

UITTREKSEL VOOR HET CENTRAAL REGISTER VOOR COLLECTIEVE ACTIES IN DE ZIN VAN ART. 1018C LID 2 RV

van de dagvaarding ex art. 3:305a BW, zoals uitgebracht op 27 maart 2024 door:

de stichting

STICHTING CUIC – PRIVACY FOUNDATION FOR COLLECTIVE REDRESS,

gevestigd in Amsterdam,

eiseres, hierna aangeduid als de “**Stichting**”,

advocaten: mr. J.H. Lemstra, mr. M.N. van Dam en prof. mr. G.J. Zwenne,

tegen:

1. de vennootschap naar het recht van de Tsjechische Republiek **AVAST SOFTWARE S.R.O.**,
gevestigd in Praag;
2. de vennootschap naar het recht van het Verenigd Koninkrijk **AVAST LTD.**,
gevestigd in Londen;
3. de besloten vennootschap met beperkte aansprakelijkheid **AVAST HOLDING B.V.**,
gevestigd in Amsterdam;
4. de besloten vennootschap met beperkte aansprakelijkheid **AVAST SOFTWARE B.V.**,
gevestigd in Amsterdam;
5. de besloten vennootschap met beperkte aansprakelijkheid **AVG ECOMMERCE CY B.V.**,
gevestigd in Amsterdam;

gedaagden, hierna tezamen aangeduid als “**Avast**”,

bij de rechtbank Amsterdam, tegen een eerste roldatum van 31 juli 2024.

1. INTRODUCTIE

- 1.1. Dit is een uittreksel van de dagvaarding die de Stichting op 27 maart 2024 heeft uitgebracht tegen Avast, waarmee een collectieve procedure als bedoeld in art. 3:305a BW is ingeleid.
- 1.2. Met dit uittreksel van de dagvaarding verstrekt de Stichting de vereiste informatie die volgt uit art. 1018c lid 2 Rv (zoals gewijzigd per 25 juni 2023)¹ en die ertoe strekt anderen een goede afweging te laten maken of zij ook een actie voor hetzelfde gebeurtenis tegen Avast willen instellen.

¹ *Kamerstukken II 2021/22, 36034, nr. 3 (MvT), p. 34-35.*



Dit uittreksel beperkt zich tot een beschrijving waartoe de collectieve actie strekt, op welke feiten de Stichting zich daarbij beroept, de namen van de gedaagden en een nauwkeurige omschrijving van de personen tot bescherming van wier belangen deze procedure strekt.

1.3. De opbouw van dit uittreksel is als volgt:

- in paragraaf 2 beschrijft de Stichting welke partijen betrokken zijn bij de procedure en ten behoeve van welke groep personen zij de procedure aanhangig heeft gemaakt;
- in paragraaf 3 wordt de kern van de zaak uiteengezet en wordt duidelijk gemaakt op welke feitelijke stellingen de collectieve actie is gebaseerd;
- in paragraaf 4 licht de Stichting het onrechtmatig handelen van Avast toe en zet zij uiteen welke schendingen van het recht zij heeft vastgesteld;
- in paragraaf 5 licht de Stichting de schade die de Achterban heeft geleden toe; en
- paragraaf 6 bevat het integrale petitum uit de dagvaarding, waaruit blijkt waartoe de collectieve actie strekt.

2. PARTIJEN BIJ DE PROCEDURE

2.1. De Stichting is een onafhankelijke stichting zonder winstoogmerk en is opgericht in 2021 door twee gevestigde organisaties op het gebied van privacybescherming. De Stichting heeft als doel de behartiging van belangen van gedupeerden van privacyschendingen. De Stichting heeft een onafhankelijk bestuur en raad van toezicht, bestaande uit voorvechters en experts op het gebied van privacybescherming en collectieve acties van maatschappelijk belang.

2.2. In deze procedure komt de Stichting op voor (voormalige) gebruikers van diensten en producten van Avast op enig moment in de periode van 1 januari 2014 tot 30 januari 2020 (de "**Relevante Periode**"). De achterban van de Stichting is voor deze procedure beperkt tot personen die consument zijn en dus niet handelden in de uitoefening van een beroep of bedrijf en die ten tijde van het gebruik van deze diensten in Nederland woonden. De Stichting verwijst naar deze groep als de "**Achterban**". De Stichting maakt deze zaak ten behoeve van de Achterban aanhangig.

2.3. De Stichting wordt bijgestaan door (onder meer) ervaren advocaten(kantoren) die gespecialiseerd zijn op het terrein van het collectief actierecht



en het privacyrecht. De Stichting en haar advocaten opereren onafhankelijk van de financier en andere derden.² De Stichting wordt ten behoeve van deze collectieve actie gefinancierd door OmniBridgeway S.A.

- 2.4. De Stichting heeft meermaals vergeefs overleg gezocht met Avast en probeerd het gevorderde zonder gerechtelijke procedure te verkrijgen. Dit heeft niet tot een minnelijke regeling geleid. Om die reden is de Stichting overgegaan tot het uitbrengen van de dagvaarding.
- 2.5. De Stichting heeft de dagvaarding uitgebracht tegen Avast Software s.r.o., Avast Ltd. en de in Nederland gevestigde groepsvennootschappen Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V.

3. KERN VAN DE ZAAK

- 3.1. Avast is een van 's werelds grootste aanbieders van antivirus- en beveiligingssoftware, onder meer onder de namen Avast en AVG. Het ging om antivirussoftware (te downloaden op de PC of door apps voor mobiele apparaten), internetbrowsers en internetbrowserextensies. Deze laatste zijn (beveiligings)invoegtoepassingen voor internetbrowsers.
- 3.2. Avast heeft naar eigen zeggen een omzet (in 2021) van ruim USD 941 miljoen en wereldwijd meer dan 435 miljoen gebruikers. Avast richtte zich ook op de Nederlandse consument. Naar schatting hebben honderdduizenden consumenten in Nederland gebruik gemaakt van deze software om hun computers en persoonlijke data te beveiligen.
- 3.3. Avast heeft op geraffineerde wijze inbreuk gemaakt op de privacyrechten van de Achterban. Terwijl de gebruikers dachten met de software van Avast veiligheid (voor hun privacy) te kopen, bleek de software in werkelijkheid een paard van Troje. Via de software verzamelde Avast op onrechtmatige wijze op grote schaal browsegegevens van haar gebruikers. Avast deelde de verzamelde gegevens buiten het zicht van de gebruikers met haar dochter- c.q. zustervennootschap Jumpshot Inc., gevestigd in de Verenigde Staten. Jumpshot Inc., actief op het gebied van *big data* en *marketing analytics*, stelde die data op commerciële wijze ter beschikking c.q. verkocht die data vervolgens aan honderden derden.
- 3.4. Eind 2019 werd bekend dat Avast zich schuldig maakte aan ongeoorloofde datahandel. Experts op het gebied van technologie hadden onderzoek gedaan naar de werking van de producten van Avast. Avast bleek via de producten heimelijk een grote hoeveelheid zeer gedetailleerde gegevens over het browsegedrag en de gehele browsegeschiedenis van gebruikers te verzamelen en deze gegevens via Jumpshot te gelde te maken. De verzamelde informatie kon gegevens bevatten over welke zoektermen een

² Meer informatie over de Stichting, haar bestuurders, toezichhouders en partners, is te vinden op www.cuic.eu.



gebruiker had gegoogeld en welke websites hij had bezocht, en daarmee over de gebruikers religieuze overtuigingen, gezondheidsproblemen, politieke voorkeuren, locatie, financiële status, bezoeken aan websites gericht op kinderen en interesse in pornosites. Deze informatie was bovendien gekoppeld aan één specifieke gebruiker door middel van een aantal unieke user-ID's.

- 3.5. Avast verzamelde dus veel meer gegevens dan nodig was voor de diensten die zij leverde (de veiligheidscontrole van websites) en veel meer dan waarover zij haar gebruikers had geïnformeerd. Na publicaties over deze onrechtmatige handelwijze heeft Avast de activiteiten van Jumpshot per 30 januari 2020 stopgezet. Jumpshot is op 26 februari 2021 ontbonden.
- 3.6. Avast heeft haar onrechtmatig handelen publiekelijk toegegeven, en toezichthouders in de VS en in Tsjechië hebben het handelen van Avast veroordeeld.
- 3.7. De Amerikaanse federale consumentenautoriteit, de Federal Trade Commission (“**FTC**”), heeft Avast op 22 februari 2024 veroordeeld tot betaling van USD 16,5 miljoen ter compensatie van de (Amerikaanse) gebruikers en haar bevolen te stoppen met het verkopen of aan derden ter beschikking stellen van de verzamelde gegevens, die verzamelde gegevens te verwijderen en een uitgebreid privacyprogramma te implementeren. De voorzitter van de FTC stelde voorop dat browsegegevens per definitie gevoelig zijn en dat de browsegeschiedenis uiterst gevoelige informatie kan bevatten. De voorzitter benadrukte dat Avasts privacyschendingen ernstiger waren dan de schendingen die de FTC normaliter onderzoekt en oordeelde dat Avasts praktijken “bijzonder stuitend” waren. Ook de Tsjechische privacytoezichthouder (UOOU) is in februari 2020 een onderzoek gestart naar het handelen van Avast. Naar aanleiding daarvan heeft de UOOU op 14 maart 2023 geconcludeerd dat Avast Software s.r.o. in strijd heeft gehandeld met onder meer de artikelen 6 lid 1 en 13 lid 1 (c) Avg en in verband daarmee een boete opgelegd van (circa) EUR 13,7 miljoen.
- 3.8. Avast heeft steeds beweerd dat de gegevens die zij via Jumpshot ter beschikking stelde c.q. verkocht, niet herleidbaar waren tot specifieke gebruikers, maar dat is onjuist. In de praktijk werden persoonsgegevens als naam, e-mailadres en huisadres vaak niet verwijderd, waardoor de individuele gebruiker alsnog op vele manieren kan worden geïdentificeerd. Iedere gebruiker had verder een unieke user-ID, waaraan zijn surfgegevens waren gekoppeld. Bovendien beschikten de ontvangers van de gegevens (de klanten van Jumpshot) zelf vaak ook over grote hoeveelheden data van internetgebruikers. Zij konden hun eigen gegevens vergelijken en/of verrijken met de gegevens die zij verkregen van Jumpshot. Zo konden de gebruikers van de software van Avast ook geïdentificeerd worden. Verder kunnen gegevens zoals Avast die via Jumpshot deelde, ook aan individuen



worden gekoppeld met behulp van openbaar beschikbare gegevens, zoals die op sociale media.

- 3.9. De gebruikte methode was dus onvoldoende om de gegevens daadwerkelijk anoniem te maken en daarmee te bewerkstelligen dat de informatie niet meer als persoonsgegevens kon worden beschouwd. Individuele gebruikers bleven identificeerbaar voor Avast, voor Jumpshot en voor de klanten van Jumpshot. Er was dan ook hooguit sprake van pseudonimisering. Het ging aldus nog steeds om persoonsgegevens, zodat op Avast verregaande verplichtingen rustten op grond van de Avg.

4. HET ONRECHTMATIG HANDELEN VAN AVAST

- 4.1. Met haar handelwijze heeft Avast de Europese en Nederlandse gegevensbeschermingswetgeving geschonden (inclusief de cookieregels). Ook is sprake van een oneerlijke handelspraktijk, althans een onrechtmatige daad. Tevens heeft Avast zich ten koste van de Achterban ongerechtvaardigd verrijkt.

- 4.2. Meer specifiek heeft Avast in de Relevante Periode:

- (i) de Achterban niet of onvoldoende geïnformeerd over de verwerking van haar persoonsgegevens. Dit is in strijd met art. 33 en 34 Wbp, art. 12-14 Avg en art. 11.7a lid 1 sub a Tw;
- (ii) persoonsgegevens verzameld voor een ander doel dan het oorspronkelijke verzameldoel, en meer gegevens verzameld dan noodzakelijk voor het doel. Dit is in strijd met art. 9 lid 1, 10 lid 1 en 11 Wbp en art. 5 lid 1 (b, c en e) Avg;
- (iii) persoonsgegevens verwerkt zonder de vereiste toestemming van de Achterban en zonder gerechtvaardigd belang. Dit is in strijd met art. 8 Wbp, art. 6 lid 1 Avg en art. 11.7a lid 1 sub b Tw;
- (iv) in strijd met het verwerkingsverbod, bijzondere categorieën van persoonsgegevens van de Achterban verwerkt. Dit is in strijd met art. 16 Wbp en art. 9 lid 1 Avg;
- (v) de persoonsgegevens van de Achterban doorgegeven aan de VS zonder adequate aanvullende maatregelen. Dit is in strijd met het doorgifteverbod uit art. 76 lid 1 Wbp en art. 44 Avg; en
- (vi) essentiële informatie weggelaten of verborgen in de zin van art. 6:193b BW.

Ad (i): Avast heeft niet voldaan aan de transparantie- en informatieplicht

- 4.3. Avast heeft haar gebruikers op geen enkele wijze geïnformeerd welke persoonsgegevens zij met behulp van haar producten zou verzamelen en voor



welke doeleinden. Avast deed het ten onrechte voorkomen alsof zij alleen die gegevens zou verzamelen die noodzakelijk waren om haar producten en diensten te kunnen aanbieden en/of te verbeteren. Avast heeft haar gebruikers ook niet geïnformeerd dat zij deze gegevens voor commerciële doeleinden zou verstrekken aan Jumpshot, dat Jumpshot deze op haar beurt aan derden ter beschikking zou stellen, noch wie die derden waren.

- 4.4. Avast heeft verder haar gebruikers niet geïnformeerd over de grondslag voor de verwerking en de bewaartermijn die zij hanteerde, noch heeft zij de overige vereiste informatie verstrekt.
- 4.5. Avast had deze informatie in duidelijke en eenvoudige taal, en voor de Nederlandse gebruikers in het Nederlands, moeten verstrekken. Het transparantievereiste geldt te meer voor Avast als leverancier van beveiligingssoftware.
- 4.6. Avast had deze informatie moeten verstrekken *voordat* zij de gegevens verzamelde, dus op het moment dat het betreffende product werd geïnstalleerd of in gebruik genomen. Dat was het moment waarop deze informatie voor de betrokkene het meest relevant was. Dat heeft Avast toen niet gedaan, noch (tardief) op een later moment.
- 4.7. Voor zover Avast haar gebruikers iets heeft gemeld over de verzameling van persoonsgegevens, deed zij dat te laat en op een voor de gemiddelde gebruiker onbegrijpelijke wijze en op een onvindbare, dan wel te moeilijk vindbare plaats, weggestopt in haar Engelstalige Privacy Policy.
- 4.8. Vanaf medio 2018 verwees Avast in de Privacy Policy naar gebruik van gegevens voor vage doelen als *“cross-product direct marketing, cross-product development and third party trend analytics.”* Voor zover gebruikers al konden begrijpen wat deze marketingtermen inhielden, konden zij hieruit hoogstens afleiden dat Avast analysetools van derden kon gebruiken om haar producten en diensten te verbeteren. Dat van doorgifte van de gegevens aan Jumpshot sprake was, en bovendien van terbeschikkingstelling daarvan aan derden, konden de gebruikers uit de aan hen verstrekte informatie redelijkerwijs niet afleiden.
- 4.9. De toelichting op de opt-out-mogelijkheid, voor zover gebruikers die konden vinden, was eveneens onvoldoende. Avast maakte ook daarin niet duidelijk dat zij gegevens over de volledige surfgeschiedenis van de gebruiker verzamelde, noch dat zij deze via Jumpshot te gelde maakte door deze aan derden ter beschikking te stellen c.q. te verkopen. Avast vermeldde als doel slechts dat gegevens met derden werden gedeeld voor *“analytics”*, maar zoals vermeld konden gebruikers daaruit hoogstens afleiden dat Avast analysetools van derden kon gebruiken voor verbetering van haar producten.



- 4.10. Ook de opt-in-mogelijkheid die Avast in juli 2019 aan nieuwe gebruikers gaf, bevatte onjuiste en onvoldoende informatie. Avast bracht daarin gebruikers ervan op de hoogte dat gegevens werden gedeeld met Jumpshot, die deze aan haar klanten “kon” doorgeven. Deze informatie was onjuist, omdat Avast ten onrechte beweerde dat de informatie die zij aan Jumpshot doorgaf niet herleidbaar zou zijn naar individuele gebruikers, terwijl in werkelijkheid ontvangers van de Jumpshot-pakketten wel degelijk gebruikers konden identificeren. Verder bevatte de opt-in-mogelijkheid niet de informatie die (eveneens) in de Privacy Policy ontbrak, zoals welke persoonsgegevens werden verzameld, met welk doel, wie de derden waren en wat de gevolgen voor gebruikers konden zijn. Tot slot was ook deze tekst onvoldoende duidelijk en concreet.

Ad (ii): De verstrekking van gegevens aan Jumpshot was niet verenigbaar met het doel waarvoor de gegevens waren verzameld

- 4.11. Avast informeerde de gebruikers uitsluitend dat zij door het verzamelen van gegevens haar eigen, op de beveiliging gerichte producten en diensten kon aanbieden en verbeteren. Avast vermeldde in de Privacy Policy niet dat de persoonsgegevens ook werden verzameld ten behoeve van Jumpshots commerciële activiteiten en dat deze voor dat doel aan Jumpshot werden verstrekt. Het verstrekken van de persoonsgegevens aan Jumpshot valt niet onder het verzameldoel dat Avast in de Privacy Policy heeft aangeduid.
- 4.12. Gegevens delen met Jumpshot, die op haar beurt deze gegevens aan derden ter beschikking stelde c.q. verkocht, betreft dus een ‘verdere verwerking’. Daarvan moet worden beoordeeld of deze verenigbaar was met het verzameldoel. Dat is niet het geval:
- Er is geen sprake van verwantschap tussen enerzijds het oorspronkelijke verzameldoel en anderzijds het nieuwe doel. Het verzameldoel was immers gebruikers beschermen en waarschuwen voor onveilige websites. De terbeschikkingstelling c.q. verkoop van gegevens (via Jumpshot) aan online marketing- en analysediensten is op geen enkele manier te rijmen met het verzameldoel. Sterker nog: deze staat haaks op het eigenlijke doel. De gegevensverstrekking aan Jumpshot vloeit niet logisch voort uit en houdt geen verband met waarschuwen van gebruikers voor onveilige websites.
 - De gebruikers waren er niet mee bekend dat hun gegevens (ook) werden verzameld ten behoeve van Jumpshot en konden dit redelijkerwijs ook niet verwachten.
 - Aangenomen moet worden dat Jumpshot als gevolg van de gegevensverstrekking de beschikking kreeg over bijzondere persoonsgegevens als bedoeld in art. 16 Wbp en art. 9 lid 1 Avg.



- De verdere verwerking houdt in dat gebruikers (tot op heden) geen enkele controle hebben over de context waarin de gegevens kunnen worden gebruikt. Dit kan zeer serieuze gevolgen hebben. Het is aannemelijk dat Jumpshot zelf of haar afnemers de gegevens gebruikt hebben om gebruikers te segmenteren of te profileren. Dat kan zeer ongewenste en zelfs discriminatoire gevolgen hebben.
 - De gegevens werden heimelijk verkregen en verstrekt aan Jumpshot. Van transparantie was dus geen sprake. Pas nadat het ongeoorloofde gedrag van Avast in 2019 in de publiciteit was gekomen, dus nadat al heel veel gegevens waren verstrekt, is Avast begonnen met een (ontoereikende) poging haar gebruikers (alsnog) om de vereiste toestemming te vragen.
- 4.13. Daarmee is duidelijk dat het verzamelen van gegevens door Avast met de bedoeling deze te verstrekken aan Jumpshot, niet in overeenstemming was met het doelbindingsbeginsel.
- 4.14. Ook heeft Avast in strijd gehandeld met het gegevensminimalisatievereiste. Avast verzamelde de gegevens met het doel om de gebruikers te waarschuwen voor onveilige en onbetrouwbare websites. Voor dit verzameldoel waren slechts bepaalde gegevens nodig (zoals gegevens over het apparaat van de gebruiker en internetadressen). Avast heeft echter ook de hele surfgeschiedenis van de gebruiker verzameld en bewaard. Verder was het voor dit verzameldoel niet nodig om gegevens ter beschikking te stellen c.q. te verstrekken aan Jumpshot. Het verzamelen van onnodige gegevens en de gegevensverstrekking aan Jumpshot waren dus niet toereikend, niet ter zake dienend en niet beperkt tot wat noodzakelijk was voor het verzameldoel.
- 4.15. Het beginsel van gegevensminimalisatie brengt ook met zich dat gegevens niet langer worden bewaard dan strikt noodzakelijk voor het verzameldoel. Avast heeft in strijd met het verzameldoel en zonder dat gebruikers dat wisten, informatie gedeeld met derden. Daarmee is Avast per definitie tekortgeschoten in haar verplichtingen dat gegevens niet langer worden bewaard dan nodig voor het doel waarvoor deze zijn verzameld (art. 10 lid 1 Wbp en art. 5 lid 1 (e) Avg). De derden bleven immers beschikken over de gegevens, ook als dit voor de door Avast aangeboden op beveiliging gerichte producten en diensten niet langer noodzakelijk was.
- Ad (iii): Avast heeft persoonsgegevens verwerkt zonder de vereiste toestemming van de Achterban en zonder gerechtvaardigd belang***
- 4.16. Tot juli 2019 hebben gebruikers helemaal geen toestemming gegeven. Avast heeft pas vanaf juli 2019 aan nieuwe gebruikers een opt-in-mogelijkheid aangeboden voor de verstrekking van persoonsgegevens aan, en



verwerking door, Jumpshot. Daarvóór hanteerde Avast een opt-out-systeem, waarbij gebruikers werden geacht geen bezwaar te hebben tegen de gegevensverwerkingen, tenzij zij actief aangaven dat dat anders was. Het opt-out-systeem leverde per definitie geen rechtsgeldige toestemming van gebruikers op. Avast mocht er niet vanuit gaan dat gebruikers geen bezwaar hadden zo lang zij niets deden. Dat kan immers niet worden beschouwd als een (actieve) wilsuiging.

- 4.17. De opt-in die in juli 2019 werd ingevoerd was bovendien volstrekt ontoereikend, gelet op de vereisten voor rechtsgeldige toestemming:
- De opt-in bevatte alleen de informatie dat de gegevens van de gebruikers met Jumpshot konden worden gedeeld, maar niet de overige informatie die Avast ook had moeten verstrekken.
 - De gevraagde toestemming was onvoldoende specifiek. Avast deed het ten onrechte voorkomen alsof alleen geanonimiseerde gegevens aan Jumpshot konden worden verstrekt. Ook maakte Avast niet duidelijk wat voor soort marketing- en analysediensten zij op basis van de gegevens ontwikkelde en wat dat kon betekenen voor gebruikers, mede gelet op het detailniveau van die diensten die Jumpshot naar eigen zeggen aan haar klanten leverde.
 - In het opt-in-scherm verwees Avast naar andere documenten, zoals een “Consent Policy”, maar maakte niet duidelijk wat daarin stond. Avast voldeed daarmee niet aan het ondubbelzinnigheidsvereiste.
 - Het opt-in-scherm bevatte een standaard aangevinkt selectievakje (met daarin “I AGREE”) dat de gebruiker moest uitzetten als hij geen toestemming wenste te geven. Toestemming die op die manier wordt gegeven is ook volgens het HvJ EU geen ondubbelzinnige actieve handeling en was en is daarom niet rechtsgeldig.
 - Ten slotte was het intrekken van de toestemming niet even gemakkelijk als het geven daarvan. Zo blijkt uit de vage bewoordingen in de Privacy Policy dat voor het intrekken van toestemming actief contact moest worden gezocht met Avast, maar hoe de gebruiker dat moest doen, bleef onduidelijk.
- 4.18. Avast beschikte dus niet over toereikende en rechtsgeldige toestemming, zelfs niet toen zij naar eigen zeggen haar gebruikers een opt-in aanbod.
- 4.19. Voor zover Avast zich op het standpunt stelt dat zij een beroep kan doen op de verwerkingsgrondslag ‘gerechtvaardigd belang’, is zij daarmee te laat. Avast had haar gebruikers immers voorafgaand aan de verwerking van de gegevens moeten informeren over de grondslag(en) daarvoor, maar dat heeft zij niet gedaan.



- 4.20. Zelfs als dat anders zou zijn, had Avast geen gerechtvaardigd belang. Avast stelde in de Privacy Policy dat de verzamelde persoonsgegevens noodzakelijk waren voor het functioneren van haar producten en (in de laatste versie van de Privacy Policy) dat deze gegevens vervolgens in gepseudonimiseerde en geanonimiseerde vorm werden verwerkt voor “*cross-product marketing, cross-product development and third party trend analytics*” en dat dit gebeurde in het belang van de gebruiker. Afgezien van het feit dat Avast zich bediende van vage omschrijvingen en daarbij essentiële informatie weglief, is duidelijk geworden dat de persoonsgegevens werden verwerkt ten behoeve van het zuiver commerciële belang van Avast bij het aanbieden van haar beveiligingsdiensten. Ook het onderliggende (heimelijke) doel, namelijk de terbeschikkingstelling c.q. verkoop van waardevolle informatieproducten gebaseerd op het surfgedrag van haar gebruikers, is (hooguit) een zuiver commercieel belang. Uitgaand van de normuitleg van de AP is dit geen gerechtvaardigd belang.
- 4.21. Er bestond ook geen noodzaak om de gegevens te verwerken. Voor het aanbieden van antivirus- en antimalware-diensten is het aantoonbaar niet nodig om zoveel persoonsgegevens, waaronder bijzondere persoonsgegevens, te verzamelen als Avast indertijd deed. Er bestonden en bestaan verschillende alternatieve, minder vergaande werkwijzen.
- 4.22. Tot slot zijn de belangen van de gebruikers onevenredig aangetast, als wordt gekeken naar de relevante factoren:
- Avast verzamelde gegevens op zeer grote schaal. De heimelijke gegevensverzameling door Avast heeft jarenlang voortgeduurd, zodat Avast waarschijnlijk van vele gebruikers hun volledige surfgeschiedenis over al die jaren heeft verzameld.
 - De gebruikers wisten niet dat deze persoonsgegevens werden verzameld en ook niet dat de gegevens werden verstrekt aan Jumpshot. De gebruikers hadden zich juist tot Avast gewend als antivirus- en antimalware-dienstverlener om hun privacybelangen te *beschermen*. Dat uitgerekend Avast heimelijk gegevens verzamelde voor commerciële doeleinden, viel buiten elke redelijke verwachting. Avast heeft ten onrechte geen rekening gehouden met de redelijke verwachtingen van de betrokkenen.
 - De gevolgen van het onrechtmatig handelen van Avast voor de gebruikers kunnen ernstig en ingrijpend zijn. Marketing- en analyse-tools leggen immers op een individueel niveau interesses, voorkeuren en overtuigingen bloot. Als zodanig moeten deze tools worden gezien als middelen waarmee invloed kan worden uitgeoefend op de gebruikers. Voorts kan het verlies van controle over persoonlijke informatie leiden tot gevoelens van irritatie, angst en stress, en tot zelfcensuur, bij de gebruikers.



- Avast verwerkte gedetailleerde gegevens over de volledige browsergeschiedenis van haar gebruikers, waaronder bijzondere persoonsgegevens. Daarmee werd inzicht verkregen in het gedrag en de mentale gesteldheid van de betreffende persoon gedurende een langere periode. Onder de gebruikers waren ook extra kwetsbare groepen als minderjarigen.

4.23. Een en ander brengt met zich mee dat de commerciële belangen van Avast niet kunnen prevaleren boven de gerechtvaardigde belangen van gebruikers bij de wettelijk geregelde bescherming van hun (bijzondere) persoonsgegevens en hun persoonlijke levenssfeer.

Ad (iv): Avast heeft bijzondere persoonsgegevens verwerkt in strijd met het verwerkingsverbod

4.24. Nu Avast de integrale browsergeschiedenis van gebruikers verzamelde, heeft Avast per definitie ook bijzondere persoonsgegevens verwerkt met behulp van haar producten. Als gebruikers bijvoorbeeld informatie willen opzoeken over een bepaalde chronische ziekte, zullen zij dat in het algemeen via internet doen. Ook kon Avast via de bezochte website vaststellen dat de gebruiker met een zekere frequentie bepaalde producten aanschaftte, zoals medicijnen of medische hulpmiddelen. Hetzelfde geldt voor bezoeken aan websites met politieke, religieuze of seksuele inhoud.

4.25. Avast mocht alleen bijzondere persoonsgegevens verwerken voor zover zij kon en kan aantonen dat gebruikers uitdrukkelijk daarvoor toestemming hadden gegeven en/of voor zover gebruikers de bijzondere gegevens zelf duidelijk openbaar hadden gemaakt, maar dat is niet het geval.

4.26. Avast had voor de gegevensverwerkingen tot juli 2019 helemaal geen toestemming van haar gebruikers gevraagd of verkregen, en vanaf juli 2019 op volstrekt ontoereikende wijze.

4.27. Mensen die gebruik maken van het internet om informatie te zoeken of dingen te regelen doen dat in de veronderstelling dat hun acties privé blijven, althans niet in het openbaar gedeeld worden. Er is dus evident geen sprake van openbaarmaking, laat staan dat de gebruikers de bedoeling hadden hun volledige browsergeschiedenis en andere persoonsgegevens openbaar te maken.

Ad (v): Avast heeft persoonsgegevens doorgegeven aan Jumpshot in strijd met het doorgifteverbod

4.28. Het staat vast dat Avast persoonsgegevens heeft verstrekt aan Jumpshot in de VS. De doorgifte van persoonsgegevens naar derde landen, d.w.z. landen buiten de EU/EER, mag volgens de gegevensbeschermingswetgeving niet ten koste gaan van het beschermingsniveau dat die wetgeving waarborgt. Om deze reden is de doorgifte van persoonsgegevens naar



deze derde landen in beginsel verboden, tenzij op een van de uitzonderingen een geslaagd beroep kan worden gedaan. Dat is hier niet het geval.

- 4.29. Er was in de Relevante Periode geen geldig adequaatheidsbesluit als bedoeld in art. 45 Avg. Twee achtereenvolgende adequaatheidsbesluiten, waarin de Commissie stelde dat de VS een passend beschermingsniveau waarborgde (“Safe Harbor” en “Privacy Shield”) zijn beide ongeldig verklaard door de hoogste Europese rechter, nadat die vaststelde dat het beschermingsniveau van de Amerikaanse wetgeving onvoldoende is. Dit betreft de arresten *Schrems I*³ en *Schrems II*.⁴
- 4.30. Voor zover Avast stelt dat zij persoonsgegevens doorgaf op basis van *standard contractual clauses* als bedoeld in art. 46 Avg, heeft zij in strijd met art. 13 en 14 Avg niet duidelijk gemaakt welke aanvullende maatregelen zij had genomen om te komen tot het vereiste beschermingsniveau. Gelet op het verantwoordingsvereiste van art. 5 lid 2 en 14 lid 1 Avg moet Avast dat kunnen aantonen. Het is daarom aannemelijk dat Avast heeft nagelaten aanvullende maatregelen te nemen. Zelfs als Avast dit wel zou hebben gedaan, geldt dat er geen passende aanvullende maatregel voorhanden was die verhindert dat de Amerikaanse overheid toegang heeft tot de gegevens. Aangezien Jumpshot de gegevens aan derden ter beschikking stelde c.q. verkocht, kan het niet anders dan dat Jumpshot de gegevens ofwel onversleuteld ontving, ofwel dat zij deze kon ontsleutelen. Toegang door de Amerikaanse overheid is dan niet verhinderd. Eventuele aanvullende maatregelen waren dan ook niet doeltreffend.
- 4.31. Voor zover de Stichting kan nagaan, heeft Avast geen *binding corporate rules* laten goedkeuren. Als Avast wel gebruik maakte van goedgekeurde *binding corporate rules*, heeft zij nagelaten deze te publiceren.

Ad (vi): De handelwijze van Avast is een oneerlijke handelspraktijk

- 4.32. Avast heeft haar gebruikers niet, althans onvoldoende duidelijk, geïnformeerd over de werking van haar producten. Uit niets blijkt dat Avast via haar producten een grote hoeveelheid persoonsgegevens zou verzamelen en deze aan derden ter beschikking zou stellen c.q. zou verkopen via Jumpshot.
- 4.33. Deze (niet met de consumenten gedeelde) informatie was van essentieel belang voor de gebruikers. Zij zijn zonder deze essentiële informatie overgegaan tot een aankoopbeslissing. Het is aannemelijk dat als de gebruikers dit hadden geweten, vele van hen de producten van Avast niet gebruikt zouden hebben, althans niet onder dezelfde voorwaarden. Hiermee is sprake van een misleidende omissie in de zin van art. 6:193d lid 2, dan wel lid 3, BW. De bewijslast dat dit anders zou zijn rust op Avast.

³

HvJ EU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*).

⁴

HvJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).



Avast heeft zichzelf ongerechtvaardigd verrijkt

- 4.34. Avast heeft zichzelf met haar onrechtmatige handelingen ten koste van de Achterban ongerechtvaardigd verrijkt in de zin van art. 6:212 BW.
- 4.35. Het profiteren van de heimelijk verzamelde persoonsgegevens door Jumpshot is voor Avast bijzonder lucratief geweest. De verrijking van Avast is ongerechtvaardigd. Avast heeft immers met haar handelen en nalaten op grote schaal de gegevensbeschermingswetgeving, inclusief de cookieregels, geschonden en zich tevens schuldig gemaakt aan misleidende handelspraktijken. De verrijking van Avast vloeit rechtstreeks voort uit deze schendingen. Nu er geen rechtvaardigingsgrond aan de verrijking ten grondslag ligt, is deze ongerechtvaardigd.
- 4.36. Door deze schendingen is de Achterban van de Stichting verarmd. De gebruikers van Avast, waaronder de Achterban, verschaften immers zonder dat te weten een grote hoeveelheid persoonsgegevens aan Avast en verloren daarmee de controle over die persoonsgegevens. Het staat vast dat persoonsgegevens (economische) waarde vertegenwoordigen. Dit leverde Avast rechtstreeks profijt op. Er is dus causaal verband tussen de verrijking van Avast en de verarming van de Achterban.

5. DOOR DE ACHTERBAN GELEDEN SCHADE DIENT DOOR AVAST TE WORDEN VERGOED

- 5.1. Het handelen van Avast heeft zowel materiële als immateriële schade tot gevolg gehad aan de zijde van de Achterban. Avast dient de door de Achterban geleden schade te vergoeden.

Materiële schade

- 5.2. Persoonsgegevens zijn geld waard. Avast heeft de Achterban echter niet betaald voor de gegevens. Het oneigenlijke gebruik van de persoonsgegevens van de Achterban heeft Avast in staat gesteld winst te behalen. De Stichting vordert de materiële schade van de Achterban te begroten in overeenstemming met art. 6:104 BW ter hoogte van de winst die Avast met haar onrechtmatig handelen in de Relevante Periode in Nederland heeft gemaakt.

Immateriële schade

- 5.3. Avast heeft moedwillig en onrechtmatig de (bijzondere) persoonsgegevens van de Achterban structureel en langdurig verwerkt en verstrekt aan Jumpshot, die deze aan derden ter beschikking heeft gesteld of verkocht, terwijl de Achterban haar persoonsgegevens met de producten van Avast juist wilde beschermen tegen onrechtmatig gebruik door derden en tegen online risico's in het algemeen, en de producten ook zo door Avast werden aangeprezen. Dit heeft ertoe geleid dat de leden van de Achterban de controle over hun persoonsgegevens zijn verloren. Verlies van controle is in



de Avg expliciet genoemd als een van de soorten schade die kan ontstaan door een privacyschending.

- 5.4. Die terbeschikkingstelling aan Jumpshot en een onbekende hoeveelheid derden heeft zonder twijfel geleid tot profilering en beïnvloeding van het (keuze)gedrag en de waargenomen 'online wereld' van gebruikers, met mogelijk ongewenste en zelfs discriminatoire gevolgen, welke eveneens in de Avg worden genoemd als soorten schade die kunnen ontstaan door een privacyschending.
- 5.5. Bovendien zijn de persoonsgegevens van de Achterban, als gevolg van de doorgifte aan Jumpshot in de VS, blootgesteld aan de wetgeving in de VS die niet een beschermingsniveau biedt dat in essentie gelijkwaardig is aan dat in de EU. In de praktijk betekent dit dat de persoonsgegevens van de Achterban kunnen zijn onderworpen aan surveillance door Amerikaanse overheidsdiensten.
- 5.6. Het is aannemelijk dat de normschending bij de Achterban heeft geleid tot gevoelens van wantrouwen, verontwaardiging en zorgen, en tot zelf-censuur. Dit geldt des te meer nu zij gebruik maakten van de software van Avast om bescherming te genieten, terwijl daarmee in werkelijkheid hun gegevens op straat kwamen te liggen. Ook dit levert immateriële schade op die voor vergoeding in aanmerking komt.
- 5.7. Gelet op de diverse criteria die in de Nederlandse rechtspraak worden meegewogen, is de normschending door Avast dusdanig ingrijpend dat nadelige gevolgen voor de Achterban moeten worden verondersteld.
- 5.8. De Stichting stelt in deze procedure een benadering voor waarbij aan diegenen die door de normschendingen van Avast zijn geraakt, eenzelfde schadebedrag wordt toegekend. Deze benadering, een standaardisering in de vorm van vaststelling van eenzelfde bedrag, is in overeenstemming met de rechtspraak van de Hoge Raad en wordt ook in de literatuur bepleit. Voor zover individuele omstandigheden een 'opslag' op het schadebedrag rechtvaardigen, bijvoorbeeld in situaties waarbij de normschending voor een specifieke persoon tot (nog) verderstreckende gevolgen heeft geleid dan de gevolgen voor het collectief, biedt het systeem van de WAMCA daarvoor een oplossing in de vorm van de opt-out-mogelijkheid van art. 1018f Rv.
- 5.9. De Stichting meent dat een vergoeding van EUR 1.000 per lid van de Achterban, gelet op de relevante omstandigheden en de verschillende aspecten van de normschendingen, redelijk en aangewezen is. Subsidiair vordert de Stichting dat de rechtbank de immateriële schade begroot op EUR 200 per jaar of gedeelte van een jaar in de Relevante Periode dat een lid van de Achterban (een van) de producten van Avast heeft gebruikt.



Hoofdelijke aansprakelijkheid

- 5.10. De verschillende Avast-entiteiten zijn hoofdelijk aansprakelijk voor de door de Achterban geleden schade omdat zij gezamenlijk verwerkingsverantwoordelijk zijn in de zin van art. 1 sub b Wbp en art. 4 sub 7 Avg. De Avast-entiteiten maakten immers deel uit van de Avast-groep en traden op als één bedrijfsvoeringseenheid die wereldwijd één dienst leverde aan betrokkenen, hanteerden één wereldwijd geldend privacybeleid en voerden wijzigingen in beleid, doelen en middelen centraal en wereldwijd door. Deze omstandigheden duiden erop dat de juridische en feitelijke beslissingsmacht met betrekking tot de verwerkingen van de persoonsgegevens ook lag bij Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V., alsmede bij Avast Ltd., zoals de FTC heeft vastgesteld.
- 5.11. De grondslag voor deze collectieve actie is art. 3:305a BW, zoals met ingang van 1 januari 2020 gewijzigd bij de inwerkingtreding van de WAMCA. In dit geval is sprake van een voortdurend nalaten door Avast gedurende de Relevante Periode, althans van een reeks gebeurtenissen die zowel voor als na 15 november 2016 hebben plaatsgevonden, zodat de WAMCA van toepassing is op grond van art. 119a Overgangswet Nieuw Burgerlijk Wetboek.

6. PETITUM

- 6.1. Hieronder is het integrale petitum ingevoegd zoals dat is opgenomen in de dagvaarding.
- 6.2. De Stichting verzoekt de rechtbank bij vonnis, voor zover mogelijk uitvoerbaar bij voorraad:
1. De Stichting aan te wijzen als exclusieve belangenbehartiger zoals bedoeld in art. 1018e Rv.
 2. Te bepalen dat deze collectieve vordering tot bescherming strekt van (voormalige) gebruikers van diensten en producten van Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. op enig moment in de periode van 1 januari 2014 tot 30 januari 2020 (de Relevante Periode), niet handelend in de uitoefening van een beroep of bedrijf, voor zover zij ten tijde van het gebruik van deze diensten in Nederland woonden (de Achterban).
 3. Te bepalen dat, in overeenstemming met art. 1018f lid 1 Rv, ieder lid van de Achterban dat in Nederland woont of domicilie heeft, binnen een maand na de aankondiging ex art. 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, door een schriftelijke mededeling aan de griffie van de rechtbank kan laten



weten zich van de behartiging van zijn belangen in deze collectieve actie te willen bevrijden.

4. Te bepalen dat, in overeenstemming met art. 1018f lid 5 Rv, ieder lid van de Achterban dat niet in Nederland woont of domicilie heeft, binnen een maand na de aankondiging ex art. 1018f lid 3 Rv van de uitspraak tot aanwijzing van de exclusieve belangenbehartiger, door een schriftelijke mededeling aan de griffie van de rechtbank kan laten weten in te stemmen met de behartiging van zijn belangen in deze collectieve actie en dat zijn belang niet wordt behartigd in een collectieve of individuele vordering, gebaseerd op soortgelijke feitelijke en rechtsvragen voor dezelfde gebeurtenis of gebeurtenissen tegen gedaagden in een andere lidstaat van de EU of de EER.
5. Op de gronden uiteengezet in deze dagvaarding te verklaren voor recht dat Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. gezamenlijk en/of ieder voor zich, gedurende de Relevante Periode, jegens de Achterban toerekenbaar onrechtmatig hebben en/of heeft gehandeld en/of ongerechtvaardigd zijn en/of is verrijkt en aansprakelijk zijn en/of is voor de daardoor geleden en te lijden schade van de Achterban.
6. Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. hoofdelijk te veroordelen tot vergoeding van de materiële schade van de Achterban, te begroten in overeenstemming met art. 6:104 BW op het bedrag van de winst die Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. door hun onrechtmatig handelen hebben genoten, per lid van de Achterban te vermeerderen met de wettelijke rente vanaf het moment dat het betreffende lid van de Achterban het (eerste) product van gedaagden in gebruik heeft genomen, althans de datum van deze dagvaarding, althans de datum van vonnis wijzen tot aan de dag der algehele voldoening.
7. Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. hoofdelijk te veroordelen tot vergoeding van de immateriële schade, te begroten op EUR 1.000 per lid van de Achterban, althans (subsidiair) EUR 200 per lid van de Achterban voor elk jaar of gedeelte van een jaar in de Relevante Periode dat hij of zij (een van) de producten van gedaagden heeft gebruikt, althans (meer subsidiair) te bepalen dat deze schade nader zal worden opgemaakt bij staat en zal worden vereffend volgens de wet; en (zowel primair als subsidiair) per lid van de Achterban te vermeerderen met de wettelijke rente vanaf het moment dat het betreffende



lid van de Achterban het (eerste) product van gedaagden in gebruik heeft genomen, althans de datum van deze dagvaarding, althans de datum van vonnis wijzen tot aan de dag der algehele voldoening.

8. Te bepalen dat de collectieve schadeafwikkeling (primair) zal worden vormgegeven op een door de Stichting te bepalen wijze, althans (subsidiar) zoals de rechtbank op basis van door de Stichting en gedaagden op grond van art. 1018i Rv over te leggen voorstellen voor de collectieve schadeafwikkeling in goede justitie geraden acht.
9. Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. te gebieden om binnen vier weken na het in dezen te wijzen vonnis:
 - (i) Alle gegevens van gebruikers die Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. onrechtmatig hebben verzameld, voor zover zij deze nog bewaren, te vernietigen.
 - (ii) Derden (buiten de Avast-groep) die gegevens van gebruikers die gedaagden onrechtmatig hebben verzameld, hebben ontvangen, te informeren dat de gegevensverstrekking onrechtmatig was en dat verder gebruik van de gegevens, waaronder het bewaren ervan, door de derden onrechtmatig is, en deze derden te verzoeken (a) deze gegevens te vernietigen en (b) gedaagden en de Achterban te laten weten aan welke partijen de gegevens nog verder zijn doorgegeven.
 - (iii) Ieder die tot de Achterban kan worden gerekend te informeren over (a) welke gegevens Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. en/of andere entiteiten binnen de Avast-groep over hem of haar hebben verzameld, (b) wanneer en hoe lang dat is gebeurd, (c) met welke (rechts)personen deze gegevens zijn gedeeld en (d) of, en zo ja wanneer, deze gegevens zijn vernietigd.
 - (iv) Een (deel van hun) website in te richten waarmee de Achterban inzage kan krijgen in de informatie bedoeld onder 9 (iii) van het petitum.
 - (v) Een onafhankelijk auditor, zoals Deloitte, E&Y of PwC, toegang te geven tot de IT-faciliteiten van Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. (waaronder, maar niet beperkt tot, externe servers bij aan gedaagden dienstverlenende derden)



en ook overigens alle benodigde medewerking te verlenen om een onafhankelijk onderzoek uit te voeren naar de naleving van de geboden als bedoeld in 9 (i) t/m (iv) van het petitum.

10. Deloitte, E&Y of PwC, of een vergelijkbare door de rechtbank in goede justitie te bepalen partij, te benoemen tot onafhankelijke onderzoekers als bedoeld in 9 (v) van het petitum.
11. Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. hoofdelijk te veroordelen tot vergoeding van redelijke en evenredige proceskosten en overige kosten van deze procedure aan de Stichting, bestaande uit: (a) de volledige proceskosten van de Stichting op grond van art. 1018l lid 2 Rv, althans de daadwerkelijk gemaakte proceskosten op grond van art. 237 Rv, te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen tot aan de dag der algehele voldoening; (b) de (buitengerechtelijke) kosten van de Stichting op grond van art. 6:96 BW, te vermeerderen met de wettelijke rente vanaf de datum van vonnis wijzen tot aan de dag der algehele voldoening; (c) de door de Stichting aan de procesfinancier te betalen overeengekomen vergoeding op grond van art. 6:96 BW en art. 1018l lid 2 Rv; en (d) de volledige kosten voor de schadeafwikkeling, een en ander zoals nader te be-groten.
12. Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V. hoofdelijk te veroordelen tot vergoeding van de door de Stichting gemaakte kosten van dit geding, te vermeerderen met de nakosten ten belope van EUR 178 zonder betekening, dan wel EUR 270 in het geval van betekening, een en ander te voldoen binnen veertien dagen na dagtekening van het vonnis, en – voor het geval voldoening van de (na-)kosten niet binnen de gestelde termijn plaatsvindt – te vermeerderen met de wettelijke rente over de (na-)kosten te rekenen vanaf bedoelde termijn voor voldoening tot aan de dag der algehele voldoening.

Deze zaak wordt behandeld door:
mr. J.H. Lemstra en mr. M.N. van Dam
Lemstra Van der Korst N.V., Postbus 75655, 1070 AR Amsterdam
T 020 2050533, E j.lemstra@lvdk.com

en:
prof. mr. G.J. Zwenne
Pels Rijcken N.V., Postbus 11756, 2502 AT Den Haag
T 071 527 8838, E g.j.zwenne@pelsrijcken.nl