrecht, artikel 6:212 BW, aant. 4.2.3.
[511] Parlementaire Geschiedenis, BW Boek 6, p. 832: A.S. Hartkamp & C.H. Sieburgh, *mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Kluwer 2011, nr. 465.

wanneer een schuldenaar inbreuk maakt op een beschermenswaardige rechtspositie van een ander. Zijn betoog sluit aan bij het Duitse verrijkings- en onrechtmatigedaadsrecht.[512] In de literatuur wordt de visie van Linssen op meerdere plekken aangehaald, bediscussieerd en verder uitgewerkt.

747. Damminga sluit zich op grote lijnen aan bij de opvatting van Linssen dat een vordering op grond van artikel 6:212 BW ontstaat in gevallen waarin de schuldenaar inbreuk heeft gemaakt op een exclusieve rechtspositie zonder concrete schade te veroorzaken. Hij stelt zich daarbij op het standpunt dat artikel 6:212 BW moet worden beperkt tot gevallen waarin de schuldenaar een inbreuk heeft gepleegd op een exclusieve rechtspositie.[513]

748. Volgens Linssen gaat het om een inbreuk op de rechtspositie van de schuldeiser, uit welke rechtspositie volgt dat de rechthebbende-schuldeiser exclusief bevoegd is om de rechtspositie te gebruiken, te exploiteren of daarover te beschikken.[514] Een voorbeeld van dergelijke rechtsposities zijn persoonlijkheidsrechten, maar ook andere categorieën zijn denkbaar. Alleen de rechthebbende is bevoegd te beschikken over deze persoonlijkheidsrechten en alleen hij is gerechtigd tot het gebruik, het genot en de exploitatie van de voordelen die hiermee behaald kunnen worden. Wanneer een ander hiervan gebruik heeft gemaakt, maakt deze een inbreuk op de rechtspositie van de gerechtigde.[515]

749. Alleen als de handeling in de rechtsbetrekking tussen de schuldeiser en schuldenaar exclusief door de schuldeiser mag worden verricht, kan worden gezegd dat het verrichten van de onbevoegde handeling door de schuldenaar een voordeel vormt dat voortvloeit uit het vermogen van de schuldeiser.

750. Linssen geeft het volgende voorbeeld: stel dat A eigenaar is van een vakantiewoning. Volgens artikel 5:1 BW komt daarom alleen aan hem het genot en gebruik van de woning toe. Als B gebruik maakt van een zaak van A, bijvoorbeeld door in de vakantiewoning van A te trekken, verkrijgt B een voordeel ten koste van A; het gebruik zelf vormt het voordeel. Volgens Linssen zou het niet van belang behoren te zijn of A door het gebruik door B inkomsten is misgelopen, andere schade heeft geleden, of dat het vermogen van B is toegenomen of dat B zich door het gebruik kosten heeft bespaard. Het voordeel dat B heeft genoten ten koste van A moet volgens Linssen worden gesteld op een redelijke gebruiksvergoeding.[516]

751. De vraag of een voordeel een uitvloeisel is van een bepaalde exclusieve rechtspositie is volgens Linssen afhankelijk van de feiten en omstandigheden van het geval, waaronder de aard van het vermogensrecht en de aard van het voordeel. Linssen merkt daarbij op dat de weging van de feiten en omstandigheden uiteraard ook gekleurd wordt door de maatschappelijke ontwikkelingen. Linssen somt vervolgens zes groepen van gevallen op als een inbreuk op een

[512] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: BJu 2001, p. 472.
[513] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (O&R nr. 80) 2014, par. 4.2.5 en 4.4.6.
[514] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: Boom Juridische uitgevers 2001, 427-473.
[515] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par. 4.4.6.
[516] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: Boom Juridische uitgevers 2001, p. 589-591.

exclusieve rechtspositie, maar geeft daarbij aan dat de opsomming niet uitputtend is bedoeld:[517]

(i) Het onbevoegd beschikken over en gebruik maken van andermans zaken;

(ii) Het gebruiken en exploiteren van geheime informatie;

(iii) Schending van persoonlijkheidsrechten;

(iv) Inbreuk op contractuele verhoudingen door een derde;

(v) Schending van contractuele verplichtingen door een contractspartij; en

(vi) Misbruik of oneigenlijk gebruik van vertrouwensrelaties.

752. Linssen lijkt uit te gaan van de vordering uit ongerechtvaardigde verrijking als een instrument van 'goederenbescherming', een verlenging van het 'eigendomsrecht'. Het leerstuk van de ongerechtvaardigde verrijking wordt dan toegepast op inbreuken op eigendom en vergelijkbare vermogensposities.

753. De Stichting stelt zich op het standpunt dat het leerstuk van de ongerechtvaardigde verrijking ook van toepassing is op het onrechtmatige gebruik van persoonsgegevens door Oracle en Salesforce. De Stichting zal waar nodig nuances aanbrengen op de zienswijze van Linssen.

754. Ten eerste merkt de Stichting op dat persoonsgegevens strikt genomen (op dit moment) niet kwalificeren als 'eigendom' in de zin van artikel 5:1 BW, maar dat hierover nog niet het laatste woord is gezegd of geschreven. Tijdens een debat in de Tweede Kamer op 10 september 2019 zijn er vragen gesteld over de mogelijkheid om in het Burgerlijk Wetboek het eigenaarschap van de burger van zijn of haar persoonsgegevens bij de overheid te regelen.[518] Dit gebeurde naar aanleiding van een advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen van de Raad van State.[519] De heer Van Der Molen (namens het CDA) zei hierover het volgende tijdens het debat:

> *"Iedere Nederlander zou wat ons betreft eigenaar moeten zijn van zijn of haar persoonsgegevens of data. (…) Een ondubbelzinnige wettelijke bepaling zou wat ons betreft zekerheid aan burgers en een solide basis moeten bieden bij de verhouding van de data tot onder andere de platforms van de overheid."*

755. De staatssecretaris van Binnenlandse Zaken en Koninkrijkrelaties deed daarbij de toezegging om nader onderzoek te (laten) verrichten naar de mogelijkheden om het eigenaarschap van persoonsgegevens te regelen. Op 15 juni 2020 werd de Tweede Kamer van de uitkomst van dit onderzoek op de hoogte gebracht. Uit de brief aan de Tweede Kamer blijkt weliswaar dat de staatssecretaris van Binnenlandse zaken en Koninkrijkrelaties van mening is dat onbeperkt zeggenschap over persoonsgegevens (nog) niet aan de orde is,[520] maar dit neemt niet weg dat

[517] J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: Boom Juridische uitgevers 2001, p. 586 e.v.
[518] *Kamerstukken II*, 2018/19, 26 643, nr. 105.
[519] Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen van de Raad van State van 31 augustus 2018, *Kamerstukken II*, 2017/18, 26 643, nr. 557.
[520] *Kamerstukken II,* 2019/20, 32 761, nr. 165.

er een maatschappelijke discussie over de bescherming en de status van persoonsgegevens in volle gang is.

756. Ten tweede merkt de Stichting op dat persoonsgegevens de bescherming dienen te genieten van artikel 1 Eerste Protocol EVRM ("**Protocol**"). Er liggen drie hoofdregels besloten in artikel 1 van het Protocol: (i) het beginsel van ongestoord eigendomsgenot (eerste zin van het eerste lid), (ii) bescherming tegen de ontneming van eigendom (tweede zin van het eerste lid) en (iii) de mogelijkheid van regulering van eigendom (tweede lid).[521]

757. Eigendom in de zin van artikel 1 van het Protocol heeft niet de betekenis die het begrip in artikel 5:1 BW kent. Het Europees Hof voor de Rechten van de Mens kent het begrip een geheel autonome betekenis toe, die vele malen ruimer is dan het eigendomsbegrip in artikel 5:1 BW.[522]

758. De grenzen van de bescherming onder artikel 1 van het Protocol zijn afgeleid van de grondgedachte: de bescherming van (economische) belangen die voldoende zeker zijn, of anders gezegd: met voldoende zekerheid, deel uitmaken van het vermogen van de desbetreffende beschermde.[523] Centraal staat hierdoor de bescherming van iemands daadwerkelijke vermogen, althans van de bestanddelen die een concrete en zekere economische waarde vertegenwoordigen.

759. Persoonsgegevens maken onderdeel uit van het vermogen van een individu en vertegenwoordigen een concrete en zekere economische waarde (zie paragraaf 5.5.5.2 hiervoor). Persoonsgegevens dienen aldus de bescherming van artikel 1 van het Protocol te genieten én in het verlengde daarvan: de bescherming van de vordering uit ongerechtvaardigde verrijking.

760. Ten derde merkt de Stichting op dat een vordering uit ongerechtvaardigde verrijking niet tot een instrument van 'goederenbescherming' beperkt zou moeten worden. De kans bestaat dat gelijke gevallen ongelijk worden behandeld. In de gevallen die Linssen opsomt zou wel een verrijkingsvordering als het gaat om intellectuele eigendomsrechten, corporate opportunities en geheimhoudingsplichten slagen, maar bijvoorbeeld niet als het gaat om onbetamelijk profiteren van wanprestatie. En juist in dat geval kan een vordering uit ongerechtvaardigde verrijking geschikt zijn om ingezet te kunnen worden.

761. De wetgever heeft de ontwikkeling van de vordering uit ongerechtvaardigde verrijking overgelaten aan de rechtspraak en literatuur. In het arrest van de Hoge Raad[524] inzake een gepleegde Ponzi-Scheme werd de vordering uit ongerechtvaardigde verrijking ingezet in een fraudekwestie (het profiteren van wanprestatie). In de uitspraak werd bevestigd dat verrijking van een partij bij een overeenkomst ten koste van een derde niet steeds en zonder meer wordt gerechtvaardigd door die overeenkomst, ook al zal dat doorgaans wel het geval zijn.[525] Wanneer echter tussen de prestaties waartoe de overeenkomst verplicht enerzijds en de verrijking anderzijds een wanverhouding bestaat, zal de overeenkomst minder snel als

[521] EHRM 23 september 1982, NJ 1988/920 m.nt. Alkema (Sporrong & Lönnroth/Zweden), r.o. 61).
[522] D.G.J. Sanderink, Het EVRM en het materiële omgevingsrecht (Staat en Recht nr. 22), Deventer: Wolters Kluwer 2015, par. 2.6.2.
[523] J.M. Emaus, 'Bescherming van goodwill op grond van het EVRM', NTBR 2018/8, par. 3.1.
[524] HR 28 oktober 2011, ECLI:NL:HR:2011:BQ5986, *NJ* 2012/496 (*Ponzi-scheme*).
[525] HR 20 september 2002, ECLI:NL:HR:2002:AE3363, *NJ* 2004/458 m.nt Hijman (*Carribean Bistros c.s. Club/Caraibeen*).

rechtvaardiging voor de verrijking worden aanvaard. De vordering uit ongerechtvaardigde verrijking bood dus ook uitkomst nu bij een Ponzi-scheme bij uitstek sprake is van een wanverhouding.

762. Ten vierde stelt de Stichting zich op het standpunt dat persoonsgegevens mogelijk strikt genomen geen eigendom zijn, maar dat de bescherming van persoonsgegevens verwant is aan persoonlijkheidsrechten, zoals we die bijvoorbeeld kennen in het auteursrecht. Net als het zonder toestemming verwijderen van naamsvermelding of wijzigen van een auteursrechtelijk beschermd werk, leidt ook het zonder grondslag (zoals toestemming) of overigens onrechtmatig gebruiken van persoonsgegevens tot aansprakelijkheid. Met de AVG heeft de Europese wetgever de betrokkene in staat willen stellen controle uit te oefenen op de bescherming van persoonsgegevens. Door in strijd met de AVG te handelen maken Oracle en Salesforce inbreuk op de exclusieve rechtspositie van de betrokkenen.

763. Linssen merkt op dat de 'exclusieve bevoegdheid' van de rechthebbende niet altijd absoluut hoeft te zijn. Linssen stelt dat het onbevoegd gebruiken en exploiteren van geheime informatie is voorbehouden aan degene die deze informatie in het kader van zijn beroep of bedrijf heeft verzameld of ontwikkeld. De exclusiviteit van de gerechtigheid tot de informatie kan relatief zijn, omdat het bepaalde personen niet is toegestaan om de informatie te gebruiken, te exploiteren of daarover te beschikken, terwijl bepaalde derden dat wel zouden mogen, bijvoorbeeld omdat hun een licentie is verschaft. Als degene die de informatie niet mag gebruiken dit toch doet, dan zou hij het daardoor genoten voordeel moeten afstaan aan degene jegens wie hij verplicht was zich van het gebruik te onthouden.

764. De betrokkene is ten aanzien van zijn persoonsgegevens exclusief gerechtigd om controle uit te oefenen op de verwerking en zijn rechten te handhaven. Zonder inachtneming van de AVG mogen zijn persoonsgegevens niet verzameld, gebruikt en/of geëxploiteerd worden. En dat is wel wat er in onderhavig geval is gebeurd.

765. Oracle en Salesforce hebben de persoonsgegevens van de Gedupeerden onrechtmatig verzameld, gebruikt en geëxploiteerd. De Stichting stelt zich op het standpunt dat Oracle en Salesforce het daardoor genoten voordeel moeten afstaan op grond van ongerechtvaardigde verrijking. Oracle en Salesforce hebben een voordeel genoten (verrijking) dat voortvloeit uit het vermogen van de Gedupeerden.

766. Het verrijkingsfeit moet een bepaalde verrijking veroorzaken, die op een bepaald bedrag kan worden begroot. Deze verrijking dan wel 'schade' moet worden afgedragen op grond van artikel 6:212 BW. De Stichting stelt zich op het standpunt dat de omvang van de verrijking moet worden begroot op de waarde die het gebruik, genot of exploitatie van de persoonsgegevens in het rechtsverkeer heeft. Deze waarde kan bijvoorbeeld volgen uit de vergoeding die de Gedupeerden hadden kunnen bedingen.[526] De Stichting is de mening toegedaan dat deze vergoeding op een bedrag van € 500 per gedupeerde kan worden gesteld.

767. In paragraaf 5.1 heeft de Stichting gemotiveerd uiteengezet dat zij een vergoeding van een schadebedrag van € 500 per betrokkene, gelet op de omstandigheden van onderhavig geval,

[526] S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par. 4.6.2; Parlementair Geschiedenis, BW Boek. 6, p. 818-819.

billijk vindt. In dat kader merkt de Stichting op dat een abstracte wijze van schadeberekening kan worden gehanteerd om ervoor te zorgen dat Oracle en Salesforce het voordeel dan zij ten onrechte hebben genoten, niet mogen behouden.

*5.8.3 Verarming*

768. Van verarming is sprake bij zowel afname van de activa als een toename in de passiva.[527] De verrijking hoeft niet het spiegelbeeld van de verarming te zijn.[528] Een goed waarmee de een verrijkt is ten koste van de ander kan voor beiden een geheel verschillende waarde hebben.[529] Voor de verzamelaar heeft bijvoorbeeld een ontbrekend exemplaar doorgaans een grotere waarde dan voor degene die uitsluitend dat exemplaar bezit. Ook wanneer iemand in zijn tuin een zwembad wil aanleggen en daarvoor een klein stuk grond van de buurman nodig heeft, hecht daaraan veel meer (vermogens)waarde dan die buurman, indien het stukje grond een onbetekenend gedeelte van diens erf vormt.[530]

769. Over het algemeen wordt gesteld dat de verarming het maximum van de vergoeding bepaalt, die de verrijkte moet betalen. Deze stelling stuit op veel kritiek in de literatuur. Vooral in het kader van partijen die geen schade hebben geleden of waarvan de verarming moeilijk is aan te tonen, terwijl de verrijkte wel aanzienlijk voordeel heeft genoten, bijvoorbeeld bij een inbreuk op het portretrecht. In de kern gaat het dan om de vraag waarom de ongerechtvaardigde verrijkte zijn voordeel in die gevallen mag behouden, terwijl dat voordeel eigenlijk toebehoort aan de verarmde.[531] In die gevallen zou het niet noodzakelijk hoeven zijn om (de omvang van) de verarming aan te tonen.

770. In dat kader kan gezegd worden dat ongerechtvaardigde verrijking eigenlijk geen grond is voor schadevergoeding, maar voor ongedaanmaking van de verrijking aldus de literatuur.[532] Dit wordt ook bevestigd in de parlementaire geschiedenis. Uit de parlementaire geschiedenis wordt duidelijk dat de wetgever een algemene vordering tot afdracht van een ongerechtvaardigde verrijking heeft willen invoeren om aan te sluiten bij de rechtssystemen van de ons omringende landen en bij het oudvaderlandse recht.[533] In deze rechtstelsels strekt de vordering tot afdracht van de verrijking.

771. De wetgever lijkt bij de uitvoering van de wet echter de vordering uit ongerechtvaardigde verrijking geformuleerd te hebben als een schadevergoedingsvordering in tegenstelling tot de

---

[527] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 312; Groene Serie Verbintenissenrecht, artikel 6:212 BW, aant. 4.1.2.
[528] R. Koolhoven, *Niederländisches Bereicherungsrecht*, Göttingen: V&R unipress 2011, p. 67; A.S. Hartkamp & C.H. Sieburgh, *mr. C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Verbintenissenrecht. Deel IV. De verbintenis uit de wet*, Deventer: Kluwer 2011, nr. 461.
[529] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 312.
[530] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 312.
[531] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 312; J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: BJu 2001, p. 453 e.v.; Damminga 2014, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht nr. 80), p. 202 e.v.; Van Boom, preadvies VBR 2002, par. 2; Hartkamp 2001, p. 315.
[532] A.S. Hartkamp, Ongerechtvaardigde verrijking naast overeenkomst en onrechtmatige daad, *WPNR* 2001/6440-6441, p. 315; B.W.M. Nieskens-Isphording, *Het fait-accompli in het vermogensrecht*, Deventer: Kluwer 1991, p. 67-68; J.G.A. Linssen, *Voordeelsafgifte en ongerechtvaardigde verrijking: een rechtsvergelijkende beschouwing*, Den Haag: BJu 2001, p. 473-494; M.H. Bregstein, *Ongegronde Vermogensvermeerdering*, Amsterdam: H.J. Paris 1927, p. 216; H.C.F. Schoordijk, *Ongegronde vermogensvermeerdering*, Zwolle: W.E.J. Tjeenk Willink 1977, p 32; W. Snijders, *Ongerechtvaardigde verrijking en het betalingsverkeer*, Deventer: Kluwer 2001, p. 17.
[533] Parlementaire Geschiedenis, BW Boek 6, p. 823-829.

ons omringende landen. De vordering lijkt te strekken tot vergoeding van de schade van de verarmde, zodat ook bijvoorbeeld afdeling 6.1.10 (artikel 6:95-110 BW) over de wettelijke verplichtingen tot schadevergoeding van toepassing lijkt te zijn.

772. In de literatuur worden verschillende problemen gesignaleerd die ontstaan wanneer de vordering uit ongerechtvaardigde verrijking wordt opgevat als een schadevergoedingsvordering. Zo bepaalt artikel 6:98 BW dat voor vergoeding slechts in aanmerking komt de schade die in zodanig verband staat met de gebeurtenis waarop de aansprakelijkheid berust, dat zij aan degene die tot vergoeding verplicht is kan worden toegerekend als gevolg van deze gebeurtenis. De aansprakelijkheid bij de ongerechtvaardigde verrijking berust echter op een toestand, de verrijking, en niet op een gebeurtenis. Ook de regeling van de eigen schuld in artikel 6:101 BW gaat uit van aansprakelijkheid die ontstaat als gevolg van een gebeurtenis. Beide artikelen dienen niet te worden toegepast bij de vordering uit ongerechtvaardigde verrijking. Artikel 6:212 BW bevat juist een eigen regel van causaal verband, namelijk de regel dat de verrijking 'ten koste van' een ander is verkregen.[534]

773. In de literatuur wordt bepleit dat indien de verarmde geen schade heeft geleden of hij de schade moeilijk kan bewijzen, een vordering tot voordeelsafgifte in plaats van een vordering tot schadevergoeding op grond van artikel 6:212 BW kan worden ingesteld. De woorden 'ten koste van een ander' en 'diens schade te vergoeden' dienen er dan enkel toe om de persoon vast te stellen wie de vordering uit ongerechtvaardigde verrijking kan instellen. Aan het verarmingsvereiste wordt dan voldaan als het voordeel voortvloeit uit het vermogen van de verrijkingsschuldeiser.[535] Deze oplossing wordt dan gerechtvaardigd door het feit dat de verrijkte wel voordeel heeft genoten en niet ingezien kan worden waarom de ongerechtvaardigd verrijkte dat voordeel zou mogen behouden.[536]

774. In het arrest van de Hoge Raad *Credit Suisse/Subway*[537] wordt een soortgelijke oplossing gevonden voor het geval dat de verarmde in beginsel geen schade lijkt te hebben geleden. De Hoge Raad oordeelt als volgt:

> *"Het onderhavige geval wordt hierdoor getypeerd dat Subway, als "zittende" onderhuurder van de bedrijfsruimte, na beëindiging van de huurovereenkomst die haar contractuele wederpartij Easy met Credit Suisse had gesloten, met laatstgenoemde heeft onderhandeld over de totstandkoming van een huurovereenkomst met haar, dat Subway de bedrijfsruimte is blijven gebruiken gedurende de periode waarin de onderhandelingen voortduurden, en dat de onderhandelingen zijn afgebroken zonder dat tussen partijen een huurovereenkomst is tot stand gekomen. Onder zodanige omstandigheden is voor dit voortgezet gebruik in beginsel een gebruiksvergoeding verschuldigd op de voet van artikel 6:212 BW. Degene die het gebruik van de bedrijfsruimte voortzet is daardoor immers verrijkt, omdat het gebruik van andermans bedrijfsruimte in het maatschappelijk verkeer in de regel slechts tegen een vergoeding plaatsvindt,*

534 A.S. Hartkamp, Ongerechtvaardigde verrijking naast overeenkomst en onrechtmatige daad, *WPNR* 2001/6440-6441, p. 315.
535 S.R. Damminga, *Ongerechtvaardigde verrijking en onverschuldigde betaling als bronnen van verbintenissen* (Onderneming en recht, nr. 80), Deventer: Kluwer 2014, par. 4.3.3.
536 J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 312.
537 HR 24 mei 2013, ECLI:NL:HR:2013:BZ1782, *NJ* 2013/540, *JOR* 2013/266, m.nt. S.R. Damminga.

*terwijl de onderhuurder is bevrijd van de met zijn wederpartij overeengekomen verplichting de huurprijs te voldoen, door de beëindiging van de overeenkomst van onderhuur. De eigenaar van de bedrijfsruimte lijdt door dat voortgezet gebruik schade, ook als hij niet elders vervangende bedrijfsruimte hoeft te huren en hij niet door dat gebruik is verhinderd de ruimte aan een derde te verhuren. Gelet op de analogie met de gevallen die zijn geregeld in de artikelen 7:225 en 7:230a BW, past het immers in het stelsel van de wet de schade van de eigenaar in het onderhavige geval naar objectieve maatstaven te berekenen. Het causaal verband tussen deze verrijking en verarming ligt in de omstandigheden van het geval besloten. Ten slotte is aanvaarding van een verrijkingsvordering in beginsel niet onredelijk omdat het gebruik van de bedrijfsruimte welbewust door de gebruiker is voortgezet, en het daaruit resulterende voordeel hem dus niet is opgedrongen, terwijl de vordering slechts toewijsbaar is tot het laagste bedrag van de verrijking en de verarming."*

775. In de literatuur wordt verder bepleit dat in dit geval ook gebruik kan worden gemaakt van het fenomeen van de abstracte schadevergoeding. Wanneer de schade van de verarmde abstract wordt begroot, kunnen onredelijke uitkomsten worden voorkomen.[538]

776. De Stichting stelt zich op het standpunt dat aan het verarmingsvereiste wordt voldaan nu het ten onrechte genoten voordeel van Oracle en Salesforce voortvloeit uit het vermogen van de Gedupeerden. De Gedupeerden hebben de controle verloren over hun persoonsgegevens. Oracle en Salesforce hebben schade veroorzaakt. Gedupeerden zijn aldus verarmd en hebben 'schade' geleden, dan wel hebben recht op afdracht van het door Oracle en Salesforce genoten voordeel, zoals hiervoor uiteengezet. Dit betekent dat de Gedupeerden (meer subsidiair) een vordering uit ongerechtvaardigde verrijking jegens Oracle en Salesforce kunnen instellen ex artikel 6:212 BW tot vergoeding van schade, dan wel afdracht van het ten onrechte genoten voordeel.

*5.8.4 Causaal verband is aanwezig*

777. De verarmde kan alleen een vordering instellen tegen diegene die ten koste van hem is verrijkt. Tussen de verrijking en de verarming dient een causaal verband aanwezig te zijn. Dit causaal verband is gelegen in de gebeurtenis waardoor de verrijking heeft plaatsgevonden. Het is niet noodzakelijk dat het causaal verband de persoon van de verarmde en verrijkte betreft: de verrijking hoeft niet door de verrijkte en/of de verarmde te zijn veroorzaakt. Dit kan ook door toedoen van een derde zijn gebeurd.[539]

778. Zoals hiervoor toegelicht, is de controle op en handhaving van rechten ten aanzien van het verzamelen, gebruik en de exploitatie van persoonsgegevens voorbehouden aan de

[538] M.H. Bregstein, *Ongegronde Vermogensvermeerdering*, Amsterdam: H.J. Paris 1927, p. 216; H.C.F. Schoordijk, *Ongegronde vermogensvermeerdering*, Zwolle: W.E.J. Tjeenk Willink 1977, p 32; W. Snijders, *Ongerechtvaardigde verrijking en het betalingsverkeer*, Deventer: Kluwer 2001, p. 17; J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, p. 380.

[539] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 313. Zie onder meer HR 29 januari 1993, ECLI:NL:HR:1993:ZC0845, *NJ* 1994/172 m.nt. P. van Schilfgaarde (*Vermobo/Van Rijswijk*); HR 27 juni 1997, ECLI:NL:HR:1997:AG7249, *NJ* 1997/719 m.nt. J. Hijma (*Setz/Brunings*); HR 30 september 2005, ECLI:NL:HR:2005:AR7928, *NJ* 2007/154 m.nt. J.B.M. Vranken (*Koker/Cornelius*).

Gedupeerden. De persoonsgegevens maken onderdeel uit van het vermogen van de Gedupeerden en vertegenwoordigen een economische waarde.

779. De Stichting stelt zich op het standpunt dat de persoonsgegevens bescherming dienen te genieten van artikel 1 van het Protocol dan wel dat de rechten die betrokkenen hebben ten aanzien van hun persoonsgegevens gelijk behandeld moeten worden met exclusieve rechtsposities (zoals eigendom).

780. Het onrechtmatig verwerken van de persoonsgegevens door Oracle en Salesforce levert aldus een vermogensverschuiving op ten koste van de Gedupeerden. Oracle Salesforce hebben een voordeel genoten dat voortvloeit uit het vermogen van de Gedupeerden. Hiermee is het causaal verband gegeven.

*5.8.5 Ongerechtvaardigde verrijking*

781. Of er sprake is van een ongerechtvaardigde verrijking hangt af van de omstandigheden van het geval. De wetgever heeft destijds geen uitwerking gegeven van het begrip. Wel zijn er in de parlementaire geschiedenis de nodige voorbeelden gegeven wanneer er wel of niet sprake zou zijn van een rechtvaardiging.[540] De verdere invulling is verder overgelaten aan de rechtspraak en de wetenschap.[541]

782. Een verrijking is ongerechtvaardigd, indien zij niet gebaseerd is op ofwel een geldige rechtshandeling tussen de verarmde en de verrijkte ofwel een wettelijke regeling die tot die vermogensverschuiving strekt.[542] Het ontbreken van een geldige en legitimerende oorzaak voor de verrijking vormt het primaire criterium voor de ongerechtvaardigdheid.[543]

783. De controle op en handhaving ten aanzien van het onrechtmatige gebruik van de persoonsgegevens van Gedupeerden, is voorbehouden aan de Gedupeerden.

784. Uit het voorgaande volgt niet alleen dat het verzamelen, gebruik, de exploitatie of het uitoefenen van controle op de persoonsgegevens door Oracle en Salesforce een vermogensverschuiving oplevert ten koste van de Gedupeerden, maar ook de controle hierop en handhaving van rechten in dat verband niet toekomen aan een ander dan de Gedupeerden en daarom – zonder rechtvaardiging – leiden tot een ongerechtvaardigde verrijking.

785. Daarnaast geldt ook dat er geen rechtvaardiging in de wet te vinden is voor de verrijking. In tegendeel, Oracle en Salesforce maken zich onder meer schuldig aan diverse schendingen van de AVG en de Tw. Er is ook geen sprake van een rechtshandeling waarbij Gedupeerden enerzijds en Oracle en/of Salesforce anderzijds partij zijn die de verrijking zou kunnen rechtvaardigen. De Stichting heeft hiervoor in hoofdstuk 4 uiteengezet dat Oracle en Salesforce onrechtmatig de persoonsgegevens van de Gedupeerden verwerken.

---

[540] Parlementaire Geschiedenis, BW Boek 6, p. 829-830 en 833 e.v.
[541] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 313.
[542] J. Spier, *Verbintenissen uit de wet en schadevergoeding* (Studiereeks burgerlijk recht deel 5), Deventer: Kluwer 2015, par. 315/316; E.F.D. Engelhard & G.E. van Maanen, *Aansprakelijkheid voor schade: contractueel en buitencontractueel*. Deventer: Kluwer, 2008 (Monografieën BW; No. A15), p. 49.
[543] E.F.D. Engelhard & G.E. van Maanen, *Aansprakelijkheid voor schade: contractueel en* buitencontractueel. Deventer: Kluwer, 2008 (Monografieën BW; No. A15), p. 49.

*5.8.6 Omvang van de vordering*

786. Gelet op het voorgaande stelt de Stichting zich (meer subsidiair) op het standpunt dat de schadevergoeding dan wel afdracht van het ten onrechte genoten voordeel kan worden gebaseerd op een vordering uit ongerechtvaardigde verrijking.

787. De Stichting stelt zich daarbij op het standpunt dat de omvang van de schade dan wel de afdracht van het ten onrechte genoten voordeel (abstract) moet worden begroot op een bedrag van € 500 per persoon, zoals hiervoor en in hoofdstuk 5 nader uiteengezet.

## 5.9 Hoofdelijke aansprakelijkheid

*5.9.1 Hoofdelijke aansprakelijkheid op grond van de AVG*

788. Artikel 82 lid 4 AVG bepaalt het volgende:

> *"Als meerdere organisaties bij dezelfde verwerking zijn betrokken (als verwerkingsverantwoordelijken of verwerkers), worden zij elk hoofdelijk aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk de schadevergoeding ontvangt. De partij die de gehele schade heeft vergoed, kan (een deel van) het betaalde bedrag verhalen op de andere betrokken organisaties"*

789. Uit het voorgaande blijkt dat bij de verwerkingen door Oracle en Salesforce meerdere partijen betrokken zijn. Primair geldt dat de gedaagde Oracle en Salesforce entiteiten ieder voor hun DMP verwerkingen de verwerkingsverantwoordelijke zijn en op grond van artikel 82 lid 4 AVG hoofdelijk aansprakelijk zijn voor de volledige in verband met hun DMP dienst geleden schade. Voor zover voor een gedeelte van de verwerkingen sprake is van gezamenlijke verantwoordelijkheid met Publishers of Advertisers (randnummer 284), geldt ook dat ieder van de betrokken partijen hoofdelijk aansprakelijk is voor de volledige in verband met die verwerkingen geleden schade. Voor cookie syncing geldt in dat geval dat Oracle en Salesforce gezamenlijk met de partijen met wie zij gegevens uitwisselen de verwerkingsverantwoordelijke zijn. Nu zij mede met elkaar gegevens uitwisselen in dit kader geldt hiervoor dat Oracle en Salesforce en alle andere betrokken partijen ieder hoofdelijk aansprakelijk zijn voor de gehele door cookie syncing veroorzaakte schade (randnummer 284).

*5.9.2 Hoofdelijke aansprakelijkheid op grond van het BW*

5.9.2.1 <u>Inleiding</u>

790. Voor zover Oracle en Salesforce stellen dat zij niet de volledige aansprakelijkheid dragen omdat ook andere partijen bijdragen aan de verwerking geldt voorts dat Oracle en Saleforce bovendien ieder op grond van artikel 6:166 BW hoofdelijk aansprakelijk zijn voor de verwerkingen in verband met hun DMP dienst. Artikel 6:166 BW bevat een (aanvullende) regel over causaal verband, betreffende een onrechtmatige daad gepleegd door één van tot een groep behorende personen.[544] Primair stelt de Stichting dat Oracle en Salesforce de

[544] Asser/Hartkamp & Sieburgh 6-IV 2015/127.

hoofdverantwoordelijkheid dragen. Subsidiair kan gesteld worden dat zij ieder met de partijen die gebruikmaken van en/of bijdragen aan hun DMP verwerking een dergelijke groep vormen.

791. Voor aansprakelijkheid op grond van artikel 6:166 BW dient aan een viertal vereisten te worden voldaan: (i) er dient sprake te zijn van handelen in groepsverband, (ii) deelneming van een groepslid aan de gedragingen in groepsverband dient een onrechtmatige daad op te leveren, (iii) deelneming van een groepslid aan de gedragingen in groepsverband moet hem als een onrechtmatige daad kunnen worden toegerekend en (iv) de handeling waardoor de schade wordt toegebracht, moet jegens de benadeelde een onrechtmatige daad opleveren.[545]

5.9.2.2 Groepsverband

792. De Stichting hoeft niet te stellen en zo nodig te bewijzen dat er causaal verband bestaat tussen de deelneming van Oracle en Salesforce aan de groep en het toebrengen van schade door één van de deelnemers in de groep. Oracle en/of Salesforce kunnen zich ook niet van aansprakelijkheid bevrijden door te stellen en te bewijzen dat causaal verband ontbreekt omdat de schade ook zonder hun deelneming aan de groep zou zijn toegebracht. Voldoende voor het aannemen van aansprakelijkheid is dat één van de deelnemers van de groep schade aan de Gedupeerden heeft toegebracht.[546]

793. Om aan vereiste (i) te voldoen dienen Oracle en Salesforce een bijdrage te hebben geleverd aan de gedragingen die het gevaar voor schade hebben doen ontstaan (het objectieve criterium). Niet is vereist dat Oracle en Salesforce daadwerkelijk aan het toebrengen van de schade hebben meegewerkt. Daarnaast dient sprake te zijn van een bewust gezamenlijk optreden van de deelnemers, waarbij opzet gericht op het toebrengen van de schade niet is vereist, maar de gezamenlijkheid van het handelen de kans op schade vergroot en deze kans door de deelnemers bewust wordt aanvaard (het subjectieve criterium).[547]

794. Aan vereiste (i) wordt voldaan. Oracle en Salesforce handelen in groepsverband, nu zij hun DMP diensten aanbieden aan een grote groep van gebruikers en daarbij doen aan cookie syncing in een systeem (RTB) dat gekenmerkt wordt door een grote mate van onderlinge afhankelijkheid.

795. Zoals reeds uiteengezet in paragraaf 5.1, spelen Oracle en Salesforce een onmisbare rol in deze gegevensverzameling. Als DMPs vormen zij de centrale datahubs in de advertentiemarkt. In dat kader vindt er tussen de verschillende partijen op de RTB markt samenwerking plaats door middel van cookie syncing, het fenomeen waarmee adtech bedrijven gemakkelijk Cookie IDs kunnen uitwisselen (zie paragraaf 3.2.6). Dit betreft één van de kernactiviteiten van Oracle en Salesforce. Binnen deze groep worden door Oracle en Salesforce op grote schaal Cookie Ids, andere online identificatoren en daaraan verbonden persoonsgegevens uitgewisseld. Op basis van de identificatoren kunnen de betrokken partijen steeds eenvoudig communiceren over dezelfde gebruiker om een zo compleet mogelijk beeld van diegene te verkrijgen. De deelnemers aan de groep werken dus bewust samen om zoveel mogelijk persoonsgegevens te

[545] Asser/Hartkamp & Sieburgh 6-IV 2015/127.
[546] R.J.B. Bonnekamp, Stelplicht & Bewijslast, Onrechtmatige daad in groepsverband bij: Burgerlijk Wetboek Boek 6, Artikel 166.
[547] Asser/Hartkamp & Sieburgh 6-IV 2015/127.

verzamelen voor commerciële doeleinden. Er is aldus sprake van een groep, die bewust gezamenlijk optreedt.

5.9.2.3 Onrechtmatige daad

796. De hiervoor omschreven handelingen van Oracle en Salesforce en hun bijdragen aan de RTB markt levert bovendien een onrechtmatige daad op. Hiermee wordt ook aan vereiste (ii) voldaan. Oracle en Salesforce hadden behoren te voorzien dat door cookie syncing de kans dat Gedupeerden de controle over hun persoonsgegevens zouden verliezen en in hun privacybelangen zouden worden geschaad zou worden verhoogd. Sterker nog, zij hadden moeten voorzien dat Gedupeerden hierdoor daadwerkelijk de controle over hun persoonsgegevens verliezen omdat zij op onrechtmatige wijze persoonsgegevens verwerken. Dit had Oracle en Salesforce moeten weerhouden van hun handelingen.[548] Oracle en Salesforce hebben bewust de verhoging van de kans op schade bij de Gedupeerden aanvaard.

5.9.2.4 Toerekenbaarheid

797. De handelingen van Oracle en Salesforce in groepsverband kunnen hen tevens worden toegerekend (vereiste iii). Elk van de deelnemers aan deze groep, en zeker Oracle en Salesforce, kunnen namelijk besluiten deze activiteiten te staken. Door dat niet te doen, maar commercieel actief te blijven in deze groep, is het onrechtmatig handelen toerekenbaar aan elk van hen.

5.9.2.5 Onrechtmatige daad jegens Gedupeerden

798. Tot slot leveren de handelingen van de groep waardoor de schade is toegebracht, een onrechtmatige daad jegens de Gedupeerden op (vereiste iv) (zie paragraaf 8.1). Oracle en Salesforce zijn, als deelnemers van de groep, verantwoordelijk voor grootschalige verwerkingen van persoonsgegevens van internetgebruikers op de RTB markt in strijd met de AVG en de Tw.

799. De Stichting meent dan ook dat Oracle en Salesforce hoofdelijk aansprakelijk zijn op grond van artikel 6:166 BW.

## 6 TOELICHTING OP HET PETITUM

### 6.1 Wet afwikkeling massaschade in collectieve actie

800. De gebeurtenissen waarop de door de Stichting ingestelde vorderingen betrekking hebben, worden door de nieuwe Wet afwikkeling massaschade in collectieve actie (WAMCA) bestreken.[549] Uit artikel 119a lid 1 Overgangswet Nieuw Burgerlijk Wetboek volgt dat de nieuwe wet geldt voor collectieve acties die worden ingesteld op of na 1 januari 2020, voor gebeurtenissen die plaatsvonden op of na 15 november 2016.

[548] Asser/Hartkamp & Sieburgh 6-IV 2015/127.
[549] Wet van 20 maart 2019 tot wijziging van het Burgerlijk Wetboek en het Wetboek van Burgerlijke Rechtsvordering teneinde de afwikkeling van massaschade in een collectieve actie mogelijk te maken (Wet afwikkeling massaschade in collectieve actie) (Staatsblad 2019/130). De Wet afwikkeling massaschade in collectieve actie is in werking getreden op 1 januari 2020 bij Koninklijk Besluit van 20 november 2019.

801. Sinds 25 mei 2018 is de AVG in de gehele Europese Unie van toepassing. Meteen van het begin hebben Oracle en Salesforce de AVG geschonden. Het gaat dus om gebeurtenissen die hebben plaatsgevonden na 15 november 2016, waardoor de nieuwe wet van toepassing is.

802. In de onderhavige zaak gaat het enkel om feiten na van toepassing zijn van de AVG, en dus ook na 15 november 2016.

**6.2 Omschrijving groepen Gedupeerden**

803. De Stichting komt, ingevolge artikel. 3 lid 1 van haar statuten (**Productie 2**), op voor de belangen van:

> *"(...) natuurlijke personen die gebruikmaken van het internet door te surfen op het internet en/of door gebruik te maken van producten en/of diensten die persoonsgegevens in digitale vorm kunnen opslaan, overdragen of verwerken, waardoor jegens die internetgebruikers op enig moment een schending van hun recht op bescherming van hun privacy of hun recht op bescherming van hun persoonsgegevens plaatsvindt of heeft plaatsgevonden, een en ander in de ruimste zin van het woord."*

804. De uitkomst in deze procedure bindt al deze personen, tenzij zij zullen kiezen voor opt-out (ex artikel 1018f Rv). Het merendeel van de Gedupeerden heeft zijn/haar gewone verblijfplaats in Nederland.

805. De groep personen die wordt vertegenwoordigd door de Stichting valt uiteen in (voor wat betreft dit geschil) twee categorieën, te weten de groep die benadeeld is door Oracle, en de groep die is benadeeld door Salesforce. Gezamenlijk vormen zij een 'Nauw Omschreven Groep' als bedoeld in de WAMCA ("**Nauw Omschreven Groep**"). Deze twee groepen laten zich als volgt definiëren:

a. De groep die door Oracle is benadeeld (hierna de "**Oracle Groep**") en die ziet op

   i. alle natuurlijke personen

   ii. die een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Tw in gebruik hebben, of hebben gehad, en

   iii. waarop een cookie met de naam '**bku**' geplaatst is of is geweest,

   iv. op een moment of gedurende een periode dat zij in Nederland woonden of verbleven, na het van toepassing zijn van de AVG.

b. De groep die benadeeld is door Salesforce (hierna de "**Salesforce Groep**") en die ziet op:

   i. alle natuurlijke personen,

   ii. die een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Tw in gebruik hebben, of hebben gehad, en

   iii. waarop een cookie met de naam '**_kuid_**' geplaatst is of is geweest,

iv. op een moment of gedurende een periode dat zij in Nederland woonden of verbleven, na het van toepassing zijn van de AVG.

806. De Stichting zal de rechtbank verzoeken te bepalen dat:

a. ieder lid van de Nauw Omschreven Groep dat in Nederland woonachtig is of domicilie heeft gedurende een periode van drie maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, de mogelijkheid zal hebben bij schriftelijk bericht aan de griffie van de rechtbank te laten weten zich van de behartiging van hun belangen in deze collectieve actie te onttrekken (opt-out);

b. ieder lid van de Nauw Omschreven Groep dat buiten Nederland woonachtig is of domicilie heeft, gedurende een periode van zes maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, de mogelijkheid zal hebben bij schriftelijk bericht aan de griffie te laten weten in te stemmen met de behartiging van hun belangen in deze collectieve vordering (opt-in).

### 6.3 Exclusieve belangenbehartiger

807. De Stichting zal in hoofdstuk 8 'Ontvankelijkheid van de Stichting' toelichten dat zij voldoet aan de eisen van ontvankelijkheid. Dit leidt ertoe dat de Stichting collectieve vorderingen instelt die ertoe strekken de Stichting aan te wijzen als exclusieve belangenbehartiger in de zin van artikel 1018e Rv.

### 6.4 Toelichting vorderingen

808. De Stichting zal in deze procedure diverse vorderingen instellen.

a. Vordering I betreft de aanwijzing van de Stichting als exclusieve belangenbehartiger.

b. Vordering II betreft de vaststelling van de Nauw Omschreven Groep waarop deze zaak ziet. Een en ander is toegelicht in het lichaam van deze dagvaarding en in het bijzonder paragraaf 6.2 hiervoor.

c. Vordering III betreft de bepaling door de rechtbank dat personen die geen prijs stellen op deelname aan deze collectieve actie, zulks tijdig dienen te laten weten op een door de rechtbank voor te schrijven wijze (opt-out), en de wijze waarop buitenlandse Gedupeerden juist kunnen laten weten wel te willen deelnemen (opt-in).

d. Vordering IV betreft de vaststelling van hoofdelijke aansprakelijkheid van Oracle en Salesforce jegens elk lid van de Oracle Groep en de Salesforce Groep, op grond van de schending van de AVG en de Tw, zoals in het lichaam van deze dagvaarding uitvoerig omschreven.

e. Vordering V betreft de veroordeling tot vergoeding van schade door de schending van de AVG en de Tw, zoals in het lichaam van deze dagvaarding uitvoerig omschreven, aan de Oracle Groep, uitgaande van 10 miljoen leden als bedrag ineens (10 miljoen maal € 500 = € 5 miljard) althans € 500 per persoon, althans de in een schadestaatprocedure

vast te stellen schade en aan de Salesforce Groep, uitgaande van 10 miljoen leden als bedrag ineens (10 miljoen maal € 500 = € 5 miljard) althans € 500 per persoon, althans de in een schadestaatprocedure vast te stellen schade. Schadevergoeding wordt gevorderd hoofdelijk van beiden voor de Oracle Groep en de Salesforce Groep, althans van ieder van hen, ten aanzien van respectievelijk de Oracle Groep en de Salesforce Groep. De schadevordering wordt gebaseerd op artikel 82 AVG (rechtstreeks, zie paragraaf 5.5 hiervoor) als ook 6:162 BW (onrechtmatige daad, paragraaf 5.7.1) en artikel 6:212 BW (ongerechtvaardigde verrijking, paragraaf 5.8). In het lichaam van deze dagvaarding is al uitvoerig omschreven dat i) Oracle en Salesforce van vrijwel iedere Nederlandse internetgebruiker gegevens verzamelen en verwerken en ii) in 2019 circa 13.25 miljoen inwoners van 12 jaar ouders of ouder vrijwel dagelijks gebruik maken van het internet. Het is dan ook aannemelijk dat de Oracle Groep en de Salesforce groep uit tenminste 10 miljoen leden zal bestaan. De hoogte van de gevorderde schade bedraagt € 500 per lid van de Oracle Groep en € 500 per lid van de Salesforce Groep (paragraaf 5.5.4.2), en deze vertegenwoordigt immateriële en/of materiële schade (paragraaf 5.5.3 en 5.5.5), begroot op forfaitaire (paragraaf 5.5.4.2) of abstracte basis (paragraaf 5.7.6.2), dan wel op basis van winstafdracht (paragraaf 5.7.6.1) en ongerechtvaardigde verrijking (paragraaf 5.8). De aard van een vordering op grond van artikel 3:305a BW brengt met zich mee dat het mogelijk is het totaalbedrag te voldoen aan de Stichting, en de Stichting vervolgens te belasten met de verdeling daarvan.

f. Vordering VI betreft de veroordeling tot vergoeding van schade ten aanzien het datalek bij Oracle, aan de leden van de Oracle Groep en/of Salesforce Groep van wie de gegevens (mogelijk) toegankelijk zijn geweest gedurende de inbreuk op de beveiliging waarover in juni 2020 is bericht (paragraaf 5.8.4). De aldus veroorzaakte schade wordt forfaitair begroot op EUR 100 per lid van de Oracle Groep en/of Salesforce Groep, althans de in een schadestaatprocedure vast te stellen schade. Dat sprake is van schade is gesteld en voldoende duidelijk. De aard van een vordering op grond van artikel 3:305a BW brengt met zich mee dat het mogelijk is het totaalbedrag te voldoen aan de Stichting, en de Stichting vervolgens te belasten met de verdeling daarvan.

g. Vordering VII en vordering VIII betreft de vordering tot het doen van verstrekken van informatie door Oracle en Salesforce. Zij hebben inzicht in de wijze waarop en ten aanzien van wie zij de AVG hebben geschonden, en het is voor de Stichting en de Nederlandse internetgebruikers vele malen belastender om dat op individueel niveau in kaart te brengen. Het is niet ongebruikelijk in collectieve acties dat de last van de identificatie van de gelaedeerden wordt neergelegd bij de (veroordeelde) gedaagde (zie bijvoorbeeld paragraaf 7.4. Voor identificatie van de personen ten aanzien van wie inbreuk is gemaakt op de bescherming van persoonsgegevens, is inzicht nodig in bij wie een cookie is geplaatst en ten aanzien van wie op andere manieren gegevens zijn verzameld. Dit is soms aantoonbaar vanaf de randapparatuur van de betrokken Nederlandse internetgebruiker, maar dat zal niet altijd het geval zijn. Met het oog daarop, en op de verdeling van de gelden, vordert de Stichting dat Oracle en Salesforce de bij hen beschikbare informatie over van wie zij persoonsgegevens verwerken zullen verstrekken (Vordering VII). Hetzelfde geldt voor de gegevens over de (categorie) personen die benadeeld zijn door de inbreuk op de beveiliging bij Oracle, de aard,

oorzaak, omvang en duur van de inbreuk, alsmede de gecompromitteerde gegevens (Vordering VIII). De Stichting vordert met het oog op deze informatie verplichtingen een boete (Vordering IX), als prikkel tot nakoming, van € 1.000 per tekortkoming per dag.

h. Vordering X betreft de vordering tot vergoeding van proceskosten en toewijzing van overige vergoedingen. Op grond van artikel 1018l Rv kan de rechter afwijken van de gewone regels van kostenveroordeling in het geval de vordering van de eiser (geheel of gedeeltelijk) wordt toegewezen (artikel 1018i Rv), dat wil zeggen: meer toewijzen, zoals de werkelijke kosten. Verwezen zij naar paragraaf 6.7.2. De Stichting is bereid de door haar gemaakte kosten te onderbouwen door overlegging van alle benodigde bescheiden, in een latere fase van de procedure. Daarbij vordert de Stichting ook vergoeding van de door de Financier bedongen vergoeding (verwezen zij naar paragraaf 6.6).

i. Vordering XI betreft het voorstel van de Stichting ten aanzien van de wijze van afwikkeling van de schade. Daarbij gaat de Stichting er vanuit dat zowel de Oracle Groep als de Salesforce Groep uit zeker 10 miljoen personen bestaat. Het kan zijn dat niet allen tijdig de aan hen toekomende schadevergoeding zullen claimen. De Stichting stelt voor dat enig overschot door haar en in lijn met haar statutaire doelstelling zal worden afgedragen aan een non-profit organisatie die actief is op het gebied van privacy bescherming, en dus niet teruggaat naar Oracle en Salesforce. Dat is anders voor wat betreft het door de Stichting gevorderde bedrag dat Oracle en Salesforce aan de Stichting dienen te betalen om te voorzien in de kosten van afhandeling van de uitkering van de schade aan de Oracle Groep en de Salesforce Groep, door inschakeling van een professionele claimafhandelaar (zie paragraaf 6.5 hierna): enig overschot daarvan zou wel terug dienen te vallen aan Oracle en Salesforce.

## 6.5 Mogelijke constructies voor het betalen van schade en/of het schikken

809. De Stichting stelt zich ten doel schadevergoeding te verwezenlijken ten behoeve van haar achterban. Zij moet daartoe zeer aanzienlijke kosten maken. Die kosten vallen echter in het niet bij de schadevergoeding die van Oracle en Salesforce in totaliteit gevraagd wordt: aangenomen dat 10 miljoen Gedupeerden in aanmerking komen voor een vergoeding van (minimaal eenmaal) € 500 per persoon, betreft de schade minimaal € 5 miljard per gedaagde partij.

810. Vergoeding van dergelijk grote bedragen, over zoveel mensen, vergt maatwerk. Onder de WCAM is daarmee ervaring opgedaan in algemeen verbindend verklaarde schikkingen, zoals in de Dexia zaak of AEGEAS.[550]

811. Wat de Stichting betreft heeft het de voorkeur als partijen in overleg met uw rechtbank komen tot een passende oplossing. In het alternatieve scenario dat uw rechtbank eenzijdig beslist op welke wijze de schadevergoeding zal dienen plaats te vinden, wordt mogelijk niet voldoende rekening gehouden met de praktische problemen en grote kosten die gepaard gaan met de afwikkeling van een dergelijke collectieve actie.

[550] Gerechtshof Amsterdam, 25 januari 2007, *NJ* 2007, 427; Gerechtshof Amsterdam, 13 juli 2018, ECLI:NL:GHAMS:2018:2422.

812. De Stichting ziet voor zich dat, indien haar vorderingen worden toegewezen, Oracle en Salesforce het totale bedrag aan schadevergoeding, overmaken aan de Stichting, die het vervolgens zal verdelen. De Stichting zal daartoe een professionele derde partij inhuren, zoals bijv. Computershare.[551] Dergelijke partijen hebben een zeer aanzienlijke track record in met name de Verenigde Staten, maar inmiddels ook in Nederland, met het afwikkelingen van collectieve acties. De rol van een claimafhandelaar is met name het identificeren van de partijen die aanspraak hebben op schadevergoeding en het betalen van schadevergoeding. In dit geval betreft het miljoenen mensen, wat wil zeggen dat mogelijk miljoenen mensen geïdentificeerd moeten worden, en wellicht nadere documentatie moeten aanleveren om aan te tonen dat zij lid zijn van de Nauw Omschreven Groep en in aanmerking komen voor schadevergoeding. Dat vergt een aanzienlijke inspanning, zowel wat betreft informatietechniek als mensenwerk. De ervaring leert dat de kosten van een dergelijke operatie al snel € 10 miljoen of meer kost, en veel tijd in beslag neemt.

813. De Stichting stelt zich voor dat, indien haar vorderingen worden toegewezen, Oracle en Salesforce aan de Stichting betalen (i) de diverse kostenveroordelingen, de vergoeding van de fee van de Financier en een voorschot voor de kosten van de claimafhandelaar van bijv. € 15 miljoen en (ii) de schadevergoeding. De bedragen onder (i) zullen door de Stichting zelf worden (door)betaald of behouden en de bedragen onder (ii) zullen door de claimafhandelaar worden beheerd, in opdracht van de Stichting.

814. Het is mogelijk dat een dispuut ontstaat tussen de Stichting en/of de claimafhandelaar enerzijds, en een persoon die betaling verzoekt anderzijds. De Stichting ziet voor zich dat Uw rechtbank bepaalt dat een ieder die uitkering wenst, zich onderwerpt aan geschillenbeslechting op basis van bindend advies, en dat partijen zich daarover nader bij akte uitlaten.

### 6.6 Vergoeding Financier

815. De Stichting heeft geen vergoeding gevraagd van de Gedupeerden, maar heeft haar kosten gefinancierd met behulp van een externe Financier. De Financier draagt het gehele procesrisico en het risico dat de gemaakte kosten niet kunnen worden terugverdiend. In ruil daarvoor vraagt de Financier een resultaatsafhankelijke vergoeding (een commissie), variërend van 25%, 15% of 10%, van de door de Stichting ten behoeve van de Nauw Omschreven Groep te ontvangen schadevergoeding.

816. Uit de wetsgeschiedenis volgt dat de Stichting ex artikel 6:96 BW en ex artikel 1018l lid 2 Rv de kosten van de Financier vergoed kan krijgen: [552]

> *(…) Als er een externe financier bij betrokken is, betaalt deze in het algemeen ook de kosten van de exclusieve belangenbehartiger. Artikel 6:96 BW en artikel 1018l van het voorstel kunnen dan gebruikt worden om de kosten van de financier vergoed te krijgen. (…)".*

[551] https://www.computershare.com.
[552] Zie ook *Kamerstukken II* 2017/18, 34 608, nr. 9, p. 5; *Kamerstukken II* 2017/18, 34 608, nr. 9, p. 14.

817. Ook de vergoeding die de Financier bedingt voor zijn bereidheid de proceskosten te financieren en het procesrisico te lopen, moet voor rekening van Oracle en Salesforce kunnen worden gebracht.[553] De Stichting vordert dan ook dat de kosten van de Financier én de vergoeding die de Financier heeft bedongen voor rekening van Oracle en Salesforce komen ex artikel 1018l lid 2 Rv of artikel 6:96 BW. In het petitum wordt deze vergoeding zowel op grond van artikel 6:96 BW alsmede op grond van artikel 1018 lid 2 Rv gevorderd, maar hier is geen dubbeltelling mee beoogd.

818. De vergoeding die de Financier heeft bedongen, is redelijk in het licht van de werkelijk verrichte werkzaamheden en het procesrisico dat zij loopt. De Financier heeft aanzienlijke investeringen en uitgaven gedaan door alle kosten van de Stichting te financieren, dat wil zeggen de kosten ter zake van het feitelijk onderzoek, juridisch onderzoek, vergoedingen voor bestuur en raad van toezicht, de kosten van het inrichten en onderhouden van websites en databanken, kosten van andere adviseurs zoals de notaris, fiscalist, accountant, en ook de advocaatkosten. Daarnaast geldt dat het gebruikelijk is dat een Financier een vergoeding in rekening brengt. Collectieve procedures kunnen kostbaar zijn. Het is echter van maatschappelijk belang dat collectieve procedures kunnen worden gevoerd, zodat daarvoor doorgaans een financiering moet worden gevonden. De Financier vraagt doorgaans in ruil voor de gemaakte kosten en het procesrisico dat zij loopt een resultaatsafhankelijke vergoeding, zoals ook in deze zaak het geval is. Daar staat tegenover dat de Stichting geen financiële bijdrage vraagt van de Gedupeerden. Gedupeerden kunnen zich kosteloos aansluiten bij de Stichting en van haar activiteiten profiteren.

819. Bovendien voldoet de Stichting ook aan de Claimcode. De Claimcode staat het immers toe dat de Stichting externe financiering aantrekt en dat de Stichting met de externe financier een vergoeding overeenkomt die is gebaseerd op een percentage van een in of buiten rechte toe te kennen collectieve (schade)vergoeding:[554]

> *"(...) Als de externe financier een vergoeding toekomt die is gebaseerd op een percentage van een in of buiten rechte toe te kennen collectieve (schade)vergoeding, vermeldt de belangenorganisatie ook het desbetreffende percentage."*

820. Uit het voorgaande volgt dat de belangen van de Gedupeerden aldus zorgvuldig worden behartigd en de vergoeding die de Financier heeft bedongen voor rekening van Oracle en Salesforce zal moeten komen.

## 6.7 Proceskostenveroordeling

### *6.7.1 Proceskostenopgave*

821. De Stichting wenst haar proceskosten vergoed te krijgen. Deze kosten bestaan onder meer uit de kosten van de deurwaarder, het vast recht, advocaatkosten en de kosten van en de vergoeding aan de Financier.

[553] Zie ook M.W. Schonewille, 'Over litigation funding: relevante praktische en juridische aspecten' *TOP* 2019/325, nummer 6, oktober 2019.
[554] Claimcode Principe III, uitwerking 7.

822. De Stichting behoudt zich het recht voor om de proceskostenopgave aan te vullen met een overzicht van gemaakte/nog te verwachten kosten na het uitbrengen van deze dagvaarding.

823. De Stichting zal hieronder toelichten dat zij aanspraak kan maken op vergoeding van de proceskosten ex artikel 1018 lid 2 Rv en/of artikel 237 Rv.

*6.7.2 Artikel 1018l lid 2 Rv*

824. Artikel 1018l lid 2 Rv voorziet in vergoeding van de daadwerkelijk gemaakte proceskosten, waaronder, maar niet beperkt tot de advocaatkosten die afwijkt van artikel 237 Rv. Door de woorden "een uitspraak ingevolge artikel 1018i" geldt de afwijkende proceskostenregeling alleen voor het geval de rechter een uitspraak doet waarbij hij een collectieve schadeafwikkeling vaststelt. Aldus is nadrukkelijk ruimte gemaakt door de wetgever voor de rechter om de door de Stichting gemaakte kosten te vergoeden en af te wentelen op de gedaagde.[555] Ook de door de Stichting aan de Financier af te dragen vergoeding kan langs deze weg ten laste van de gedaagde worden gebracht, zoals hiervoor toegelicht.[556] De Stichting vordert dan ook op grond van artikel 1018l lid 2 Rv een hoofdelijke veroordeling van Oracle en Salesforce in de redelijke en evenredige gerechtskosten en andere kosten die de Stichting heeft gemaakt.

*6.7.3 Artikel 237 Rv*

In het geval de collectieve schadeafwikkeling wordt afgewezen en uitsluitend de verklaringen voor recht worden toegewezen, vordert de Stichting primair een hoofdelijke veroordeling van Oracle en Salesforce in de daadwerkelijk gemaakte proceskosten ex artikel 1019h Rv en subsidiair een hoofdelijke veroordeling tot vergoeding van de gemaakte proceskosten ex artikel 237 Rv.[557]

## 6.8 Buitengerechtelijke kostenveroordeling

825. De Stichting vordert ook vergoeding van de volledig gemaakte (buitengerechtelijke) kosten op grond van artikel 6:96 BW, waaronder begrepen de kosten van de Financier,[558] voor zover die niet reeds geheel in aanmerking zijn genomen op basis van artikel 1018l lid 2 Rv.

826. Deze kosten bestaan uit de gemaakte en nog te maken deskundigenkosten en de gemaakte en nog te maken kosten van juridisch advies. Deze kosten bestaan ook uit de kosten ter verkrijging van voldoening buiten rechte ex artikel 6:96 lid 2 c BW.

827. In totaal bestaan de buitengerechtelijke kosten uit een bedrag van € 10 miljoen, exclusief de vergoeding die de Stichting verschuldigd zal zijn aan de Financier. Gelet op de omstandigheden van dit geval waren de verrichte werkzaamheden redelijkerwijs noodzakelijk en zijn de kosten naar hun omvang redelijk.[559] De Stichting komt op ten behoeve van 10

[555] *Kamerstukken II* 2016/17, 34 608, nr. 3, p. 54.
[556] *Kamerstukken II* 2017/18, 34 608, nr. 9, p. 14.
[557] Zie ook over hoofdelijke veroordeling in de proceskosten ex artikel 237 RV: Tekst & Commentaar Burgerlijke Rechtsvordering, Proceskostenbeslissing, algemeen bij: Wetboek van Burgerlijke Rechtsvordering. Artikel 237; Zie ook de bevestiging hiervan in: Asser Procesrecht/Van Schaick 2 2016/136.
[558] *Kamerstukken II* 2017/18, 34 608, nr. 9, p. 14, waar nadrukkelijk wordt overwogen dat deze kosten ook op grond van artikel 6:96 BW voor vergoeding in aanmerking komen.
[559] Zie ook Parlementaire Geschiedenis, Boek 6, p. 337 (MvA II).

miljoen mensen, die gezamenlijk een vordering hebben die vele malen groter is dan de door de Stichting gemaakte kosten. De individuele leden van de Nauw Omschreven Groep zijn niet in staat op vergelijkbaar efficiënte wijze genoegdoening te verkrijgen, gegeven het – in vergelijking met de door hen te maken kosten van onderzoek en juridische kosten – relatief geringe schadebedrag.

# 7 BEWIJS

## 7.1 Inleiding

828. Aan de vorderingen van de Stichting liggen met name de volgende feiten en stellingen ten grondslag:

a) Oracle en Salesforce verwerken zonder grondslag de gegevens van Nederlandse internetgebruikers, door zonder toereikende toestemming cookies te plaatsen en op andere wijzen gegevens te verzamelen en te verwerken in het kader van hun DMP dienst (zie paragraaf 4.6.1);

b) Oracle en Salesforce verstrekken geen adequate informatie ten aanzien van het gebruik van cookies, cookie syncing en de verdere verwerking in het kader van het aanbieden van de DMP dienst (zie paragraaf 4.6.3 “Verwerking niet transparant”);

c) Oracle en Salesforce verzamelen, combineren en delen onbeperkt en bovenmatig persoonsgegevens (zie paragraaf 4.6.4 “Verwerking in strijd met dataminimalisatie”);

d) Oracle en Salesforce geven persoonsgegevens aan de Verenigde Staten door, waar geen passend beschermingsniveau kan worden geboden (zie paragraaf 4.6.5 “‘Verboden doorgifte aan de Verenigde Staten’”);

e) Oracle heeft geen adequate technische en organisatorische maatregelen genomen om persoonsgegevens adequaat te beveiligen. Dit blijkt uit een datalek van Oracle in 2020, waardoor miljoenen persoonsgegevens die zij heeft verzameld, op straat zijn komen te liggen (zie paragraaf 4.7 “Oracle beschermt persoonsgegevens onvoldoende, blijkens een datalek in 2020”); en

f) De gedupeerden lijden door de inbreukmakende handelingen van Oracle en Salesforce (enige vorm van) schade.

829. De Stichting meent dat zij met deze dagvaarding meer dan voldoende heeft gesteld ter zake van elk van deze feiten en stellingen. Tezelfdertijd is het zo dat een groot deel van de feitelijke gang van zaken zich aan de waarneming van de Stichting (en de internetgebruikers) onttrekt en dat die ook voor de door de Stichting ingeschakelde externe specialisten, niet na te gaan is zonder medewerking van Oracle en Salesforce zelf. De verwerkingen in het kader van de DMPs vinden immers grotendeels “achter de schermen” plaats op de servers en in de systemen van met name Oracle en Salesforce, waartoe de Stichting geen toegang heeft. De Stichting hoeft echter niet te stellen en bewijzen hoe de DMP activiteiten precies werken, en welke rol ieder van de deelnemers daarbij precies vervullen. Dat is niet dragend voor de door de Stichting ingestelde vorderingen en de stelplicht/bewijslast daarvan rust niet op haar.

### 7.2 Bewijsrechtelijke uitgangspunten

830. De Stichting hoeft ook niet te bewijzen dat Oracle en Salesforce de beginselen van de AVG hebben geschonden. Hiervoor heeft de Stichting toegelicht dat in onderhavige zaak de volgende bewijsrechtelijke uitgangspunten hebben te gelden (zie onder meer paragraaf 4.3.2.2, 5.2.1, 5.2.2 en 5.2.3 en randnummers 401, 412 en 624):

- Oracle en Salesforce worden vermoed persoonsgegevens te verwerken op grond van de Tw;
- Oracle en Salesforce zijn verwerkingsverantwoordelijke in de zin van de AVG. Indien Oracle en Salesforce menen dat zij geen verwerkingsverantwoordelijke zijn, dienen zij dit aan te tonen;
- De bewijslast ten aanzien van de naleving van de AVG rust op Oracle en Salesforce;
- Oracle en Salesforce dienen (op grond van de transparantieverplichting) duidelijkheid te verschaffen over wie de verantwoordelijke is en wie overigens (als bron of ontvanger) betrokken zijn bij de verwerking van de persoonsgegevens;
- Zelfs als Oracle en Salesforce onder de AVG slechts de verwerker zouden zijn en zelfs als geen sprake zou zijn van een verwerking van persoonsgegevens, rust op hen krachtens artikel 11.7a Tw de bewijslast om aan te tonen dat toestemming is verkregen en is geïnformeerd en dat die toestemming en informatie aan de AVG voldoen, omdat zij de cookies plaatsen; en
- Het causaal verband (csqn-verband) wordt reeds aangenomen bij schending van de AVG door Oracle en Salesforce.

831. In deze zaak stelt Oracle zich op het standpunt dat zij slechts als verwerker moet worden beschouwd voor haar DMP dienst (zie hierna in hoofdstuk 10 ‘Bekende verweren en weerlegging’). De Stichting heeft reeds in deze dagvaarding gemotiveerd uiteengezet dat deze stelling onjuist is. Zoals hiervoor opgesomd, geldt als uitgangspunt dat Oracle dient aan te tonen dat zij geen verwerkingsverantwoordelijke is.

832. Daarnaast kwalificeert het verweer van Oracle dat zij slechts (gedeeltelijk) verwerker zou zijn, als een ‘zelfstandig’ of ‘bevrijdend’ verweer. Dit betekent dat op Oracle de bewijslast rust van de aan haar verweer ten grondslag liggende feiten en omstandigheden. Ook ten aanzien van Salesforce geldt dat indien Salesforce zich op het standpunt zou stellen dat zij slechts als verwerker moet worden beschouwd, op Salesforce de bewijslast rust van de daaraan ten grondslag liggende feiten en omstandigheden.

### 7.3 Subsidiair: verzoek tot het leveren van bewijs door een deskundigenbericht te bevelen ex artikel 194 Rv

833. Indien onverhoopt wordt geoordeeld dat enige bewijslast op de Stichting komt te rusten, verzoekt de Stichting de rechtbank dat zij wordt toegelaten bewijs te leveren door middel van een deskundigenadvies. De rechter heeft een discretionaire bevoegdheid om al dan niet een deskundigenbericht te bevelen.

834. Daarbij merkt de Stichting op dat hierbij in aanmerking moet worden genomen dat de Gedupeerden schade hebben geleden door de inbreukmakende handelingen van Oracle en Salesforce en deze schade vergoed dient te worden. Een groot gedeelte van de inbreukmakende handelingen speelt zich echter af achter de schermen bij Oracle en Salesforce. Door allerhande informatie te analyseren heeft de Stichting een beeld kunnen schetsen van wat Oracle en Salesforce achter de schermen doen. De Stichting beschikt echter niet over alle relevante informatie en gegevens in deze zaak. De enige manier om alle gegevens boven water te krijgen, indien nodig, is via de inbreukmakende partijen zelf, te weten Oracle en Salesforce.

835. De Stichting verzoekt uw rechtbank dan ook zo nodig een deskundige in te schakelen ex artikel 194 Rv. De deskundige kan (onder meer) onderzoek verrichten naar:

- De rol van Oracle en Salesforce in het RTB systeem;
- Hoe de DMP activiteiten precies werken, en welke rol ieder van de deelnemers daarbij precies vervullen;
- Welke DMP activiteiten Oracle en Salesforce verrichten;
- Op welke manier Oracle en Salesforce precies de persoonsgegevens van de Gedupeerden verwerken;
- Welke persoonsgegevens Oracle en Salesforce precies verwerken;
- Hoe lang Oracle en Salesforce persoonsgegevens bewaren;
- De wijze waarop Oracle de persoonsgegevens beveiligt;
- De waarde van de persoonsgegevens die onrechtmatig door Oracle en Salesforce zijn verwerkt.

### 7.4 Subsidiair: andere mogelijkheden om noodzakelijke informatie te verkrijgen in onderhavige zaak

836. Indien en voor zover zou worden vastgesteld dat de bewijslast op de Stichting rust en zij nog niet (volledig) in het leveren van bewijs is geslaagd, dan ziet de Stichting er aanleiding toe dat zij ten behoeve van de Gedupeerden in deze procedure op bewijsrechtelijk gebied tegemoet wordt gekomen. Artikel 150 Rv en regels van geschreven en ongeschreven recht maken dit mogelijk. De ernst van de handelingen van Oracle en Salesforce, zoals uitgebreid besproken in deze dagvaarding, de aard van de vorderingen van de Gedupeerden en de omstandigheden van het geval geven daartoe aanleiding. Hierbij geldt ook dat de belangen van de Gedupeerden om meer duidelijkheid en informatie te verkrijgen aanmerkelijk zwaarder wegen dan de belangen van Oracle en Salesforce om hun (inbreukmakende) handelen geheim te houden.

837. De feiten spelen zich grotendeels achter de schermen bij Oracle en Salesforce af. Het is aldus noodzakelijk dat zij de relevante informatie en gegevens op tafel leggen. Er zijn meerdere manieren voor de rechtbank om hieraan vorm te geven in het geval Oracle en Salesforce de noodzakelijke informatie niet op tafel leggen. Deze zullen hieronder een voor een worden toegelicht.

a. Op basis van algemene ervaringsregels kan een feitelijk vermoeden worden aangenomen ten nadele van Oracle en Salesforce;[560]

   i. Zo kan gezien (de aard van) de handelingen, de motieven en de inbreuk van Oracle en Salesforce, bijvoorbeeld reeds op basis van een vermoeden worden aangenomen dat de Gedupeerden daar schade door hebben geleden.

b. De bewijslast kan op enigerlei andere wijze worden verdeeld of omgekeerd, in overeenstemming met de redelijkheid en billijkheid;[561]

   i. De rechtbank kan de bewijslast omkeren naar Oracle en Salesforce in verband met de stellingen van de Stichting rondom de inbreuk, het onrechtmatig handelen van Oracle en Salesforce, en de omvang van de schade die deze heeft veroorzaakt bij de Gedupeerden.

c. Oracle en Salesforce kunnen bezwaard worden met een verzwaarde stel- of motiveringsplicht teneinde de bewijsnood van de Stichting te verlichten;[562]

   i. De Stichting stelt vast dat in dit geval Oracle en Salesforce, anders dan de Gedupeerden en de Stichting, over de relevante informatie en gegevens beschikken, althans over veel meer informatie beschikken dan Gedupeerden en de Stichting kunnen doen. Een groot deel van de feitelijke gang van zaken onttrekt zich aan de waarneming van de Stichting en de internetgebruikers. Oracle en Salesforce beschikken over de informatie hoe zij deelnemen aan het RTB systeem, welke DMP activiteiten zij verrichten en op welke manier zij precies de persoonsgegevens van de Gedupeerden verwerken en hun privacy schenden. De Stichting stelt zich dan ook op het standpunt dat op Oracle en Salesforce (in ieder geval) een verzwaarde stelplicht (motiveringsplicht van het verweer) dient te rusten.

d. De rechtbank kan ook gebruikmaken van de omkeringsregel met betrekking tot het causaal verband bij de onrechtmatige daad; [563]

   i. De Stichting stelt zich primair op het standpunt dat het bestaan van causaal verband (in de zin van het csqn-verband) tussen de onrechtmatige daad van Oracle en Salesforce en de schade wordt aangenomen nu artikel 6:162 BW (en artikel 6:98 BW) AVG-conform dient te worden uitgelegd (paragraaf 5.7.5).

   ii. Subsidiair stelt de Stichting zich op het standpunt dat indien de AVG-conforme uitleg niet wordt gevolgd ook in dat geval het bestaan van het csqn-verband tussen de onrechtmatige daad van Oracle en Salesforce en de schade dient te worden aangenomen nu sprake is van schending van een norm die ertoe strekt een specifiek gevaar te voorkomen en dit specifieke gevaar zich heeft verwezenlijkt (paragraaf 5.7.5).

[560] Asser Procesrecht 3 Bewijs 2017/304; Asser/Vonken 10-I 2018/193.
[561] Asser Procesrecht 3 2017/291.
[562] Asser Procesrecht 3 Bewijs 2017/306 en 307.
[563] Asser Procesrecht 3 2017/302.

### 7.5 Waarheidsplicht (artikel 21 Rv)

838. Verder geldt dat de waarheidsvinding een fundamenteel beginsel is van procesrecht (artikel 21 Rv). Hieraan kan in rechte alleen betekenisvol invulling gegeven worden met een zo veel mogelijk volledige en correcte vaststelling van de feiten. Op de partijen rust derhalve een waarheids- en volledigheidsplicht. De rechter heeft de opdracht recht te doen op grond van de werkelijkheid (de waarheidsvinding). Dit vertaalt zich erin dat de procespartijen ten opzichte van elkaar ook informatierechten en -plichten hebben.[564] Zij kunnen er aanspraak op maken dat informatie die voor hen relevant is en waarover alleen de wederpartij beschikt, hen niet behoort te worden onthouden.[565] Zij dragen aan wat van belang is voor het geschil. Partijen hebben geen zwijgrecht en kunnen verplicht worden tegen zichzelf bewijsmateriaal in de procedure te brengen of tegen zichzelf te getuigen.[566]

839. Nu voor een groot gedeelte van de onderhavige handelingen van Oracle en Salesforce geldt dat zij achter de schermen plaatsvinden, ligt het voor de hand dat Oracle en Salesforce in dit kader verplicht worden de informatie te verstrekken waarover zij beschikken, waaronder gedetailleerde informatie over hoe zij hun servers en systemen hebben ingericht. Dit sluit tevens goed aan op de hiervoor besproken beginselen van transparantie en accountability.

### 7.6 Bewijsverrichtingen op grond van artikel 22 Rv

840. Het is tegen deze achtergrond dat de wetgever de rechter de bevoegdheid geeft om zelf, ambtshalve, het initiatief te nemen tot bewijsverrichtingen (art. 22 Rv). Hij kan partijen vragen stellen, bevelen stukken in de procedure te brengen, een deskundige benoemen die hem zal voorlichten, ter plaatse situaties gaan bekijken, en getuigen horen. Daarmee is de rechter niet helemaal afhankelijk van wat partijen aan bewijsmiddelen en bewijsinformatie aandragen. De rechter kan zo ook de goede kwaliteit van de waarheidsvinding bevorderen en daarmee de kwaliteit van zowel het proces als de uitspraak.[567]

841. Op deze manier kunnen zwakkere partijen, zoals de Gedupeerden, geholpen worden om hun recht te halen ten opzichte van een sterkere wederpartij, zoals Oracle en Salesforce. Met de aanduiding “zwakkere partijen” doelt de Stichting overigens niet alleen op de positie van de eenling, van de zijde van Oracle en Salesforce zou immers aangevoerd kunnen worden dat de Stichting niet zo zwak staat als een individuele internetgebruiker. Het gaat om de positie van de partij die benadeeld is doordat zij niet beschikt over de informatie en documenten die bepalend kunnen zijn voor de grondslagen van de vordering, terwijl de wederpartij wél over die informatie beschikt. Het is een kwestie van informatie-asymmetrie, die zou kunnen leiden tot bewijsnood aan de kant van individuele internetgebruikers en de Stichting. Die kennis ligt binnen het domein van Oracle en Salesforce, en het is dan aan hen om een eventuele betwisting nader te onderbouwen. De Stichting kan bijvoorbeeld ook de stellingen van Oracle en Salesforce, zoals ingenomen in de sommatiebrief, niet (geheel) controleren door het gebrek aan informatie.

[564] Asser Procesrecht 3 2017/41; HR 25 maart 2011, ECLI:NL:HR:2011:BO9675, *NJ* 2012/627 (*Waarheidsplicht*).
[565] Asser Procesrecht 3 2017/29.
[566] Asser Procesrecht 3 2017/40.
[567] Asser Procesrecht 3 2017/76.

842. Juist in het geval een eiser (met de stelplicht) aan een structureel informatietekort lijdt met name in het kader van het bewijzen van de causaliteit en de schade, omdat alle benodigde informatie zich in het domein van de wederpartij bevindt die de vorderingen en de gronden ervan betwist, is het noodzakelijk dat de wederpartij opening van zaken geeft. Doet een gedaagde dat niet, dan komen beginselen als fairplay en equality of arms, zoals volgend uit artikel 6 EVRM in het gedrang.

### 7.7 Vordering tot het verstrekken van informatie door Oracle en Salesforce

843. De Stichting heeft hiervoor al meerdere malen toegelicht dat er een informatie asymmetrie is, omdat een groot deel van de informatie in het domein van Oracle en Salesforce bevindt. Oracle en Salesforce weten precies op welke manier zij deelnemen aan het RTB systeem, welke DMP activiteiten zij verrichten en op welke manier zij de persoonsgegevens van de Gedupeerden verwerken en hun privacy schenden. De Gedupeerden weten vaak niet eens dat hun persoonsgegevens worden verwerkt, laat staan op welke wijze. Voorkomen moet worden dat Oracle en Salesforce hier ongehinderd mee door kunnen gaan.

844. In hun brieven van 18 juni en 17 juni en de gevoerde gesprekken van 7 juli en 3 juli betwisten Oracle en Salesforce een deel van de vorderingen en de feiten die de Stichting daaraan ten grondslag legt. Juist in dat geval, en gelet op de specifieke omstandigheden van deze zaak, is het nodig dat Oracle en Salesforce opening van zaken geven.

845. De Stichting maakt er dan ook aanspraak op dat de informatie die voor de ingestelde vorderingen relevant is en waarover alleen Oracle en Salesforce beschikken, haar niet wordt onthouden.[568]

846. Meer specifiek stelt de Stichting een vordering in die ertoe strekt dat zij inzicht krijgt in de wijze waarop en ten aanzien van wie Oracle en Salesforce de AVG en Tw hebben geschonden in verband met hun DMP activiteiten (waaronder mede moet worden begrepen de dienst die Oracle als ADM aanmerkt). Het is niet ongebruikelijk in collectieve acties, dat de last van de identificatie van de gelaedeerden wordt neergelegd bij de (veroordeelde) gedaagde (zie bijv. paragraaf 7.4). Relevant voor identificatie van de personen op ten aanzien van wie de AVG is geschonden, is inzicht in bij wie een cookie is geplaatst. Dit is soms aantoonbaar vanaf de randapparatuur van de betrokken Nederlandse internetgebruiker, maar gegeven de beperkte levensduur van cookies zal dit niet altijd het geval zijn. In dat geval kan relevant zijn welke websites, wanneer zijn bezocht, omdat daaruit kan worden afgeleid of zij een cookie geplaatst gekregen zullen hebben. Met het oog daarop, en de verdeling van de gelden, vordert de Stichting dat Oracle en Salesforce deze informatie zullen opgeven. Hetzelfde geldt voor de gegevens van de personen die benadeeld zijn door het datalek bij Oracle.

847. De Stichting behoudt zich daarnaast het recht voor om aanvullende vorderingen tot het verkrijgen van informatie in te stellen over in deze dagvaarding genoemde en andere onderwerpen.

848. Dat Oracle en Salesforce opening van zaken moeten geven, wordt ook onderstreept door de AVG. Wanneer Oracle en Salesforce niet veroordeeld worden tot het verstrekken van deze

[568] Asser Procesrecht 3 2017/29.

informatie, is de bescherming die aan de AVG kan worden ontleend feitelijk een wassen neus. De AVG heeft onder meer tot doel de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens te waarborgen. In de AVG is ook expliciet opgenomen dat de verwerkingsverantwoordelijken, in dit geval Oracle en Salesforce, moeten aantonen dat zij voldoen aan de verplichtingen die op grond van de AVG voor hen gelden. Oracle en Salesforce moeten openheid van zaken geven en de benodigde informatie verstrekken en niet door die informatie onder zich te houden aan (gedeeltelijke) aansprakelijkheid ontkomen.

849. Daarnaast wijst de Stichting er – ten overvloede op – dat de rechter bij begroting van schade niet gebonden is aan de regels van stelplicht en bewijslast. Als kan worden afgeleid dat schade is geleden dan mag de rechter niet zomaar de vergoeding daarvan afwijzen wegens gebrek aan onderbouwing van de omvang daarvan.[569]

850. Indien de benadeelde feiten stelt waaruit in het algemeen het geleden zijn van schade kan worden afgeleid, staat het de rechter vrij om, mede in aanmerking genomen de aard van de schade, zonder nader bewijs aannemelijk te achten dat schade is geleden en de omvang hiervan te schatten.

851. De Stichting stelt zich op het standpunt dat zij in deze dagvaarding voldoende feiten heeft gesteld waaruit het geleden zijn van schade door Gedupeerden kan worden afgeleid. Oracle en Salesforce hebben op grote schaal en voor commerciële doeleinden de persoonsgegevens van de Gedupeerden verzameld en verwerkt. Daarbij schenden zij op structurele wijze onder meer de AVG, Tw en het recht op privacy van de Nederlandse internetgebruikers. Hierdoor hebben de Gedupeerden de controle verloren over hun persoonsgegevens verloren. Uit deze feiten en omstandigheden kan worden afgeleid dat de Gedupeerden schade hebben geleden. Deze schade dient gelet op haar aard (verlies van controle over persoonsgegevens) voor vergoeding in aanmerking te komen.

852. De Stichting heeft in paragraaf 5.5.4-5.5.5 de omvang van de schade onderbouwd. Gelet op het voorgaande stelt de Stichting zich op het standpunt dat ook in het geval de onderbouwing niet afdoende zou zijn, de schadevorderingen niet mogen worden afgewezen.

853. De Stichting wijst er in dat kader ook op dat bij de begroting van de schade artikel 6:97 BW AVG-conform moeten worden uitgelegd. Dat betekent dat bij de begroting van de schade recht moet worden gedaan aan de doelstellingen van de AVG. De AVG heeft als uitgangspunt (overweging 146) dat de schade ruim moet worden uitgelegd in het licht van de rechtspraak van het HvJEU, op een wijze die ten volle recht doet aan de doelstellingen van deze verordening. De betrokkenen dienen volledige en daadwerkelijke vergoeding van door hen geleden schade te ontvangen. Dit uitgangspunt zal ook gevolgd moeten worden genomen bij de begroting van de schade die de Gedupeerden hebben geleden.

854. Voor wat betreft de schadevordering van de Stichting, die gebaseerd is op winstafdracht, wijst de Stichting erop dat het uiterst lastig is te stellen en te bewijzen om welke bedragen het gaat. Deze informatie is niet publiek. Nu begroting van schade op grond van winstafdracht echter een discretionaire bevoegdheid is van de rechter, behoeft concreet nadeel niet door de Stichting te worden aangetoond. Het is voldoende dat de aanwezigheid van enige (vorm van)

[569] HR 28 april 2000, ECLI:NL:PHR:2000:AA5651 (*Gemeente Dordrecht/Stokvast*).

schade aannemelijk is. Het is aan Oracle en Salesforce om aannemelijk te maken dat geen schade kan zijn ontstaan als gevolg van de gedraging waarvoor zij aansprakelijk worden gesteld.[570]

855. Zoals reeds uiteengezet in randnummers 734 e.v., beschikt de Stichting niet over informatie omtrent de winstgevendheid van de DMP activiteiten op de RTB markt voor Oracle en Salesforce. Door hen gepubliceerde (jaar)cijfers laten weliswaar miljarden Euro's aan inkomsten zien, maar geven onvoldoende inzicht in de revenuen die specifiek met cookie syncing op de Nederlandse (RTB) markt worden gegenereerd. De Stichting verzoekt Uw rechtbank dan ook om Oracle en Salesforce te bevelen concrete informatie over te leggen die ten minste een schatting van de winst mogelijk maakt van hun genoten voordeel gedurende de periode vanaf de het van toepassing zijn van de AVG.[571]

856. Tenslotte behoudt de Stichting zich het recht voor de schade van de Gedupeerden in de loop van deze procedure nader te onderbouwen.

### 7.8 Stichting biedt bewijs aan

857. Indien en voor zover het bewijs nog niet op alle onderdelen volledig geleverd wordt geacht, biedt de Stichting bewijs aan van al haar stellingen met alle middelen die tot haar beschikking staan. Hieronder valt ook het horen van getuigen, de benoeming van deskundigen en het in het geding brengen van nadere stukken. De Stichting aanvaardt daarbij vrijwillig geen enkele bewijslast die niet op haar rust.

## 8 ONTVANKELIJKHEID VAN DE STICHTING

### 8.1 Algemeen: de recente herziening van artikel 3:305a BW en het thans geldende normenkader

858. De Stichting procedeert op basis van artikel 3:305a BW. Artikel 3:305a BW is gewijzigd bij de inwerkingtreding van de Wet afwikkeling massaschade in collectieve actie.[572] Met de inwerkingtreding van de Wet afwikkeling massaschade in collectieve actie zijn de eisen aangescherpt voor de ontvankelijkheid van de belangenorganisaties die een collectieve actie voor een groep Gedupeerden willen instellen.

859. De eisen zijn met name aangescherpt om oneigenlijk gebruik van de collectieve actie procedure te voorkomen.[573] Dat perspectief noodzaakt tot een terughoudende opstelling voor de rechter bij het toetsen van de inrichting van een belangenorganisatie. Dat weerhoudt partijen die worden aangesproken in een collectieve actie procedure er doorgaans niet van om ontvankelijkheidsverweren te voeren. Die verweren worden dan met name gevoerd om te

[570] HR 18 juni 2010, ECLI:NL:HR:2010:BL9662, m.nt. T. Hartlief (*Setel/AVR*); HR 18 juni 2010, ECLI:NL:HR:2010:BM0893 (*Stichting Ymere*); G. van Dijck & R. Olde Wolbers, 'Winstafdracht en het schadevereiste, mede aan de hand van een vergelijking met Zwitsers recht', *WPNR*, 2015, p. 2.
[571] HR 18 juni 2010, ECLI:NL:HR:2010:BL9662, m.nt. T. Hartlief (*Setel/AVR*); HR 18 juni 2010, ECLI:NL:HR:2010:BM0893 (*Stichting Ymere*); Groene Serie Schadevergoeding, 3 Behaalde winst als maatstaf bij: Burgerlijk Wetboek Boek 6, Artikel 104.
[572] Wet van 20 maart 2019 tot wijziging van het Burgerlijk Wetboek en het Wetboek van Burgerlijke Rechtsvordering teneinde de afwikkeling van massaschade in een collectieve actie mogelijk te maken (Wet afwikkeling massaschade in collectieve actie) *(Stb.* 2019/130). De Wet afwikkeling massaschade in collectieve actie is in werking getreden op 1 januari 2020 bij Koninklijk Besluit van 20 november 2019.
[573] *Kamerstukken II* 2017/18, 34 608, 9, p.1.

ontkomen aan de hoofdzaak.[574] Daarvoor mag een ontvankelijkheidsverweer niet worden ingezet.

860. In artikel 3:305a lid 1 BW is bepaald dat (onder meer) de belangenorganisatie (i) een rechtsvordering kan instellen die strekt tot bescherming van gelijksoortige belangen van andere personen ('gelijksoortigheidsvereiste'), (ii) voor zover zij deze belangen ingevolge haar statuten behartigt ('het statutenvereiste') en (iii) met de rechtsvordering de belangen van de personen ten behoeve van wie de vordering is ingesteld voldoende zijn gewaarborgd ('het waarborgvereiste'). Het waarborgvereiste wordt verder uitgewerkt in artikel 3:305a lid 2 BW.

861. Artikel 3:305a lid 3 BW bevat een aantal aanvullende ontvankelijkheidseisen. Onderdeel a bepaalt dat bestuurders betrokken bij de oprichting van een belangenorganisatie en hun opvolgers, geen rechtstreeks of middellijk winstoogmerk mogen hebben, dat via de belangenorganisatie wordt verwezenlijkt. Onderdeel b bevat het vereiste dat de collectieve vordering een voldoende nauwe band met de Nederlandse rechtssfeer heeft. Onderdeel c bepaalt dat een belangenorganisatie in de gegeven omstandigheden voldoende moet hebben getracht het gevorderde door het voeren van overleg met Gedaagden, te bereiken.

862. Hierna staat de Stichting eerst stil bij het gelijksoortigheidsvereiste. Vervolgens zal de Stichting het statutenvereiste bespreken. Daarna wordt uitgewerkt waarom de Stichting voldoende geëquipeerd is om de belangen van de Gedupeerden te behartigen c.q. de belangen voldoende zijn gewaarborgd. Tevens zal toegelicht worden dat zowel de Stichting als de bestuurders geen winstoogmerk hebben en dat de vorderingen een voldoende nauwe band met de Nederlandse rechtssfeer hebben. Tenslotte zal ook aan bod komen dat voldoende is getracht een oplossing buiten rechte te bewerkstelligen met Oracle en Salesforce, maar dat dit niet is gelukt.

### 8.2 Gelijksoortigheidsvereiste

863. De bevoegdheid van belangenorganisaties om rechtsvorderingen in te stellen op grond van artikel 3:305a BW is beperkt tot de bescherming van gelijksoortige belangen. Uit vaste rechtspraak van de Hoge Raad volgt dat het vereiste van gelijksoortigheid vervuld is wanneer de belangen ter bescherming waarvan de vordering strekt, zich lenen voor bundeling, zodat een efficiënte en effectieve rechtsbescherming ten behoeve van de belanghebbenden kan worden bevorderd. De vorderingen lenen zich voor bundeling als daarover in één procedure geoordeeld kan worden zonder naar de bijzondere omstandigheden van de individuele belanghebbenden te kijken.[575]

864. De belangen van de Gedupeerden zijn in ieder geval gelijksoortig nu (i) hun persoonsgegevens worden verwerkt, en (ii) inbreuk wordt gemaakt op hun privacyrechten, waardoor zij schade hebben geleden, en (iii) de schade is veroorzaakt door Oracle en Salesforce. De belangen waar de vorderingen op zien laten zich voldoende veralgemeniseren om te kunnen worden gerekend tot de gelijksoortige belangen waarop artikel 3:305a BW het oog heeft. Alle leden van de Nauw Omschreven Groep hebben met elkaar gemeen getroffen te zijn door de (onrechtmatige)

[574] Zie ook K. Rutten, 'Art. 3:305a lid 2 BW schiet zijn doel voorbij!', *MvV* 2015/11.5, p. 324 en C.M.D.S. Pavillon & D.G.J. Althoff, 'Wijze raad is halve daad of veel raad maar weinig baat? De impact van de Aanbevelingen van de Juristengroep op het wetsvoorstel Afwikkeling massaschade in een collectieve actie', *MvV* 2017, p. 106.
[575] HR 26 februari 2010, ECLI:NL:HR:2010:BK5756 (*Stichting Baas in Eigen Huis/Plazacasa).*

verwerking van hun persoonsgegevens door Oracle en Salesforce voor louter commerciële doeleinden, op grote schaal en onbeperkt in tijd, zonder dat hier een rechtvaardigingsgrond voor bestaat en terwijl daarbij op overige voornoemde punten de AVG en Tw worden geschonden. Alle leden van de Nauw Omschreven Groep worden daarmee geschaad in hun privacyrechten.

865. De vorderingen zoals weergegeven onder paragraaf 6.4 vereisen een abstracte toets, zonder dat hiervoor bijkomende individuele omstandigheden behoeven te worden beoordeeld. In deze zaak gaat het bij alle Nederlandse internetgebruikers om precies dezelfde omstandigheid, namelijk dat Oracle en Salesforce inbreuk maken op de verplichtingen uit de AVG en Tw en onrechtmatig handelen jegens Nederlandse internetgebruikers, door de grootschalige en onbeperkte verwerking van hun persoonsgegevens, zonder rechtvaardigingsgrond, transparantie, etc. De privacybelangen van de Nederlandse internetgebruikers die hierdoor zijn benadeeld komen aldus met elkaar overeen en die zijn dus bundelbaar. De vorderingen lenen zich dan ook voor beoordeling in een collectieve actie.

866. Uit het voorgaande volgt dat aan het vereiste van gelijksoortigheid is voldaan.

### 8.3 Statutenvereiste

867. Het statutenvereiste houdt in dat het te behartigen belang in de statuten van de Stichting is geformuleerd en er activiteiten op het desbetreffende gebied zijn ontplooid.

868. De behartiging van de belangen van de Gedupeerden in deze procedure valt binnen de statutaire doelomschrijving van de Stichting. Zoals aangegeven, bepaalt artikel 3, lid 1 van de statuten (**Productie 2**) hierover:

> *"De Stichting heeft ten doel het behartigen van belangen van natuurlijke personen die gebruikmaken van het internet door te surfen op het internet en/of door gebruik te maken van producten en/of diensten die persoonsgegevens in digitale vorm kunnen opslaan, overdragen of verwerken, waardoor jegens die internetgebruikers op enig moment een schending van hun recht op bescherming van hun privacy of hun recht op bescherming van hun persoonsgegevens plaatsvindt of heeft plaatsgevonden, een en ander in de ruimste zin van het woord."*

869. Artikel 3 lid 2 van de statuten somt de activiteiten van de Stichting op:

> *"De Stichting tracht dit doel te bereiken door het doen van onderzoek naar de aansprakelijkheid van partijen die deze rechten schenden van de personen wier belangen door de Stichting worden behartigd, het voeren van onderhandelingen, het ondersteunen en initiëren van een of meer gerechtelijke procedures in Nederland of daarbuiten, waaronder, maar niet beperkt tot procedures als bedoeld in artikel 305a van Boek 3 van het Burgerlijk Wetboek en artikel 240 van Boek 6 van het Burgerlijk Wetboek, en het initiëren van andere juridische procedures, waaronder het eisen van verklaringen voor recht, het vragen om voorzieningen om onrechtmatig handelen aan te pakken en het eisen van passende vergoeding en voldoening, het treffen van schikkingen, het aangaan van een collectieve vaststellingsovereenkomst ter beëindiging van geschillen, en het (laten) berekenen*

*en vaststellen en (door)betalen van schadevergoedingen en het verrichten van al hetgeen met het vorenstaande in de ruimste zin verband houdt of daartoe bevorderlijk kan zijn."*

870. Aan de eis van feitelijke belangenbehartiging wordt voldaan. De Stichting heeft niet stil gezeten en neemt haar taken meer dan serieus. Zij heeft onder meer de volgende activiteiten ondernomen om de belangen van de Gedupeerden te behartigen:

- De Stichting doet (technisch) onderzoek naar de privacyaspecten bij de grootschalige verzameling en verwerking van persoonsgegevens van internetgebruikers en de rol van Oracle en Salesforce daarbij;
- De Stichting voert doorlopend campagne om het onrechtmatig gebruik van persoonsgegevens van internetgebruikers in Nederland en daarbuiten tegen te gaan. Daarvoor heeft zij een overkoepelende campagnewebsite in het leven geroepen: https://theprivacycollective.eu/nl/ waarop aanvullende informatie is te vinden over onder andere haar activiteiten in Nederland. Op deze campagnewebsite zijn ook diverse artikelen en onderzoeken gepubliceerd over adtech, RTB, cookies en andere tracking technologieën en over hoe bedrijven onrechtmatig persoonsgegevens verzamelen en gebruiken door netwerken van online platforms;
- De Stichting heeft ook een website die specifiek is ontwikkeld voor de collectieve actie Nederland (https://theprivacycollective.nl/). Hier vinden Gedupeerden uitgebreide informatie over de Stichting, haar werkwijze en activiteiten en biedt de Stichting de mogelijkheid tot het stellen van vragen;
- De Stichting heeft steun vergaard van belangrijke belangenorganisaties in Nederland die als doel hebben het behoud en de bevordering van het recht op privacy, zoals Bits of Freedom, Privacy First, Freedom Internet en Qiy Foundation;
- De Stichting is in overleg getreden met Oracle en Salesforce. Op 7 juli 2020 heeft zij een gesprek met Oracle gevoerd. Op 3 juli 2020 heeft zij een gesprek met Salesforce gevoerd. Zie hierna onder 8.5.4.

## 8.4 Waarborgvereiste

871. Artikel 3:305a lid 1 BW bepaalt dat de belangen van degenen waarvoor de belangenorganisatie opkomt voldoende dienen te zijn gewaarborgd. Daarbij mogen de uitgangspunten niet uit het oog worden verloren. Belangenorganisaties hebben namelijk de vrijheid om hun eigen organisatie in te richten.[576] Ook mag het recht op toegang tot de rechter niet licht worden beperkt.[577]

872. Artikel 3:305a lid 2 BW preciseert en versterkt deze eisen nader. Artikel 3:305a lid 2 BW bepaalt dat de belangen voldoende gewaarborgd zijn wanneer (i) de belangenorganisatie voldoende representatief is, gelet op de achterban en de omvang van de vorderingen en (ii) de belangenorganisatie voldoet aan een aantal eisen uit de Claimcode 2019 die gecodificeerd zijn

[576] Onder meer vanwege het bepaalde in art. 11 EVRM.
[577] Onder meer in verband met het bepaalde in art. 6 EVRM.

in dit lid. De Stichting zal deze vereisten hierna bespreken en toelichten dat zij aan deze vereisten voldoet.

*8.4.1 (i) Stichting is representatief voor de groep Gedupeerden*

873. Het gaat hierbij om de mate waarin een belangenorganisatie als representatief voor de groep Gedupeerden kan worden gezien. Representativiteit is van belang om te voorkomen dat een belangenorganisatie een rechtsvordering kan instellen zonder de vereiste ondersteuning van een achterban.

874. Of een belangenorganisatie voldoende representatief is, kan uit verschillende gegevens worden afgeleid. Een vastomlijnde invulling van dit begrip is niet gegeven, omdat dit tekort zou doen aan andere gegevens die er ook op kunnen wijzen dat een belangenorganisatie representatief is.

875. Zo kan gekeken worden naar de vraag in hoeverre de Gedupeerden de organisatie zelf als representatief ervaren, expertise en ervaring van de organisatie, de overige werkzaamheden die de organisatie verricht heeft, het aantal aangesloten gedupeerden, de omvang van hun vorderingen ten opzichte van het totaal aantal gedupeerden van een massagebeurtenis en de door hen gevorderde schadevergoeding.[578]

876. Op voorhand moet duidelijk zijn dat de belangenorganisatie kwantitatief gezien voor een voldoende groot deel van de groep getroffen gedupeerden opkomt. Wat genoeg is, verschilt per geval en kan alleen bepaald worden in relatie tot het totaal aantal gedupeerden. Dit kan bijvoorbeeld worden getoetst door middel van het aantal gedupeerden dat zich actief voor de vordering heeft aangemeld.[579]

877. Voldoende is dat nauwkeurig wordt omschreven voor welke groep van personen de belangenorganisatie opkomt.[580] De Stichting komt, ingevolge artikel 3 lid 1 van haar statuten (**Productie 2**), op voor de belangen van:

> *"(...) natuurlijke personen die gebruikmaken van het internet door te surfen op het internet en/of door gebruik te maken van producten en/of diensten die persoonsgegevens in digitale vorm kunnen opslaan, overdragen of verwerken, waardoor jegens die internetgebruikers op enig moment een schending van hun recht op bescherming van hun privacy of hun recht op bescherming van hun persoonsgegevens plaatsvindt of heeft plaatsgevonden, een en ander in de ruimste zin van het woord."*

878. De Stichting komt in deze procedure uitsluitend op voor internetgebruikers in Nederland. De achterban van de Stichting wordt aldus gevormd door (in beginsel) alle natuurlijke personen in Nederland die gebruikmaken van het internet. Uit cijfers van het Centraal Bureau voor de Statistiek blijkt dat in Nederland in 2019 ongeveer 87,6% van Nederlandse personen van 12 jaar of ouder vrijwel dagelijks van het internet gebruik maken.[581] In 2019 had Nederland

[578] *Kamerstukken II* 2003/04, 29414, 3, p. 15.
[579] *Kamerstukken II* 2016/17, 34608, 3, p. 19.
[580] *Kamerstukken II* 2016/17, 34608, 3, p. 19.
[581] https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?fromstatweb.

15.121.956 inwoners van 12 jaar en ouder.[582] 87,6% van dit aantal is 13.246.833 personen. In 2019 had Nederland daarmee circa **13,25 miljoen** inwoners van 12 jaar of ouder die vrijwel dagelijks gebruik maken van het internet.

879. Daarnaast heeft de Stichting de steun van toonaangevende belangenorganisatie in Nederland, zoals de stichting Bits of Freedom,[583] de stichting Privacy First,[584] Freedom Internet B.V.[585] en Qiy Foundation.[586] Deze belangenorganisaties komen op voor de belangen en rechten van internetgebruikers in Nederland.

880. Zo zet de stichting Bits of Freedom zich al jarenlang in voor een betere bescherming van persoonsgegevens van internetgebruikers in Nederland. Bits of Freedom was onder andere actief betrokken bij de totstandkoming van de AVG.[587] Op 29 mei 2019 heeft zij een handhavingsverzoek ingediend bij de Nederlandse Autoriteit Persoonsgegevens in het kader van een stelselmatige schending van de AVG en inbreuk op de rechten van Nederlanders in de RTB markt.

881. De stichting Privacy First stelt zich ten doel het behoud en de bevordering van het recht op privacy. Zij doet dit door lobbywerk, juridische acties en rechtszaken, informatieverstrekking en campagnes voor het grote publiek.

882. De Freedom community (Freedom B.V.) maakt zich sterk voor een vrij, open en toegankelijk internet. Zij is in 2019 opgericht door oud XS4ALL-medewerkers en combineert haar technische expertise met een ethische kijk op privacy.

883. Qyi Foundation is een Nederlandse non-profitorganisatie, gericht op het geven van controle aan consumenten over hun eigen (persoons)gegevens. Qyi Foundation heeft een afsprakenstelsel ontwikkeld dat zorgt voor toegang tot, het beheren van en het delen van de eigen gegevens door consumenten. De Stichting heeft niet stilgezeten en diverse werkzaamheden verricht (randnummer 870) waaruit ook volgt dat zij opkomt voor de belangen van de Gedupeerden.

884. De Stichting zal hierna ook toelichten dat zij over voldoende expertise en ervaring beschikt om de belangen van de Gedupeerden te behartigen. Ook hieruit volgt dat de Stichting voldoende representatief is om de belangen van de Gedupeerden te behartigen.

*8.4.2 (ii) De eisen van art. 3:305a lid 2 sub a tot en met e BW*

8.4.2.1 Inleiding

885. Ingevolge het nieuwe art. 3:305a lid 2 sub a tot en met e BW zijn de belangen van de personen ten behoeve van wie de rechtsvordering is ingesteld, voldoende gewaarborgd indien de rechtspersoon:

[582] https://opendata.cbs.nl/statline/?dl=1EFBB#/CBS/nl/dataset/7461bev/table.
[583] https://www.bitsoffreedom.nl.
[584] https://www.privacyfirst.nl.
[585] https://www.freedom.nl/.
[586] https://www.qiyfoundation.org/
[587] Voor een overzicht van de activiteiten van Bits of Freedom zie: https://www.bitsoffreedom.nl/dossiers/europese-privacyregels/.

a. beschikt over een toezichthoudend orgaan;

b. passende en doeltreffende mechanismen biedt voor de deelname aan of vertegenwoordiging bij de besluitvorming van de personen tot bescherming van wier belangen de rechtsvordering strekt;

c. over voldoende middelen beschikt om de kosten voor het instellen van een rechtsvordering te dragen;

d. over een algemeen toegankelijke internetpagina beschikt met daarop:

- de statuten
- de bestuursstructuur
- de laatst vastgestelde jaarlijkse verantwoording op hoofdlijnen van het toezichthoudend orgaan over het door haar uitgevoerde toezicht
- het laatste vastgestelde bestuursverslag
- de bezoldiging van bestuurders en leden van het toezichthoudend orgaan
- de doelstellingen en werkwijzen van de rechtspersoon
- een overzicht van de stand van zaken in lopende procedures en indien een bijdrage wordt gevraagd van personen tot bescherming van wier belangen de rechtsvordering strekt
- inzicht in de berekening van die bijdrage en een overzicht van de wijze waarop personen tot bescherming van wier belangen de rechtsvordering strekt zich kunnen aansluiten bij de rechtspersoon en de wijze waarop zij deze aansluiting kunnen beëindigen.

e. beschikt over voldoende ervaring en deskundigheid ten aanzien van het instellen en voeren van de rechtsvordering.

886. Twee centrale vragen zijn hiervoor van belang:[588] (i) in hoeverre hebben de Gedupeerden uiteindelijk baat bij de collectieve actie indien het gevorderde wordt toegewezen? en (ii): in hoeverre mag erop worden vertrouwd dat de belangenorganisatie over voldoende kennis en vaardigheden beschikt om de procedure te voeren?

887. De Stichting is zo georganiseerd dat de Gedupeerden daadwerkelijk baat zullen hebben bij de onderhavige actie. De Stichting vraagt geen vergoeding aan de Gedupeerden. Indien de vorderingen van de Stichting worden toegewezen, draagt de Stichting enkel een vergoeding aan de Financier af, omdat de Financier de onderhavige procedure financiert.[589] Daarnaast heeft de Stichting er ook voor gezorgd dat zij voldoende kennis en vaardigheden in huis heeft om de procedure te kunnen voeren.[590] Dat zal de Stichting hieronder nader toelichten.

[588] *Kamerstukken II* 2011/12, 33 126, 3, p. 12-13.
[589] Zie over de financiële middelen van de Stichting paragraaf 8.4.2.4 en over de externe financiering pararagraaf 8.4.3, Principe III. Externe Financiering.
[590] *Kamerstukken II* 2011/12, 33 126, 3.

8.4.2.2 Samenstelling van bestuur en Raad van Toezicht

888. De Stichting heeft door middel van een zorgvuldig selectieproces zeer deskundige personen aan zich verbonden. De Stichting is verheugd dat zij kan steunen op de volgende personen.

Bestuur

889. Het bestuur bestaat uit de volgende drie bestuursleden: de heer Hugo Hollander, de heer Joris van Hoboken en mevrouw Annelies van der Ploeg.

890. De heer Hugo Hollander is de voorzitter van het bestuur. De heer Hollander is registeraccountant en partner van zijn eigen maatschappelijk accountantskantoor Share Impact Accountants. Tot 2016 was hij audit partner bij EY en naast algemeen accountant tevens verantwoordelijk voor de duurzaamheidsaccountants. Daarnaast is hij actief als commissaris en toezichthouder bij diverse maatschappelijke organisaties. Hij is tevens jurylid van de duurzaamheidsprijs van de Koning Willem I stichting. Verder is hij co-auteur van een tweetal management boeken: Leidraad voor inspirerend leiderschap (2014) en Duurzaamheid is Passé (2017).[591]

891. De heer Van Hoboken (algemeen lid) is hoogleraar aan de Vrije Universiteit Brussel en universitair hoofddocent aan het instituut voor informatierecht (IViR) aan de Faculteit Rechtsgeleerdheid van de Universiteit van Amsterdam. De heer Van Hoboken werkt op het snijvlak van bescherming van grondrechten (gegevensprivacy, vrijheid van meningsuiting, non-discriminatie) en de regulering van platformen en internetdiensten en is een specialist in Europese gegevensbescherming, algoritmische regulering en regulering van online tussenpersonen. De heer Van Hoboken is jarenlang voorzitter geweest van het bestuur van Bits of Freedom.[592]

892. Mevrouw Van der Ploeg (algemeen lid) is advocaat op het gebied van (commerciële) geschilbeslechting en als partner verbonden aan het kantoor BarentsKrans te Den Haag.[593]

893. Het bestuur bestaat dus uit deskundige personen die beschikken over de specifieke ervaring en de financiële en juridische expertise die nodig is voor de waarborging van de belangen van de achterban van de Stichting.

Raad van Toezicht

894. De Raad van Toezicht bestaat (op dit moment) uit de volgende twee leden: mevrouw Tonkens-Gerkema en mevrouw Toxopeus. Er is ten tijde van dagvaarding een vacature in de Raad van Toezicht, die op korte termijn zal worden ingevuld.

895. Mevrouw Tonkens-Gerkema is de voormalig vice-president en rechter van de rechtbank Amsterdam. Zij heeft na haar pensionering nog enkele jaren als raadsheer-plaatsvervanger bij het Gerechtshof Amsterdam gefungeerd. Zij is commissielid van de Commissie die in 2019 een herziene versie van Nederlandse Claimcode heeft opgesteld en heeft aldus ruime expertise op het gebied van collectieve acties. Zij is tevens lid van de Raad van Toezicht van de stichting

[591] https://theprivacycollective.nl/over-ons/.
[592] https://theprivacycollective.nl/over-ons/.
[593] https://theprivacycollective.nl/over-ons/.

OCA (Onderzoek Collectieve Acties) en de Elco Foundation. Zij was van 2001 tot 2008 Voorzitter van de Nederlandse Vereniging voor Rechtspraak. Zij is nog werkzaam als onafhankelijk arbiter. Zij is ook voorzitter van het Comité van het Nederlands Arbitrage Instituut dat beslist over verzoeken tot wraking van NAI-arbiters.[594]

896. Mevrouw Toxopeus is een professional met meer dan twintig jaar aan ervaring, opgedaan binnen zowel het accountancydomein als de advocatuur. Zij is sinds 2012 verbonden als partner aan Hermes-Advisory. Zij geldt als een expert in het uitvoeren en managen van fraudeonderzoeken, waarbij ze zich toelegt op het berekenen van vermogensschade en het geven van ondersteuning in juridische geschillen. In haar vroege loopbaan werkte mevrouw Toxopeus bij PwC, waar ze zich in 1998 aansloot bij de internationale controlepraktijk van het Big Four-kantoor. Later was ze bij PwC werkzaam binnen de forensische tak, waar haar focus onder andere lag op het doorvoeren van fraudeonderzoek. Volgend op haar tijd bij PwC heeft mevrouw Toxopeus ook ruim vijf jaar gewerkt bij advocatenkantoor NautaDutilh, waar ze was aangesteld als Advisor Corporate Litigation. Sinds 2014 is ze als docent en programmamanager verbonden aan de Erasmus School of Accounting & Assurance, waar ze onder meer de FFD-opleiding ('Financieel Forensisch Deskundige') mede heeft vormgegeven. Mevrouw Toxopeus zal bij BDO, vanuit haar nieuwe rol als partner, leidinggeven aan de Forensics & Litigation Support-praktijk, onderdeel van Risk Advisory Services.[595] Mevrouw Toxopeus is voorgedragen door de Financier.

897. Ook de Raad van Toezicht bestaat dus uit deskundige personen. De Raad van Toezicht beschikt (reeds thans, zelfs nu er een vacature bestaat) over de specifieke ervaring en de financiële en juridische expertise die nodig is voor de waarborging van de belangen van de achterban van de Stichting. Met de Raad van Toezicht beschikt de Stichting over intern toezicht op het bestuur en voldoet zij aldus aan artikel 3:305a lid 2, onderdeel a BW.[596]

8.4.2.3 Deelname aan of vertegenwoordiging bij de besluitvorming

898. Artikel 3:305a BW lid 2, onderdeel b BW verplicht een belangenorganisatie die een collectieve actie instelt over doeltreffende en passende mechanismen te beschikken voor de deelname aan of vertegenwoordiging bij de besluitvorming van de personen voor wie de rechtsvordering is ingesteld. Belangenorganisaties zijn vrij om te bepalen op welke manier zij hieraan invulling geven. Wanneer een belangenorganisatie is ingericht overeenkomstig de Claimcode, kan worden aangenomen dat is voldaan aan dit vereiste.[597]

899. De Stichting zal in paragraaf 8.4.3 toelichten dat zij is ingericht overeenkomstig de Claimcode. Daarnaast geldt dat de Stichting Gedupeerden zal raadplegen in het geval zij overweegt een schikking met Oracle en/of Salesforce te steunen. De wijze waarop de Stichting dit precies doet, bepaalt zij aan de hand van de reikwijdte van die schikking en de op dat moment meest geschikte wijze om de Gedupeerden in dit proces te betrekken. Hiermee voldoet de Stichting aan artikel 3:305a BW lid 2, onderdeel b BW.

[594] https://theprivacycollective.nl/over-ons/.
[595] https://theprivacycollective.nl/over-ons/
[596] *Kamerstukken II* 2016/17, 34608, 3, p. 19; Principe VI van de Claimcode 2019.
[597] *Kamerstukken II* 2016/17, 34608, 3, p. 20.

8.4.2.4 Stichting heeft voldoende financiële middelen

900. Artikel 3:305a lid 2, onderdeel c BW geeft de rechter de mogelijkheid om marginaal te toetsen of de rechtspersoon die een collectieve vordering instelt, beschikt over voldoende middelen om de procedure te kunnen voeren, en waarbij bovendien de zeggenschap over de vordering in voldoende mate bij de belangenorganisatie (in overleg met de achterban) moet liggen.[598] Voldoende is dat een rechtspersoon kan aangeven dat hij, op het moment van toetsing, over voldoende middelen beschikt of kan beschikken om de procedure te kunnen voeren. De toetsing is marginaal. Niet nodig is dat de wederpartij inzage in de financieringsovereenkomst krijgt.[599]

901. De Stichting heeft een financieringsovereenkomst (de "**Financieringsovereenkomst**") gesloten met Innsworth Capital Limited (de "**Financier**"). De Financier heeft via aan haar gelieerde (project)vennootschappen ruime ervaring met het financieren van class actions en massaschadezaken. Van die ervaring kan de Stichting gebruik maken.

902. In de Financieringsovereenkomst wordt door de Stichting en de Financier onderkend dat de Gedupeerden in deze zaak zekerheid dienen te hebben over de financiering van de onderhavige procedure. De Financier heeft dan ook ruimschoots voldoende middelen aan de Stichting ter beschikking gesteld om de procedure in eerste aanleg te kunnen voeren. Hiermee wordt dan ook voldaan aan het vereiste van artikel 3:305a lid 2, onderdeel c BW.

903. De Stichting zal bij de bespreking van Principe III van de Claimcode de externe financiering in meer detail toelichten.

8.4.2.5 De Stichting heeft een toegankelijke website

904. De Stichting onderhoudt een website, https://theprivacycollective.nl, waarop informatie te vinden is en zal zijn, zoals de statuten van de Stichting, de bestuursstructuur van de Stichting, de laatst vastgestelde jaarlijkse verantwoording op hoofdlijnen van het toezichthoudend orgaan over het door haar uitgevoerde toezicht, het laatst vastgestelde bestuursverslag, de bezoldiging van bestuurders en de leden van de Raad van Toezicht, de doelstellingen en werkwijzen van de Stichting, zodra relevant een overzicht van de stand van zaken in lopende procedures en een overzicht van de wijze waarop personen tot bescherming van wier belangen de rechtsvordering strekt zich kunnen aansluiten bij de rechtspersoon en de wijze waarop zij deze aansluiting kunnen beëindigen.

905. Daarnaast onderhoudt de Stichting (mede) een overkoepelende campagnewebsite: https://theprivacycollective.eu/nl/ (randnummer 870). Op deze campagnewebsite is aanvullende informatie te vinden over haar activiteiten. Ook zijn diverse artikelen en onderzoeken gepubliceerd op de campagnewebsite.

906. Hiermee voldoet de Stichting dus ook aan de voorwaarden genoemd in art. 3:305a lid 2 onderdeel d BW.

[598] *Kamerstukken II* 2016/17, 34608, 3, p. 11-12, 20.
[599] HR 20 december 2002, ECLI:NL:PHR:2002:AE3350 (*Lightning Casino/Antillen*); *Kamerstukken II* 2017/18, 34608, 6, p. 11-12.

8.4.2.6 Ervaring en deskundigheid

907. De Stichting beschikt over de expertise en deskundigheid die noodzakelijk is voor het instellen van deze collectieve actie procedure. Zij heeft deze expertise inhouse, doordat haar bestuursleden en leden van de Raad van Toezicht over de vereiste expertise en deskundigheid beschikken, zoals hiervoor in paragraaf 8.4.2.2 nader toegelicht. Zij hebben ruime ervaring op het gebied van collectieve acties, juridische ervaring en expertise op het gebied van gegevensbescherming en bescherming van grondrechten, kennis en kunde van digitale commercie en de benodigde financiële expertise en ervaring.

908. Daarnaast maakt de Stichting gebruik van externe specialisten die onderzoek doen naar de praktijken van Oracle en Salesforce en de technieken waar zij zich van bedienen. De specialisten zijn onder meer gespecialiseerd in technisch onderzoek naar privacy aspecten bij het gebruik van onder meer cookies en vergelijkbare technieken.

909. Ook wordt de Stichting gesteund door de belangenorganisaties Bits of Freedom, Privacy First, Freedom Internet B.V. en Qiy Foundation (randnummer 870). Deze organisaties hebben jarenlange ervaring en expertise op dit terrein.

*8.4.3 Stichting voldoet aan eisen van de Claimcode*

910. Hiervoor heeft de Stichting uiteengezet dat de belangen van de Gedupeerden waarvoor zij opkomt voldoende zijn gewaarborgd. Dit wordt versterkt doordat de Stichting zich niet alleen richt op de eisen van de wetgever, die een aantal eisen uit de Claimcode heeft gecodificeerd, maar zich ook heeft laten inspireren door de overige eisen uit de Claimcode. De Stichting zal hierna aan de hand van de indeling van de Claimcode 2019 en de corresponderende wetsbepalingen toelichten op welke wijze zij de betrokken voorwaarden, dan wel richtlijnen heeft ingepast in haar structuur en governance.

Principe I. – Naleving en handhaving van de code

911. Het bestuur en de Raad van Toezicht van de Stichting zijn verantwoordelijk voor naleving van de Claimcode en de governancestructuur. Zij leggen hierover verantwoording af doordat zij op de website van de Stichting, https://theprivacycollective.nl haar governance in hoofdlijnen heeft uitgewerkt. Op de website heeft zij een Claimcode document gepubliceerd (**Productie 31**). In het document licht de Stichting toe in hoeverre zij de in de Claimcode opgenomen bepalingen opvolgt en zo niet, waarom en in hoeverre zij daarvan afwijkt.[600] De informatie blijft op de website staan zolang de Stichting actief is. Aldus voldoet de Stichting aan Principe I, uitwerking 1.

912. In artikel 17 lid 3 van de statuten van de Stichting is opgenomen dat elke voorgenomen wijziging in de governancestructuur van de Stichting en in de naleving van de Claimcode onder een afzonderlijk agendapunt ter bespreking wordt voorgelegd aan de Raad van Toezicht van de Stichting. Dit is in overeenstemming met Principe I, uitwerking 3.

[600] Zie ook art. 17 van de statuten van de Stichting.

Principe II. – Stichting heeft geen winstoogmerk

913. De Stichting is niet opgericht om geld te verdienen. Dit heeft ook zijn weerslag gekregen op de organisatie van de Stichting. Uit de doelstelling van de Stichting blijkt dat zij geen winstoogmerk heeft.[601] Geen enkele bestuurder, lid van de Raad van Toezicht of de Financier kan beschikken over gelden van de Stichting, anders dan ter uitvoering van het budget van de Stichting (art. 3 lid 4 van de statuten). Daarnaast geldt dat de Stichting geen vergoeding vraagt aan de Gedupeerden, hetgeen het risico van oneigenlijk gebruik van de gelden van de Stichting ook aanzienlijk beperkt.

914. De Stichting heeft ervoor gekozen om de onderhavige procedure te laten financieren door de Financier. Deze streeft wél winst na op zijn financiering. Een gevolg daarvan is dat de Stichting binnen zekere grenzen rekening zal moeten houden met de belangen van de Financier. Daar staat dan weer het voordeel voor de Gedupeerden tegenover dat zij de procedure niet hoeven te voorfinancieren en geen proceskostenrisico dragen en dat gebruik kan worden gemaakt van de expertise en middelen van de Financier. Een redelijke vergoeding voor vreemd vermogen is op grond van uitwerking 2 bij Principe II géén verboden winstoogmerk van de Stichting en is derhalve in overeenstemming met de Claimcode.

915. Tenslotte bepaalt artikel 21 lid 3 van de statuten dat indien het bestuur besluit tot ontbinding tevens de bestemming van het liquidatiesaldo wordt vastgesteld. Deze bestemming moet zoveel mogelijk in overeenstemming zijn met het doel van de Stichting en ten goede komen aan de achterban van de Stichting of aan een algemeen nut beogende instelling met een soortgelijk doel als de Stichting. Het besluit tot ontbinding en de daarvan deel uitmakende bestemming van het liquidatiesaldo behoeft de voorafgaande schriftelijke goedkeuring van de Raad van Toezicht. In andere gevallen van ontbinding wordt de bestemming van het liquidatiesaldo door de vereffenaars vastgesteld. Hiermee wordt voldaan aan uitwerking 3 bij Principe II.

Principe III. – Externe financiering

916. Het bestuur van de Stichting heeft onderzoek gedaan naar de kapitalisatie, het trackrecord en de reputatie van de Financier. In dat verband heeft zij desgevraagd nadere toelichting en toezeggingen van de Financier en haar oprichters gekregen. Hierbij heeft de Stichting zich laten adviseren en ondersteunen door haar eigen advocaten. Ten aanzien van de onderhavige procedure heeft de Stichting een budget afgestemd met de Financier, die uit hoofde van die afspraak verplicht is tot nakoming.

917. In artikel 18 van de statuten heeft de Stichting opgenomen dat zij zich ervan vergewist dat individuele bestuursleden en leden van de Raad van toezicht, alsmede de door de Stichting ingeschakelde advocaat of andere dienstverleners zelfstandig en onafhankelijk zijn van de Financier, alsmede dat de Financier onafhankelijk is van de wederpartij in de collectieve actie. In dit artikel is tevens opgenomen dat de Financieringsovereenkomst voorziet in een dergelijke regeling. Tenslotte is opgenomen dat het bestuur erop toe ziet dat de financieringsvoorwaarden (waaronder begrepen de omvang en systematiek van de overeen te

[601] Zie art. 3 van de statuten van de Stichting (**Productie 2**).

komen vergoeding) redelijkerwijs niet strijdig zijn met het collectieve belang van de Gedupeerden.

918. De uitwerkingen van principe III van de Claimcode hebben de volgende plek gekregen binnen de Financieringsovereenkomst:

a. Uitwerking 2: De Financieringsovereenkomst is schriftelijk aangegaan en bevat een rechtskeuze voor Nederlands recht en een forumkeuze voor de Nederlandse rechter.

b. Uitwerking 3: De zeggenschap over de proces- en schikkingsstrategie berust uitsluitend bij de Stichting. Wél hebben de Stichting en de Financier afspraken gemaakt over de consultatie van de Financier en doorlopende verstrekking van informatie.

c. Uitwerking 4: De Stichting heeft in de opdrachtbevestigingen van haar advocaten laten vastleggen dat de advocaten uitsluitend zullen optreden voor en ten behoeve van de Stichting. De advocaten nemen zo lang zij werkzaam voor de Stichting zijn geen opdrachten aan van de Financier.

d. Uitwerking 5: De Financieringsovereenkomst voorziet in een passende regeling omtrent het delen van informatie met de Financier van de aan de belangenorganisatie toebehorende informatie. In deze regeling is afgebakend tot welke informatie de Financier toegang heeft.

e. Uitwerking 6: In de Financieringsovereenkomst is financiering geregeld die de Stichting in staat stelt als exclusieve belangenbehartiger de gehele eerste aanleg te betalen.

f. Uitwerking 7: De website van de Stichting vermeldt dat sprake is van een Financier, (ii) de identiteit en woonplaats van de Financier en (iii) de systematiek op hoofdlijnen van de met de Financier overeengekomen vergoeding(en) en overeengekomen diensten. Ook is het percentage van de vergoeding die toekomt aan de Financier vermeld:

*"De Stichting wordt gefinancierd door Innsworth Capital Limited, een procesfinancier, gevestigd in Jersey. Afhankelijk van de mate van succes zal de commissie van de procesfinancier worden gedifferentieerd op 25%, 15% en 10% van de toegekende vergoeding. Het percentage neemt dus af naarmate de omvang van de te behalen vergoeding groter wordt. De uiteindelijke vergoeding zal redelijk en adequaat zijn gelet op de risico's die door de procesfinancier worden gedragen. Voor de Gedupeerden staat daar tegenover dat zij zich kosteloos bij de Stichting kunnen aansluiten en van haar activiteiten kunnen profiteren. De commissie die aan de procesfinancier moet worden betaald, zal het bedrag dat beschikbaar is voor de Gedupeerden verminderen, tenzij de kosten van de Stichting (inclusief de commissie die de procesfinancier heeft bedongen voor de financiering en het procesrisico) zijn inbegrepen in de door Oracle en Salesforce te betalen vergoedingen."*

g. Uitwerking 8: In de Financieringsovereenkomst is opgenomen dat de Stichting bevoegd is nadere informatie aan de rechtbank te verstrekken op basis van een daartoe strekkend bevel. In zoverre de rechtbank hiertoe aanleiding ziet, vraagt de Stichting de rechtbank uitdrukkelijk om inzage te nemen op een wijze waarbij Oracle en Salesforce géén inzage

in deze informatie krijgen. Een dergelijke inzage is niet wenselijk. De toetsing door de rechter dient in de regel slechts marginaal te zijn.[602]

Principe IV. – Onafhankelijkheid en vermijding van belangentegenstelling

919. Het bestuur van de Stichting is zodanig samengesteld dat de leden ten opzichte van elkaar, de Raad van Toezicht, de Financier en de Gedupeerden bij de Stichting, onafhankelijk en kritisch kunnen opereren. Dit is ook opgenomen in art. 4 lid 5 en art. 14 van de statuten van de Stichting.

920. Daarbij dient te worden opgemerkt dat de Financier mevrouw Toxopeus, lid van de Raad van Toezicht, heeft benoemd als haar vertegenwoordiger. De Stichting heeft dit ook op haar website gepubliceerd. De benoeming van mevrouw Toxopeus door de Financier wordt uitdrukkelijk toegestaan door Principe VII, uitwerking 3.

921. De Stichting is met geen van de bestuurders of de leden van de Raad van Toezicht een overeenkomst aangegaan, behoudens de aanstellingsbrieven die de voorwaarden voor de uitoefening van hun taken ten behoeve van de Stichting bevatten.

Principe V. – De samenstelling, taak en werkwijze van het bestuur

922. Het bestuur van de Stichting is evenwichtig samengesteld. Het bestuur bestaat uit de heer Hugo Hollander, de heer Joris van Hoboken en mevrouw Annelies van der Ploeg. Zoals hiervoor al uiteen is gezet in paragraaf 8.4.2.2 “Samenstelling van Bestuur en Raad van Toezicht” beschikt het bestuur bovendien over onder meer de specifieke ervaring en juridische en financiële expertise die vereist is voor de Stichting om de belangen van de Gedupeerden adequaat te kunnen behartigen.[603] Dit sluit ook aan bij artikel 4 lid 5 van de statuten van de Stichting, waarin is opgenomen dat het bestuur zodanig is samengesteld dat zij beschikt over de specifieke deskundigheid die noodzakelijk is voor een adequate behartiging van de belangen van de Gedupeerden.

923. De bevoegdheid tot vertegenwoordiging komt steeds toe aan twee van de drie bestuurders, zo volgt uit artikel 9 van de statuten (Principe V, uitwerking 5). Alle belangrijke overeenkomsten waarbij de Stichting partij is, zoals bijvoorbeeld de Financieringsovereenkomst zijn door twee bestuurders ondertekend namens de Stichting.

924. Ook legt het bestuur de balans, staat van baten, lasten en begroting ter goedkeuring voor aan de Raad van Toezicht (conform Principe V, uitwerking 6).

925. Het bestuur overlegt regelmatig met leden van de Raad van Toezicht. Dit gebeurt doorgaans via videoconference. Van het overleg worden notulen opgemaakt. De Raad van Toezicht wordt ook op structurele basis geïnformeerd over relevante ontwikkelingen. Mogelijk ingrijpende besluiten legt het bestuur ter goedkeuring voor aan de Raad van Toezicht. Artikel 5 lid 4 van de statuten van de Stichting bevat een opsomming van goedkeuringsplichtige besluiten (conform Principe V, uitwerking 7). Daaruit volgt bijvoorbeeld dat de toestemming van de Raad van Toezicht nodig is voor het sluiten van een schikkingsovereenkomst.

[602] Zie ook *Kamerstukken II* 2017/18, 34608, 6, p. 11-12.
[603] Zie ook art. 4 lid 6 en lid 7 van de statuten van de Stichting.

926. Ook onderhoudt het bestuur een website, https://theprivacycollective.nl, waarop uitgebreide informatie is te vinden (randnummer 870). Hiermee wordt voldaan aan Principe V, uitwerking 8.

Principe VI. – Vergoedingen aan bestuurders

927. Artikel 4 lid 8 van de statuten van de Stichting bepaalt dat de Raad van Toezicht een beloning kan toekennen aan de leden van het bestuur. Dit sluit aan bij Principe VI, uitwerking 1. De bestuurders mogen voor hun werkzaamheden geen vergoeding accepteren van enig ander dan de Stichting of de Raad van Toezicht (artikel 4 lid 9 van de statuten van de Stichting, conform Principe VI, uitwerking 2).

928. Omtrent het beloningsbeleid en de gedane betalingen aan leden van het bestuur zal de Stichting rapporteren in haar jaarverslag (Principe VI, uitwerking 3). De hoofdlijnen van het beloningsbeleid zijn ook terug te vinden op de website van de Stichting, https://theprivacycollective.nl (Principe VI, uitwerking 4).

Principe VII. – de Raad van Toezicht

929. De Raad van Toezicht bestaat uit mevrouw Tonkens-Gerkema en mevrouw Toxopeus. Zoals hiervoor al uiteen is gezet in paragraaf 8.4.2.2 “Samenstelling van Bestuur en Raad van Toezicht” beschikt de Raad van Toezicht bovendien over onder meer de specifieke ervaring en juridische en financiële expertise die vereist is voor de Stichting om de belangen van de Gedupeerden adequaat te kunnen behartigen (Principe VII, uitwerkingen 4 en 5).

930. Mevrouw Toxopeus is door de Financier benoemd als de vertegenwoordiger van de Financier. De Stichting heeft dit ook op haar website gepubliceerd (Principe VII, uitwerking 3).

931. De leden van de Raad van Toezicht zijn onafhankelijk van elkaar, het bestuur en ten aanzien van de door de Stichting behartigde belangen (artikel 10, lid 2 van de statuten en Principe VII, uitwerking 2). De leden van de Raad van Toezicht kunnen onafhankelijk en kritisch opereren (en doen dat ook). De Raad van Toezicht krijgt alle stukken te zien waar zij om vraagt en krijgt tijdig de noodzakelijke stukken en inlichtingen verstrekt (Principe VII, uitwerking 6).

932. De Raad van Toezicht komt regelmatig per jaar bijeen om de strategie en het beleid te bespreken (Principe VII, uitwerking 1).

933. Verder kan de Raad van Toezicht het bestuur opdragen de balans en staat van baten en lasten te doen onderzoeken door een door de Raad van Toezicht aangewezen registeraccountant of andere deskundige (artikel 16 lid 3 van de statuten van de Stichting). Hiermee wordt voldaan aan Principe VII, uitwerking 7.

934. Ook stelt de Raad van Toezicht jaarlijks een document op waarin op hoofdlijnen verantwoording wordt afgelegd over het uitgevoerde toezicht. Dit document wordt ook op de website van de Stichting, https://theprivacycollective.nl, gepubliceerd. Dit volgt ook uit artikel 12 lid 4 van de statuten van de Statuten en is in overeenstemming met Principe VII, uitwerking 8.

935. Tenslotte publiceert de Stichting op haar website de vastgestelde kostenvergoeding en vacatiegeld voor de leden van de Raad van Toezicht (artikel 5 lid 6 k. van de statuten van de Stichting en principe VII, uitwerking 9).

## 8.5 Aanvullende ontvankelijkheidseisen

### *8.5.1 Inleiding*

936. Artikel 3:305a lid 3 BW bevat een aantal aanvullende ontvankelijkheidseisen voor belangenorganisaties. De Stichting zal hierna toelichten dat zij ook aan deze eisen voldoet: het bestuur heeft geen winstoogmerk, de collectieve vorderingen hebben een voldoende nauwe band met de Nederlandse rechtssfeer en de Stichting heeft Oracle en Salesforce uitgenodigd voor overleg, maar de gevoerde gesprekken hebben niet tot het gewenste resultaat geleid.

### *8.5.2 Geen winstoogmerk*

937. Artikel 3:305a lid 3, onderdeel a, bepaalt dat bestuurders betrokken bij de oprichting van een belangenorganisatie en hun opvolgers, geen rechtstreeks of middellijk winstoogmerk mogen hebben, dat via de belangenorganisatie wordt verwezenlijkt.

938. De Stichting heeft geen winstoogmerk (artikel 3 lid 3 van de statuten). Ook haar bestuurders hebben geen winstoogmerk. Bij de bespreking van Principe II van de Claimcode heeft de Stichting toegelicht dat haar bestuursleden, leden van de Raad van Toezicht en de Financier niet kunnen beschikken over gelden van de Stichting, anders dan ter uitvoering van het budget van de Stichting (artikel 3 lid 4 van de Statuten).

939. In artikel 21 lid 3 van de statuten is tevens bepaald dat op verantwoorde wijze met een batig liquidatiesaldo wordt omgegaan.[604]

### *8.5.3 Voldoende nauwe band met de Nederlandse rechtssfeer*

940. Ingevolge artikel 3:305a lid 3 sub b BW dient de collectieve vordering een voldoende nauwe band met de Nederlandse rechtssfeer te hebben. De Stichting dient genoegzaam aannemelijk te maken dat:

(i) het merendeel van de personen tot bescherming van wier belangen de rechtsvorderingen strekken, hun gewone verblijfplaats in Nederland hebben; of

(ii) degene tegen wie de rechtsvordering zich richt, woonplaats in Nederland heeft en bijkomende omstandigheden wijzen op voldoende verbondenheid met de Nederlandse rechtssfeer; of

(iii) de gebeurtenis of de gebeurtenissen waarop de rechtsvordering betrekking heeft, in Nederland heeft of hebben plaatsgevonden.

[604] Zie ook par. 915 hiervoor: Principe II. – Stichting heeft geen winstoogmerk; *Kamerstukken II* 2016/17, 34608, 3, p. 21.

941. Ad (i): de Stichting komt in deze procedure op voor Nederlandse internetgebruikers die hun gewone verblijfplaats in Nederland hebben. De achterban kan haar steun uitspreken voor deze procedure middels de campagnewebsite.[605]

942. Ad (ii): Oracle Nederland B.V. (gedaagde sub 1) en SFDC Netherlands B.V. (gedaagde sub 2) zijn vestigingen in de zin van de AVG van Oracle en Salesforce, en zijn gevestigd in Nederland. Het feit dat Oracle Corporation (gedaagde sub 3), Oracle America Inc. (gedaagde sub 4) en Salesforce.com, Inc (gedaagde sub 5) gevestigd zijn in Amerika doet niet af aan de ontvankelijkheid van de Stichting ten aanzien van deze partijen. Daarnaast hebben de schendingen van de privacyrechten en de inbreuken op de persoonsgegevens zich voorgedaan in Nederland.

943. Ad (iii): dit vereiste verwijst naar de plaats waar daadwerkelijk de gebeurtenissen zich hebben voorgedaan. Het is geen verwijzing naar de plaats waar de directe schade is geleden.[606] De schending van de privacyrechten en de inbreuken op de persoonsgegevens van Nederlandse internetgebruikers, de Gedupeerden, hebben zich in Nederland voorgedaan.

944. Uit het voorgaande volgt dat de collectieve vorderingen in onderhavige procedure een voldoende nauwe band hebben met de Nederlandse rechtssfeer.

*8.5.4 Stichting heeft Oracle en Salesforce uitgenodigd voor overleg*

945. Per aangetekende brief van 3 juni 2020 heeft de Stichting zowel Oracle (**Productie 3**) als Salesforce (**Productie 4**) aansprakelijk gesteld voor de door haar achterban geleden schade als gevolg van de inbreuken op het recht op bescherming van privacy en het recht op bescherming van persoonsgegevens. De Stichting heeft Oracle en Salesforce daarbij uitgenodigd om in overleg te treden met de Stichting over het toekennen van een redelijke vergoeding voor de door haar achterban geleden schade.

946. Met Oracle is overlegd op 7 juli 2020. Het overleg heeft er niet toe geleid dat partijen nader tot elkaar zijn gekomen.

947. Met Salesforce heeft overleg plaatsgevonden op 3 juli 2020. Ook dat overleg heeft niet geleid tot een oplossing.

948. De Stichting heeft dus ook voldaan aan het overlegvereiste van artikel 3:305a lid 3 sub c BW.

**8.6 Conclusie**

949. Aan de vereisten van artikel 3:305a BW voor het instellen van een collectieve actie is zonder meer voldaan.

[605] Zie hiervoor: paragraaf 6.2.
[606] *Kamerstukken II* 2016/17, 34608, 3, p. 28.

# 9 RECHTSMACHT EN TOEPASSELIJK RECHT

## 9.1 Rechtsmacht

950. De rechtbank heeft rechtsmacht met betrekking tot het voorliggende geschil om de volgende redenen.

*9.1.1 Primair: 79 lid 2 GDPR*

951. De AVG bevat een eigen bevoegdheidsregeling in Artikel 79. Het tweede lid luidt:

> *"Een procedure tegen een verwerkingsverantwoordelijke of een verwerker wordt ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke of de verwerker een vestiging heeft. Een dergelijke procedure kan ook worden ingesteld bij de gerechten van de lidstaat waar de betrokkene gewoonlijk verblijft, tenzij de verwerkingsverantwoordelijke of de verwerker een overheidsinstantie van een lidstaat is die optreedt in de uitoefening van het overheidsgezag."*

952. De Nederlandse rechter is dus bevoegd indien de verwerkingsverantwoordelijke of de verwerker waartegen de vordering wordt ingesteld een vestiging heeft in Nederland, *of* de betrokkene zijn gewone verblijfplaats heeft in Nederland.

953. Overweging 145 AVG verduidelijkt dat de klager zelf mag kiezen waar hij de zaak aanhangig maakt:

> *"Voor procedures tegen een verwerkingsverantwoordelijke of een verwerker dient de klager te kunnen kiezen om de zaak aanhangig te maken bij de gerechten in de lidstaat waar de verwerkingsverantwoordelijke of de verwerker een vestiging heeft, of dit te doen in de lidstaat waar de betrokkene verblijft, tenzij de verwerkingsverantwoordelijke een overheidsinstantie van een lidstaat is die krachtens overheidsbevoegdheid handelt."*

954. Zoals in paragraaf 6.2 toegelicht, heeft het merendeel van de personen tot bescherming van wier belangen de rechtsvorderingen strekken, hun gewone verblijfplaats in Nederland. De Stichting richt zich in deze zaak op betrokkenen waarvan er circa 10 miljoen hun gewone verblijfplaats hebben in Nederland (zie randnummer 878).

955. Het voorgaande betekent dat de rechtbank op grond van artikel 79 lid 2 rechtsmacht heeft met betrekking tot dit geschil.

*9.1.2 Subsidiair: artikel 2 jo. artikel 7 Wetboek van Burgerlijke Rechtsvordering*

956. De Nederlandse rechter heeft in deze zaak rechtsmacht en de rechtbank is relatief bevoegd om kennis te nemen van de vorderingen tegen alle gedaagden. Dit vloeit voort uit artikel 7 van het Wetboek van Burgerlijke Rechtsvordering ("**Rv**") in samenhang met de regels van Nederlands commuun internationaal bevoegdheidsrecht, te weten de artikelen 1-13 Rv.

957. Nu Oracle Nederland B.V. en SFDC Netherlands B.V. gevestigd zijn in Nederland, geldt dat de rechtbank rechtsmacht heeft jegens Oracle Nederland B.V. en SFDC Netherlands B.V. op grond van de in artikel 2 Rv opgenomen hoofdregel.

958. Salesforce.com Inc., Oracle Corporation en Oracle America, Inc. zijn gevestigd in Amerika. Derhalve draagt de zaak ten aanzien van deze gedaagden een internationaal karakter. De Verordening (EU) Nr. 1215/2012 van het Europees Parlement en de Raad betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken (hierna: "**Brussel I bis-Vo**") is niet van toepassing ten aanzien van deze gedaagden nu zij geen woonplaats hebben op het grondgebied van een lidstaat van de Europese Unie. Ook andere internationale regelingen op het gebied van de rechterlijke bevoegdheid missen in de onderhavige zaak toepassing. Dat betekent dat de internationale bevoegdheid van de rechtbank ten aanzien van deze gedaagden eveneens beoordeeld dient te worden aan de hand van de artikelen 1-13 Rv.

959. Op grond van artikel 7 Rv komt de rechtbank ook rechtsmacht toe ten aanzien van deze gedaagden. Tussen de ingestelde vorderingen jegens deze gedaagden en de Nederlandse gedaagden, Oracle Nederland B.V. en SFDC Netherlands B.V. bestaat een zodanige samenhang dat redenen van doelmatigheid een gezamenlijke behandeling rechtvaardigen. Bovendien moet vermeden worden dat bij afzonderlijke behandeling en berechting van de zaken onverenigbare beslissingen worden gegeven.

### 9.2 Toepasselijk recht

960. Op de handelingen van Oracle en Salesforce zijn de AVG (zie paragraaf 4.4.1) en de Tw (zie paragraaf 4.4.2) van toepassing.

961. Nu zowel de Stichting als Oracle Nederland B.V. en SFDC Netherlands B.V. gevestigd zijn in Nederland, is Nederlands recht van toepassing op de vorderingen van de Stichting tegen deze gedaagden.

962. Op de vorderingen jegens de Amerikaanse gedaagden, Salesforce.com Inc., Oracle Corporation en Oracle America, Inc. is ook Nederlands recht van toepassing.

963. De vorderingen jegens deze gedaagden houden geen verband met een verbintenis uit overeenkomst, maar met een niet-contractuele verbintenis, een onrechtmatige daad of een species daarvan. Dit betekent dat in beginsel de EU-verordening nr. 864/2007, betreffende het recht dat van toepassing is op niet-contractuele verbintenissen (hierna: "**Rome II-Verordening**"), in aanmerking komt voor toepassing.

964. Een aantal van de vorderingen hangt echter deels samen met onderwerpen die van het materiële toepassingsgebied van de Rome II-Verordening zijn uitgesloten. Zo zijn niet-contractuele verbintenissen die voortvloeien uit een inbreuk op de persoonlijke levenssfeer of op de persoonlijkheidsrechten, waaronder begrepen smaad uitgesloten (artikel 1, lid 2, sub g van de Rome II-Verordening).[607]

965. In dat geval is de Rome II-Verordening niet van toepassing, tenzij de verordening op grond van artikel 10:159 BW van overeenkomstige toepassing is op de verbintenissen die in beginsel buiten de werkingssfeer van de verordening vallen.[608] Op grond van artikel 10:159 BW is de Rome II-Verordening van overeenkomstige toepassing op de vorderingen jegens

[607] Asser/Kramer & Verhagen, 10-III, 2015/984.
[608] Asser/Kramer & Verhagen, 10-III, 2015/975.

Salesforce.com Inc., Oracle Corporation en Oracle America, Inc. die in beginsel van het toepassingsbereik uitgezonderd zouden zijn. Volgens de hoofdregel, neergelegd in artikel 4 lid 1 van de Rome II-Verordening, is het recht van toepassing van het land waar de schade zich voordoet (lex loci damni), te weten Nederland.[609] Nederlands recht is aldus tevens van toepassing op de vorderingen jegens de Amerikaanse gedaagden.

## 10 BEKENDE VERWEREN EN WEERLEGGING

### 10.1 Verweren Oracle

966. Oracle heeft zich, onder meer bij brief van 18 juni 2020 (**Productie 5**), als volgt verweerd:

a. Oracle beweert dat de argumenten van de Stichting ongegrond zijn, omdat:

i. de Stichting de door Oracle geleverde diensten verkeerd zou begrijpen en haar conclusies zou baseren op onjuiste veronderstellingen of misverstanden over de Oracle-diensten;[610]

ii. de diensten van Oracle niet "cruciaal" zouden zijn voor het RTB-proces;[611]

iii. zij voldoet aan de vereisten in het kader van de AVG en de Tw.[612]

Oracle maakt in haar brief een onderscheid tussen haar DMP dienst en een dienst genaamd “Audience Data Marketplace” (“**ADM**”). Zij beweert dat zij als verwerker moet worden beschouwd voor haar DMP dienst. Volgens Oracle is slechts sprake van “first-party cookies” die door haar klanten worden geplaatst.[613] Oracle zou daarbij niet dicteren of controleren welke informatie haar klanten verzamelen, noch zou zij de door haar klanten verzamelde gegevens voor haar eigen doeleinden gebruiken.[614] Oracle meent dat zij daarom niet hoeft te voldoen aan de AVG-verplichtingen die gelden voor verwerkingsverantwoordelijken.[615] In paragraaf 4.4 is uiteengezet waarom deze bewering van Oracle onjuist is. Het is Oracle die het initiatief neemt tot de gegevensverwerking, de middelen ertoe vaststelt en het grootste commerciële belang erbij heeft. Uit onderzoek blijkt dat Oracle zelf de cookies plaatst (**Productie 16**). Bovendien erkent Oracle zelf in haar privacy documentatie dat zij verwerkingsverantwoordelijke is.

b. Oracle erkent in haar brief dat zij een (onafhankelijke) verwerkingsverantwoordelijke is ten aanzien van de ADM dienst, die zij omschrijft als een “*optional cloud-based third-party data marketplace service offered to DMP customers*”.[616] Het onderscheid dat Oracle tracht te maken tussen haar DMP en de ADM dienst, bestaat echter niet. De ADM dienst is een onlosmakelijk onderdeel van de DMP dienst van Oracle. Dit onderschrijft

[609] Asser/Kramer & Verhagen, 10-III, 2015/977.
[610] Brief Oracle van 18 juni 2020, onder 1 ‘Oracle’s Services in the Netherlands’, p 1.
[611] Brief Oracle van 18 juni 2020, onder 2 ‘Oracle’s DMP and ADM Services are not “crucial” to the RTB Process’, p. 3.
[612] Brief Oracle van 18 juni 2020, onder 3 ‘Oracle complies with the GDPR and DTA with respect to the ADM services’, p. 3.
[613] Brief Oracle van 18 juni 2020, onder 1.a.1 ‘Data Management Platform’, p. 1.
[614] Ibidem.
[615] Brief Oracle van 18 juni 2020, onder 1.a.1 ‘Oracle is a processor for the DMP’, p 2.
[616] Brief Oracle van 18 juni 2020, onder 1.a.2 ‘Audience Data Marketplace’ en ‘Oracle is an independent controller for the ADM’, p. 2.

Oracle zelf ook in haar commerciële documentatie. Zij beschrijft haar DMP op haar website als volgt:

*"Oracle DMP (formerly BlueKai) is the industry's leading cloud-based big data platform that enables marketing organizations to personalize online, offline, and mobile marketing campaigns with richer and more-actionable information about targeted audiences."*[617]

Als de potentiële klant op de website van Oracle op "Request a Consultation" klikt om meer informatie op te vragen over de Oracle DMP, vermeldt Oracle:

*"With the Oracle DMP, marketers will:*

*Access the industry's largest 3rd party data marketplace*

*Gain a holistic view of your customers with 1st and 3rd party data*

*Resolve disparate identities and deliver streamlined experiences*

*With the addition of Oracle OnRamp, extract the full value from your offline customer data with online audiences that deliver superior customer experiences and drive new customer growth"*[618]

Oracle omschrijft ADM hiermee als onlosmakelijk onderdeel van haar DMP dienst. Zij is ook daarom de verwerkingsverantwoordelijke voor de totale DMP dienst, inclusief ADM.

c. Oracle beweert verder dat de Stichting ten onrechte stelt dat Oracle haar DMP dienst combineert met andere diensten, zoals AddThis.[619] Er zou in 2018 besloten zijn de gegevensverzameling van AddThis in Europa te staken. Volgens Oracle zouden de gegevens verzameld met AddThis in gebieden buiten de EU, niet gecombineerd of gebruikt worden voor de ADM dienst in Nederland. Oracle specificeert in haar brief echter niet wanneer in 2018 (vóór of na 25 mei 2018) dit besluit precies genomen is, noch wanneer en in welke mate dit besluit in de praktijk is uitgevoerd. De Stichting neemt aan dat een en ander niet voor 25 mei 2018 zijn beslag heeft gekregen. Voorts is opvallend dat de AddThis knoppen nog wel gebruikt worden en veel Publishers ervan uitgaan dat hiermee ook gegevens verzameld worden. Dit blijkt bijvoorbeeld uit de uitleg over cookies van RTL, die rtlnieuws en buienradar beheert.[620] AddThis staat hier opgenomen in de "lijst van de advertentie- en gedragscookies". De link die hier is opgenomen achter "Oracle AddThis" functioneert niet.

d. Oracle beweert dat de "third-party data" die zij voor de ADM dienst ontvangt van geselecteerde leveranciers van gegevens in de EU, bestaat uit cookiegegevens, bepaalde device identificatoren zoals IP-adressen, en "interest segments".[621] Binnen de EU zou Oracle geen directe identificatoren ontvangen, zoals voornaam, achternaam, e-

[617] https://www.oracle.com/data-cloud/products/data-management-platform/, geraadpleegd op 23 april 2020.
[618] https://go.oracle.com/LP=90408, geraadpleegd op 21 juli 2020.
[619] Brief Oracle van 18 juni 2020, onder 1.b 'Incorrect allegations regarding the DMP and ADM services', p. 2.
[620] https://privacy.rtl.nl/uitleg-over-cookies
[621] Brief Oracle van 18 juni 2020, onder 1.b 'Incorrect allegations regarding the DMP and ADM services', p. 2.

mailadres, postadres of telefoonnummer. Zelfs als Oracle alleen de hiervoor genoemde gegevens zou verwerken, hetgeen de Stichting betwist, dan nog is sprake van de verwerking van persoonsgegevens waarvoor toestemming nodig is. Immers ook cookiegegevens, device identificatoren, IP adressen en "interest segments" kwalificeren als persoonsgegevens in de zin van de AVG (zie paragraaf 4.3.1) en Oracle kan zich niet beroepen op een andere grondslag (zie paragraaf 4.6.2.1). Oracle beweert verder dat het de datasets niet verzamelt, verwerkt of verrijkt met offline gegevens van betrokkenen binnen de EU. Dat is moeilijk te begrijpen, nu Oracle in haar Nederlandse privacy documentatie vermeldt dat zij zowel offline als online informatie verzamelt over betrokkenen, met inbegrip van informatie die afkomstig is van openbaar beschikbare bronnen of externe gegevensleveranciers (zie paragraaf 3.2.4). In haar privacy documentatie staat bovendien dat de offline informatie over betrokkenen maximaal 5 jaar bewaard blijft als deze in de EU/EER is verzameld.

e. In dit verband beweert Oracle dat het een "robust due diligence program" heeft ingericht voor leveranciers van gegevens.[622] Daarmee zou Oracle zorgvuldig controleren of deze partijen wel aan de AVG voldoen. Uit haar eigen informatie volgt echter dat ShareThis één van de leveranciers is die door de selectie is gekomen.[623] Zoals blijkt uit onderzoek is ShareThis een partij die op intransparante wijze op grote schaal gegevens verzamelt (zie onder meer randnummers 422 e.v.). Het is onmogelijk om daar toereikende toestemming voor te claimen.[624]

f. Oracle beweert bovendien dat haar DMP-activiteiten voldoen aan de vereisten van toestemming,[625] transparantie[626] en dataminimalisatie.[627] In paragraaf 4.6.1 t/m 4.6.4 is uitvoerig uiteengezet dat dit niet het geval is.

g. In het gesprek dat op 7 juli 2020 heeft plaatsgevonden heeft Oracle verder nog verklaard dat het gepubliceerde artikel van Techcrunch[628] over haar datalek ongefundeerd is, zonder daarbij aan te geven wat er niet klopt aan de in het artikel genoemde feiten.

### 10.2 Verweren Salesforce

967. Salesforce geeft in haar brief van 17 juni 2020 geen inhoudelijk antwoord.[629] Salesforce verklaart alleen dat zij het niet eens is met de conclusie van de Stichting dat Salesforce ten aanzien van haar DMP dienst de AVG en Tw schendt. Salesforce beweert dat deze conclusie gebaseerd zou zijn op een aantal misvattingen en onjuiste aannames ten aanzien van de DMP van Saleforce en de gegevensverwerking in het kader van DMP. Salesforce stelt dat haar DMP niet werkt zoals "de meeste andere DMPs".[630] Het is de Stichting niet duidelijk geworden waarin Salesforce zich dan onderscheidt van andere DMPs.

---

[622] Brief Oracle van 18 juni 2020, onder 3 'Oracle complies with the GDPR and DTA with respect to the ADM services', p. 4.
[623] http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf, geraadpleegd op 23 april 2020.
[624] The Irish Times, *Data from HSE website users 'leaked to commercial actors',* 18 maart 2019, te raadplegen via: https://www.irishtimes.com/business/technology/data-from-hse-website-users-leaked-to-commercial-actors-1.3829547.
[625] Brief Oracle van 18 juni 2020, onder 3.a 'Oracle's ADM service is lawful and based on consent', p. 4.
[626] Brief Oracle van 18 juni 2020, onder 3.b 'Oracle is transparent about its ADM processing activities', p. 5-6.
[627] Brief Oracle van 18 juni 2020, onder 3.c 'Oracle's processing activities are fair, necessary, and proportionate', p. 7.
[628] Techcrunch, *Oracle's BlueKai tracks you across the web. That data spilled online',* 19 juni 2020, te raadplegen via: https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/ (zie **Productie 12**).
[629] Brief van Salesforce van 17 juni 2020.
[630] Brief van Salesforce van 17 juni 2020, p. 2, paragraaf 1.

## 11 PETITUM

**REDENEN WAAROM**

De Stichting de rechtbank verzoekt te oordelen als volgt, voor zover mogelijk uitvoerbaar bij voorraad:

Vordering I: exclusieve belangenbehartiger

I. De Stichting aan te wijzen als exclusieve belangenbehartiger in de zin van artikel 1018e lid 1 BW;

Vordering II: definitie nauw omschreven groep

II. Te bepalen dat onderhavige collectieve actie op de navolgende groep van natuurlijke personen betrekking heeft in de zin van artikel 1018d Rv:

a. De groep van natuurlijke personen die door Oracle Nederland B.V, Oracle Corporation en Oracle America, Inc. (hierna gezamenlijk 'Oracle') is benadeeld (hierna de 'Oracle Groep') en die bestaat uit:

i. alle natuurlijke personen

ii. die een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Telecommunicatiewet in gebruik hebben, of hebben gehad, en

iii. waarop een cookie met de naam '**bku**' geplaatst is of is geweest,

iv. op een moment of gedurende een periode dat zij in Nederland woonden of verbleven, na inwerkingtreding van de AVG in deze zaak; en

b. De groep van natuurlijke personen die door SFDC Nederland B.V. en Salesforce.com, Inc. (hierna gezamenlijk 'Salesforce') is benadeeld (hierna de 'Salesforce Groep') en die bestaat uit:

i. alle natuurlijke personen,

ii. die een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Telecommunicatiewet in gebruik hebben, of hebben gehad, en

iii. waarop een cookie met de naam '**_kuid_**' geplaatst is of is geweest,

iv. op een moment of gedurende een periode dat zij in Nederland woonden of verbleven, na het van toepassing zijn van de AVG in deze zaak.

Vordering III: opt-out mogelijkheid

III. Te bepalen dat:

a. ieder lid van de Oracle Groep en/of Salesforce Groep dat in Nederland woonachtig is of domicilie heeft gedurende een periode van drie maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, de mogelijkheid zal hebben bij schriftelijk bericht aan de griffie

van de rechtbank te laten weten zich van de behartiging van hun belangen in deze collectieve actie te onttrekken; en

b. ieder lid van de Oracle Groep en/of Salesforce Groep dat buiten Nederland woonachtig is of domicilie heeft, gedurende een periode van zes maanden na de aankondiging in de zin van artikel 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, de mogelijkheid zal hebben bij schriftelijk bericht aan de griffie te laten weten in te stemmen met de behartiging van hun belangen in deze collectieve vordering.

Vordering IV: verklaring voor recht aansprakelijkheid

IV. Voor recht te verklaren dat:

a. Oracle en Salesforce, om redenen zoals in het lichaam van deze dagvaarding gesteld in strijd handelen met de in het lichaam van deze dagvaarding bedoelde fundamentele rechten, de AVG en de Telecommunicatiewet, en

b. ieder van Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. en Salesforce.com, Inc., hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, aansprakelijk zijn jegens elk lid van de Oracle Groep en de Salesforce Groep op grond van artikel 82 AVG en/of artikel 6:162 BW, althans artikel 6:212 BW, voor de door ieder van die leden geleden en nog te lijden schade;

althans dat

a. Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc. hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, aansprakelijk zijn jegens elk lid van de Oracle Groep op grond van artikel 82 AVG en/of artikel 6:162 BW althans artikel 6:212 BW, voor de door ieder van die leden geleden en nog te lijden schade, en

b. SFDC Netherlands B.V. en Salesforce.com, Inc., hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, aansprakelijk zijn jegens elk lid van de Salesforce Groep op grond van artikel 82 AVG en/of artikel 6:162 BW, althans artikel 6:212 BW, voor de door ieder van die leden geleden en nog te lijden schade.

Vordering V: veroordeling tot vergoeding van schade ten aanzien van verwerken persoonsgegevens

V. Ieder van Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. en Salesforce.com, Inc., hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, te veroordelen de (immateriële en materiële) schade te vergoeden, welke schade, al dan niet begroot op basis van artikel 6:104 BW,

a. in totaal voor de gehele Oracle Groep bedraagt **€ 5 miljard**, en voor de gehele Salesforce Groep bedraagt **€ 5 miljard** een en ander te vermeerderen met de

wettelijke rente vanaf de datum van vonnis wijzen, tot aan de dag der algehele voldoening;

Althans

b. **€ 500 per persoon** in de Oracle Groep voor het geval hij of zij een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Telecommunicatiewet in gebruik heeft, of heeft gehad, waarop een cookie met de naam 'bku' geplaatst is of is geweest sinds het van toepassing zijn van de AVG in deze zaak en **€ 500 per persoon** in de Salesforce Groep voor het geval hij of zij een of meer computer(s) met internettoegang of andere randapparatuur in de zin van de Telecommunicatiewet in gebruik heeft, of heeft gehad, waarop een cookie met de naam '_kuid_' geplaatst is of is geweest sinds het van toepassing zijn van de AVG, een en ander te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen, tot aan de dag der algehele voldoening;

Althans

c. Te bepalen dat de door de Oracle Groep en Salesforce Groep geleden en nog te lijden schade uit hoofde van in het lichaam van de dagvaarding gestelde nader zal worden opgemaakt bij staat en zal worden vereffend zoals bij wet voorgeschreven;

Vordering VI: veroordeling tot vergoeding van schade ten aanzien van datalek Oracle

VI. Ieder van Oracle Nederland B.V., Oracle Corporation en Oracle America, Inc. hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, te veroordelen de (immateriële en materiële) schade te vergoeden, al dan niet begroot op basis van artikel 6:104 BW,

a. **€ 100 per persoon** voor elk van de leden van de Oracle Groep en/of Salesforce Groep van wie de gegevens (mogelijk) toegankelijk zijn geweest gedurende de inbreuk op de beveiliging waarover in juni 2020 is bericht als aangegeven in de dagvaarding, te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen, tot aan de dag der algehele voldoening;

Althans

b. Te bepalen dat de door de Oracle Groep en/of Salesforce Groep ter zake geleden en nog te lijden schade uit hoofde van in het lichaam van de dagvaarding gestelde nader zal worden opgemaakt bij staat en zal worden vereffend zoals bij wet voorgeschreven;

Vordering VII/VIII verstrekken van informatie

VII. Dat Oracle en Salesforce opgave zal doen, in de vorm van een Excel lijst of daarmee vergelijkbaar algemeen gangbaar bestand, binnen 4 weken na het in dezen te wijzen vonnis, van:

a. Alle vanuit Nederland bezoekbare websites via welke cookies van Oracle c.q. Salesforce geplaatst zijn, en op welke data en gedurende welke periode(n) zulks het geval is (geweest); en

b. Alle partijen met wie Oracle c.q. Salesforce gegevens op basis van cookie identificatoren hebben uitgewisseld en op welke data en gedurende welke periode(n) zulks het geval is (geweest); en

c. Alle gegevensbronnen die Oracle c.q. Salesforce hebben gebruikt om profielen van leden van de Oracle Groep en/of Salesforce Groep te verrijken en op welke data en gedurende welke periode(n) zulks het geval is (geweest), en

steeds voor zover betrekking hebbend op de periode vanaf van toepassing zijn van de AVG (25 mei 2018) tot en met de datum van betekening van het vonnis in deze zaak,

En

VIII. Dat Oracle opgave zal doen, in de vorm van een Excel lijst of daarmee vergelijkbaar algemeen gangbaar bestand, binnen 4 weken na het in dezen te wijzen vonnis, van het aantal (mogelijk) in Nederland woonachtige of verblijvende personen van wie de gegevens (mogelijk) toegankelijk zijn geweest gedurende de inbreuk op de beveiliging waarover in juni 2020 is bericht als aangegeven in de dagvaarding, alsmede de naam en contactgegevens van deze personen indien en voor zover bekend, althans een zodanige technische voorziening zal treffen dat eenieder zelf gratis en op eenvoudige wijze kan verifiëren of een inbreuk is gemaakt in verband met zijn of haar persoonsgegevens, alsmede van de aard, oorzaak, omvang en duur van de inbreuk en de daarbij gecompromitteerde gegevens;

IX. Onder bepaling dat ieder van Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. en Salesforce.com, Inc. een boete verschuldigd zal zijn indien door Oracle c.q. Salesforce aan enig onderdeel van deze veroordelingen VI en VII niet volledig of niet tijdig zal zijn voldaan, ten bedrage van € 1.000 per tekortkoming, per dag, met een maximum van € 50 miljoen (ieder).

<u>Vordering X: proceskosten en vergoedingen</u>

X. Ieder van Oracle Nederland B.V., Oracle Corporation, Oracle America, Inc., SFDC Netherlands B.V. en Salesforce.com, Inc. hoofdelijk, des dat voor zover de een zal hebben betaald de ander in zoverre zal zijn gekweten, te veroordelen te vergoeden aan de Stichting:

a. De volledige proceskosten van de Stichting op grond van artikel 1018l Rv, althans de daadwerkelijk gemaakte proceskosten op grond van artikel 237 Rv, een en ander te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen, tot aan de dag der algehele voldoening; en

b. De volledig door de Stichting gemaakte (buitengerechtelijke) kosten op grond van artikel 6:96 BW, een en ander te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen, tot aan de dag der algehele voldoening,

Welke bedragen a. en b. gezamenlijk zijn te begroten op € 10 miljoen, althans nader te begroten; en

c. De volledige door de Stichting aan de Financier te betalen overeengekomen vergoeding, op grond van artikel 6:96 BW en artikel 1018l lid 2 Rv, zoals nader te begroten op basis van door de Stichting nader over te leggen informatie;

Vordering XI: wijze van afwikkeling collectieve schade

XI. Te bepalen dat:

a. Oracle en Salesforce aan de Stichting zullen betalen:

i. alle op grond van dit petitum aan de Stichting, de Oracle Groep en Salesforce Groep te betalen bedragen, uitgaande van 10 miljoen leden van de Oracle Groep en/of Salesforce Groep, en te bepalen dat enig deel dat 24 maanden na betaling door Oracle en Salesforce, althans een door Uw rechtbank in goede justitie te bepalen termijn, resteert, door de Stichting zal mogen worden uitgekeerd aan een of meer door de Stichting aan te wijzen organisaties zonder winstoogmerk die actief zijn op het gebied van privacybescherming,

ii. te vermeerderen met een aanvullend bedrag van **€ 15 miljoen** althans een in goede justitie te bepalen bedrag dat zal strekken tot delging van de door de Stichting te maken kosten van verdeling onder de leden Oracle Groep en/of Salesforce Groep van de schadevergoeding (hierna: 'Aanvullend Bedrag'), onder bepaling dat indien en voor zover enig deel zal resteren van het Aanvullend Bedrag nadat de verdeling onder de leden van de Oracle Groep en Salesforce Groep zal zijn voltooid en alle daarmee samenhangende kosten van de Stichting zullen zijn gedelgd, aan Oracle en Salesforce binnen 30 dagen zal worden terugbetaald; en

b. De Stichting een te goeder naam en faam bekend staande professionele claimafhandelaar zal inhuren en opdracht geven de juiste verdeling van de door Oracle en Salesforce te betalen schadevergoedingen onder de leden van de Oracle Groep en Salesforce Groep te verzorgen, en

c. Dat de leden van de Oracle Groep en Salesforce Groep die in aanmerking wensen te komen voor een uitkering dienen in te stemmen met een bindend advies procedure, waarbij een door de rechtbank na overleg met partijen als bindend adviseur zal worden aangewezen, zoals nader door de Stichting te bepalen en door Uw rechtbank goed te keuren;

Althans

d. de collectieve schadeafwikkeling zodanig vorm te geven als Uw rechtbank geraden zal achten op basis van de door de Stichting en Oracle en Salesforce op grond van artikel 1018i Rv over te leggen voorstellen voor een collectieve schadeafwikkeling;

De kosten dezes zijn € 100,89

Deze zaak wordt behandeld door
mr. Chr. A. Alberdingk Thijm, mr. F.M. Peters, mr. S.C. van Schaik, mr. M. Krekels
bureau Brandeis
Sophialaan 8, 1075 BR Amsterdam
T: 020 7606 505 / F: 020 7 606 555
info@bureaubrandeis.com / bureaubrandeis.com

bB

**PRODUCTIEOVERZICHT**

| | |
|---|---|
| **Productie 1** | Information Commisioner's Office, "Update report into adtech and real time bidding" van 20 juni 2019 – een onderzoek van de Britse privacytoezichthouder naar de RTB markt. |
| **Productie 2** | Akte van oprichting, inclusief statuten van Stichting The Privacy Collective van 29 mei 2020. |
| **Productie 3** | Sommatiebrief van 3 juni 2020 aan Oracle. |
| **Productie 4** | Sommatiebrief van 3 juni 2020 aan Salesforce. |
| **Productie 5** | Antwoordbrief Oracle van 18 juni 2020. |
| **Productie 6** | Antwoordbrief Salesforce van 17 juni 2020. |
| **Productie 7** | Webpagina's van Oracle over haar DMP dienst. |
| **Productie 8** | Webpagina's van Salesforce over haar DMP dienst. |
| **Productie 9** | Voorbeeld van een door Oracle's domein bluekai.com geplaatste bku cookie die op verschillende websites hetzelfde Cookie ID toont waarmee de internetgebruiker gevolgd wordt. |
| **Productie 10** | Voorbeeld van een door Salesforce' domein krxd.net geplaatste _kuid_ cookie die op verschillende websites hetzelfde Cookie ID toont waarmee de internetgebruiker gevolgd wordt. |
| **Productie 11** | Nu.nl logboek – overzicht van wat er in enkele seconden op de achtergrond gebeurt wanneer de voorpagina van www.nu.nl wordt geladen. |
| **Productie 12** | Artikel technologiewebsite TechCrunch van 19 juni 2020 over een datalek bij de DMP dienst van Oracle. TechCrunch beschrijft hierin ook de Werking van Oracle's DMP. |
| **Productie 13** | "Create Audience Segments" pagina van de website van Oracle van 22 juli 2020 waarin Oracle uitlegt hoe met de Oracle BlueKai DMP doelgroepen kunnen worden gemaakt met gebruik van onder meer Oracle gegevens en gegevens van derde partijen. |
| **Productie 14** | "Segment Builder Guide" pagina van de website van Salesforce van 22 juli 2020 waarin Salesforce uitlegt hoe met de Salesforce DMP dienst (Audience Studio) doelgroepen kunnen worden gemaakt met o.a. Salesforce gegevens en gegevens van derde partijen. |
| **Productie 15** | "Oracle Marketing Cloud Teams with Eyeota to Enhance Global Data Offering", nieuwsbericht van 19 januari 2017 op de website van Oracle waarin zij onder meer beschrijft dat Oracle's BlueKai Marketplace (onderdeel van DMP) meer dan 30.000 |

datapunten bevat van meer dan 2 miljard consumenten, verkregen via meer dan 1500 gegevenspartners.

**Productie 16** Onderzoeksrapport van Dr. Bashir van 12 augustus 2020 naar de aanwezigheid van Oracle en Salesforce technologie op populaire Nederlandse websites. Dr. Bashir concludeert onder meer dat op 41 van 100 geselecteerde populaire Nederlandse websites technologie van Oracle en Salesforce wordt gebruikt en dat beide partijen met tientallen andere partijen doen aan cookie syncing.

**Productie 17** Revelante onderdelen van de Oracle 2019 Data Directory waarin de gegevenspartners van Oracle staan beschreven. In verband met de grote omvang van het document worden alleen de pagina's overgelegd die zien op gegevenspartners die aldus Oracle in de EU beschikbaar zijn.

**Productie 18** Overzicht van in Nederland populaire websites waarop cookies van Oracle en/of Salesforce zijn aangetroffen met o.a. informatie over de wijze van informatieverstrekking en toestemmingsmechanisme.

**Productie 19** Webpagina's van Oracle waaruit onder meer volgt dat Oracle haar DMP dienst mede richt op de Nederlandse markt.

**Productie 20** Webpagina's van Salesforce waaruit onder meer volgt dat Salesforce haar DMP dienst mede richt op de Nederlandse markt en nieuwsbericht van 24 september 2018 waarin verschillende grote (mede) op Nederland gerichte mediabedrijven aangeven gebruik te maken van de Salesforce DMP.

**Productie 21** Overzicht van gegevens die Oracle naar eigen zeggen verwerkt over een Nederlandse internetgebruiker, waaronder 11 pagina's aan verschillende gegevenssegmenten die Oracle over deze persoon verwerkt.

**Productie 22** Privacydocumentatie van Oracle (gedeelte):

**a** Privacybeleid voor Oracle Data Cloud (Nederlandstalig)

**b** Oracle AddThis Privacy Policy (Engelstalig)

**c** Oracle Data Cloud Privacy Policy (Engelstalig), versie na 11 juni 2020

**d** Oracle Data Cloud Privacy Policy (Engelstalig), versie tot 11 juni 2020

**Productie 23** Privacydocumentatie van Salesforce (gedeelte):

**a** Nederlandse overzichtspagina privacy documentatie Salesforce: https://www.salesforce.com/nl/company/privacy/

**b** Salesforce Algemene privacyverklaring (Nederlandstalig)

**c** Engelse overzichtspagina privacy documentatie Salesforce: https://www.salesforce.com/eu/company/privacy/

**d** Salesforce Audience Studio Privacy Policy (Engelstalig)

**e** Salesforce Trust and Compliance pagina (Engelstalig): https://trust.salesforce.com/en/trust-and-compliance-documentation/audience-studio-and-data-studio/

**f** Audience Studio Notices and License Information (Engelstalig)

**Productie 24** Oracle Online Data Agreement v120119 en Data Processing Agreement versie 26 juni 2019.

**Productie 25** Salesforce Data Processing Addendum, versie juli 2020.

**Productie 26** Uittreksel van de Kamer van Koophandel van Oracle Nederland B.V. van 24 juni 2020.

**Productie 27** Uittreksel van de Kamer van Koophandel van SFDC Netherlands B.V van 20 mei 2020.

**Productie 28** Overzicht van 24-28 juli 2020 van populaire Nederlandse websites die op onjuiste wijze toestemming vragen voor het plaatsen van cookies van Oracle en Salesforce.

**Productie 29** W. Christl, “Corporate surveillance in everyday life – How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions” van juni 2017 – een rapport over de adtech markt waarin onder meer uitleg over DMPs staat en een case study van Oracle.

**Productie 30** Oracle tool waarmee internetgebruikers zichzelf zouden kunnen afmelden en/of hun gegevens laten verwijderen.

**Productie 31** Claim Code Compliance Document van Stichting The Privacy Collective, augustus 2020.