LEMSTRA VAN DER KORST PELS RIJCKEN

EXTRACT FOR THE CENTRAL REGISTER OF COLLECTIVE ACTIONS WITHIN THE MEANING OF ARTICLE 1018C DCCP

of the summons pursuant to article 305a of Book 3 DCC, as issued on 27 March 2024 by:

STICHTING CUIC - PRIVACY FOUNDATION FOR COLLECTIVE REDRESS,
a foundation having its registered office in Amsterdam,
claimant, hereinafter referred to as the "**Foundation**",
represented by: J.H. Lemstra LLM, M.N. van Dam LLM and G.J. Zwenne LLM,

versus:

1. **AVAST SOFTWARE S.R.O.**,
a company incorporated and existing under the law of the Czech Republic, having its registered office in Prague;
2. **AVAST LTD.**,
a company incorporated and existing under the law of the United Kingdom, having its registered office in London;
3. **AVAST HOLDING B.V.**,
a private company with limited liability,
having its registered office in Amsterdam;
4. **AVAST SOFTWARE B.V.**,
a private company with limited liability,
having its registered office in Amsterdam;
5. **AVG ECOMMERCE CY B.V.**,
a private company with limited liability,
having its registered office in Amsterdam;

defendants, hereinafter collectively referred to as "**Avast**",

at the Amsterdam District Court, with effect from a first scheduled date of 31 July 2024.

1. INTRODUCTION

1.1. This is an extract from the summons issued by the Foundation on 27 March 2024 against Avast, whereby a collective action as referred to in article 305a of Book 3 DCC is initiated.

1.2. With this extract from the summons, the Foundation is providing the required information pursuant to article 1018c(2) DCCP (as amended as at 25 June 2023)[1], the purpose of which is to enable others to properly consider whether they also wish to bring an action against Avast regarding

[1] *Parliamentary Papers II* 2021/22, 36034, no. 3, pp. 34-35.

the same event. This extract confines itself to providing a description of the purpose of the collective action, the facts relied on by the Foundation, the names of the defendants and a precise description of the persons whose interests this action seeks to protect.

1.3. This extract is structured as follows:

- in paragraph 2, the Foundation describes which parties are involved in the proceedings and for whose benefit it has brought the proceedings;
- paragraph 3 sets out the essence of the case and clarifies the factual contentions on which the collective action is based;
- in paragraph 4, the Foundation explains Avast's wrongful conduct and sets out the breaches of law it has established;
- in paragraph 5, the Foundation explains the damage suffered by the Members; and
- paragraph 6 contains the full claim for relief of the summons, showing the purpose of the collective action.

2. PARTIES TO THE PROCEEDINGS

2.1. The Foundation is an independent non-profit foundation established in 2021 by two established organizations in the field of privacy protection. The object of the Foundation is to represent the interests of victims of privacy violations. The Foundation has an independent board and supervisory board, consisting of advocates and experts in the field of privacy protection and collective actions of social importance.

2.2. In these proceedings, the Foundation represents (former) users of Avast services and products at any time during the period from 1 January 2014 to 30 January 2020 (the "**Relevant Period**"). For the purposes of these proceedings, the Foundation's constituency is limited to persons who are consumers and therefore were not acting in the exercise of a profession or business and who resided in the Netherlands at the time of the use of these services. The Foundation refers to this group as the "**Members**". The Foundation is bringing this case on behalf of the Members.

2.3. The Foundation is *inter alia* assisted by experienced lawyers or law firms, specializing in the field of collective action law and privacy law. The Foundation and its lawyers operate independently of the funder and other third parties.[2] The Foundation is funded for the purposes of this collective action by OmniBridgeway S.A.

[2] More information about the Foundation, its directors, supervisors and partners, can be found at www.cuic.eu.

2.4. The Foundation unsuccessfully sought consultations with Avast on several occasions and tried to obtain the claimed without legal proceedings. This did not lead to an amicable settlement. For this reason, the Foundation proceeded to issue the writ of summons.

2.5. The Foundation has issued the summons against Avast Software s.r.o., Avast Ltd. and the group companies Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. based in the Netherlands.

3. THE ESSENCE OF THE MATTER

3.1. Avast is one of the world's leading providers of antivirus and security software, including under the names Avast and AVG. It was concerned with antivirus software (downloadable on PC or by apps for mobile devices), internet browsers and internet browser extensions. The latter are (security) add-ons for internet browsers.

3.2. Avast said it had revenues (in 2021) of over USD 941 million and more than 435 million users worldwide. Avast also targeted Dutch consumers. It is estimated that hundreds of thousands of consumers in the Netherlands have used it to secure their computers and personal data.

3.3. Avast cunningly infringed on the privacy rights of the Members. While users thought they were buying security (for their privacy) with Avast's software, in reality the software turned out to be a Trojan horse. Through the software, Avast unlawfully collected its users' browsing data on a large scale. Avast shared the collected data – without the users being aware of this – with its US-based subsidiary, or sister company, as the case may be, Jumpshot Inc. Jumpshot, active in the field of *big data* and *marketing analytics*, made that data commercially available, or subsequently sold it, to hundreds of third parties.

3.4. In late 2019, it was revealed that Avast was guilty of unauthorised data trading. Technology experts had conducted investigations into the operation of Avast's products. Avast tuned out to be secretly collecting a large amount of very detailed data on users' browsing behaviour and their entire browsing history via its products and to sell this data via Jumpshot. The information collected could include data on which search terms a user had googled and which websites he had visited, and thus on the users' religious beliefs, health problems, political preferences, location, financial status, visits to websites aimed at children and interest in porn sites. Moreover, this information was linked to one specific user through a number of unique user IDs.

3.5. Avast thus collected far more data than was necessary for the services it provided (website security monitoring) and far more than it had informed its users about. Following publications about this unlawful conduct, Avast

ceased Jumpshot's operations with effect from 30 January 2020. Jumpshot was dissolved on 26 February 2021.

3.6. Avast has publicly admitted its unlawful actions, and regulators in the US and in the Czech Republic have since condemned Avast's actions.

3.7. The US federal consumer authority, the Federal Trade Commission ("**FTC**"), on 22 February 2024 ordered Avast to pay USD 16.5 million in compensation to the users, or American users, and ordered it to stop selling or making the collected data available to third parties, to delete that collected data and to implement a comprehensive privacy programme. The FTC chairwoman first and foremost stated that browsing data is sensitive by definition and that the browsing history may contain extremely sensitive information. The chairwoman emphasized that Avast's privacy breaches were more serious than those the FTC normally investigates and ruled that Avast's practices were "*especially galling*". The Czech privacy regulator (UOOU) also launched an investigation into Avast's actions in February 2020. As a result, the UOOU concluded on 14 March 2023 that Avast Software s.r.o. had acted in breach of, *inter alia*, articles 6(1) and 13(1)(c) GDPR and imposed a fine of (approximately) EUR 13.7 million in connection therewith.

3.8. Avast has at all times alleged that the data it made available or sold through Jumpshot could not be traced to specific users, but that is incorrect. In practice, personal data such as name, e-mail address and home address were often not removed, so that the individual user could still be identified in many ways. Each user further had a unique user ID, to which his browsing data was linked. Moreover, the recipients of the data (Jumpshot's customers) often had large amounts of internet user data themselves. They could compare and/or enrich their own data with the data they obtained from Jumpshot. Thus, users of Avast's software could also be identified. Furthermore, data such as Avast shared through Jumpshot could also be linked to individuals using publicly available data, such as those on social media.

3.9. Thus, the method used was insufficient to make the data effectively anonymous and thus achieve that the information could no longer be considered personal data. Individual users remained identifiable to Avast, to Jumpshot and to Jumpshot's customers. There was therefore at most pseudonymisation. It was thus still personal data, so that Avast had far-reaching obligations under the GDPR.

4. AVAST'S UNLAWFUL CONDUCT

4.1. With its conduct, Avast violated European and Dutch data protection legislation (including cookie rules). It also constitutes an unfair commercial

practice, or at least an unlawful act. Avast has also unjustly enriched itself at the expense of its users.

4.2. More specifically, in the Relevant Period, Avast:

(i) did not or insufficiently inform the Members about the processing of its personal data. This contravenes articles 33 and 34 of the Personal Data Protection Act ("**Wbp**"), articles 12-14 GDPR and article 11.7a(1)(a) of the Telecommunications Act ("**Tw**");

(ii) collected personal data for a purpose other than the original purpose of collection and collected more data than necessary for the purpose. This violates articles 9(1), 10(1) and 11 Wbp and article 5(1) (b, c and e) GDPR;

(iii) processed personal data without the required consent of the constituency and without legitimate interest. This is in violation of article 8 Wbp, article 6(1) GDPR and article 11.7a(1)(b) Tw;

(iv) in breach of the ban on processing, processed special categories of personal data of the Members. This violates article 16 Wbp and article 9(1) GDPR;

(v) transferred personal data of the Members to the US without appropriate additional safeguards. This violates the transfer prohibition in article 76(1) Wbp and article 44 GDPR; and

(vi) omitted or concealed essential information within the meaning of article 193b of Book 6 DCC.

Re (i): Avast failed to comply with transparency and disclosure obligations

4.3. Avast did not inform its users in any way what personal data it would collect with the help of its products and for what purposes. Avast falsely pretended that it would collect only those data as was necessary to be able to offer and/or improve its products and services. Avast also did not inform its users that it would provide this data to Jumpshot for commercial purposes, that Jumpshot would in turn make it available to third parties, nor who those third parties were.

4.4. Avast furthermore failed to inform its users about the basis for the processing and the period for which the personal data would be stored, nor did it provide the other required information.

4.5. Avast should have provided this information in clear and simple language, and for Dutch users in Dutch. The transparency requirement applies all the more to Avast as a supplier of security software.

4.6. Avast should have provided this information *before* it collected the data, i.e. at the time the product in question was installed or put into use. That

was the time when this information was most relevant to the data subject. Avast did not do so then, nor (out of time) at a later moment.

4.7. To the extent that Avast in any way notified its users of the collection of personal data, it did so too late and in a manner that was incomprehensible to the average user and in a place that could not be found by that user, or with great difficulty only, tucked away in its English-language Privacy Policy.

4.8. From the middle of 2018 onwards, Avast's Privacy Policy referred to use of data for vague purposes such as "*cross-product direct marketing, cross-product development and third-party trend analytics.*" To the extent that users could at all understand what these marketing terms meant, they could at best infer from these that Avast could use third-party analytics tools to improve its products and services. Data being transferred to Jumpshot, and on top of that being made available to third parties, could not reasonably be inferred by the users from the information provided to them.

4.9. The clarification of the opt-out option, insofar as users could find it, was also inadequate. There too, Avast did not make it clear that it collected data on the user's entire browsing history, nor that it monetised it through Jumpshot by making it available and/or selling it to third parties. Avast only mentioned as a purpose that data was shared with third parties for *"analytics"*, but as mentioned, users could at best infer that Avast could use third-party analysis tools to improve its products.

4.10. The opt-in option Avast gave to new users in July 2019 also contained incorrect and insufficient information. In it, Avast informed users that data was shared with Jumpshot, who "could" pass such data on to its customers. This information was incorrect, because Avast falsely claimed that the information it passed on to Jumpshot could not be traced to individual users, when in reality recipients of the Jumpshot packages in fact could identify users. Furthermore, the opt-in option did not contain the information that was (also) missing from the Privacy Policy, such as what personal data was collected, for what purpose, who the third parties were and what the consequences for users could be. Finally, this text was also insufficiently clear and specific.

Re (ii): The provision of data to Jumpshot was not compatible with the purpose for which the data had been collected

4.11. Avast informed users only that data collection allowed it to offer and improve its own security-focused products and services. Avast did not mention in the Privacy Policy that the personal data was also collected for the purpose of Jumpshot's commercial activities and provided to Jumpshot for

that purpose. The provision of the personal data to Jumpshot is not covered by the purpose for collecting data as mentioned by Avast in the Privacy Policy.

4.12. Sharing data with Jumpshot, which in turn provided and/or sold this data to third parties, thus constitutes 'further processing'. Of this, it must be assessed whether it was compatible with the purpose for collecting data. Such is not the case:

- There is no connection between the original purpose for collecting data on the one hand, and the new purpose on the other. After all, the purpose for collecting data was to protect users and warn them about unsafe websites. Making data available and/or selling it (via Jumpshot) to online marketing and analysis services is in no way compatible with the purpose for collecting data. Indeed: it is completely at odds with the original purpose. The provision of data to Jumpshot does not logically result from and is not related to warning users about unsafe websites.
- Users were not aware that their data was (also) being collected for the benefit of Jumpshot and could not reasonably expect this to be so.
- It must be assumed that, as a result of the provision of data, Jumpshot obtained special personal data as referred to in article 16 Wbp and article 9(1) GDPR.
- The further processing means that users (so far) have had no control over the context in which the data can be used. This may have very serious consequences. It is likely that Jumpshot itself or its customers have used the data to segment or profile users. This could have highly undesirable and even discriminatory consequences.
- The data was covertly obtained and provided to Jumpshot, meaning that there was no transparency. Only after Avast's unauthorised behaviour had been publicised in 2019, i.e. after a great deal of data had already been provided, did Avast start an (inadequate) attempt to ask its users (as yet) for the required consent.

4.13. This makes it clear that Avast's collection of data with the intention of providing it to Jumpshot was not in line with the purpose limitation principle.

4.14. Avast also violated the data minimisation requirement. Avast collected the data for the purpose of warning users about unsafe and unreliable websites. This purpose for collecting required certain data only (such as data about the user's device and internet addresses). However, Avast also collected and stored the user's entire browsing history. Furthermore, this

purpose did not require data to be made available or provided to Jumpshot. The collection of unnecessary data and the provision of data to Jumpshot were thus inadequate, irrelevant and not limited to what was necessary for the purpose for which the data was collected.

4.15. The principle of data minimisation also implies that data should not be kept longer than strictly necessary for the purpose for which it is collected. Avast shared information with third parties contrary to the purpose for which it was collected and without users being aware of this, meaning that Avast has by definition failed in its obligation not to store data longer than is necessary for the purpose for which it was collected (article 10(1) Wbp and article 5(1)(e) GDPR). After all, the third parties continued to have access to the data, even if this was no longer necessary for the security-oriented products and services offered by Avast.

Re (iii): Avast processed personal data without the required consent of the Members and without legitimate interest

4.16. Until July 2019, users did not give any consent at all. Avast only offered new users an opt-in option for the provision of personal data to, and processing by, Jumpshot from July 2019. Before that time, Avast operated an opt-out system, whereby users were deemed not to object to data processing unless they actively indicated otherwise. The opt-out system by definition did not constitue legally valid consent from users. Avast was not entitled to assume that users did not object as long as they did nothing. After all, that could not be considered an (active) expression of will.

4.17. Moreover, the opt-in introduced in July 2019 was wholly inadequate, given the requirements for legally valid consent:

- The opt-in included only the information that users' data could be shared with Jumpshot, but not the other information that Avast should also have provided.
- The requested consent was not sufficiently specific. Avast incorrectly made it appear as if only anonymised data could be provided to Jumpshot. Also, Avast did not clarify what kind of marketing and analytics services it was developing based on the data and what that could mean for users, also considering the level of detail of those services that Jumpshot said it provided to its customers.
- In the opt-in screen, Avast referred to other documents, such as a "Consent Policy", but did not clarify what was contained therein. Avast thus did not meet the unambiguity requirement.
- The opt-in screen contained a default ticked checkbox (containing "I AGREE") that the user had to uncheck if he did not wish to give consent. Consent given in that way is not an unambiguous active act, according to the CJEU, and therefore was and is not legally valid.

- Finally, withdrawing consent was not as easy as giving it. For example, the vague wording in the Privacy Policy showed that withdrawing consent required actively contacting Avast, but how the user should do so remained unclear.

4.18. Avast therefore did not have adequate and legally valid consent, even when it said it offered its users an opt-in.

4.19. To the extent that Avast takes the position that it can rely on the processing basis 'legitimate interest', it is too late in doing so, for Avast should have informed its users about the ground(s) for processing the data prior to actually processing the data, but it failed to do so.

4.20. Even if such were different, Avast still had no legitimate interest. Avast stated in the Privacy Policy that the personal data collected was necessary for the functioning of its products and (in the latest version of the Privacy Policy) that these data was then processed in pseudonymised and anonymised form for *"cross-product marketing, cross-product development and third-party trend analytics"* and that this was done in the interest of the user. Apart from the fact that Avast used vague descriptions and left out essential information, it has become clear that the personal data was processed for Avast's purely commercial interest in offering its security services. The underlying (covert) purpose, namely the provision and/or sale of valuable information products based on the surfing behaviour of its users, is also (at most) a purely commercial interest. Based on the standard explanation of the Dutch DPA, this is not a legitimate interest.

4.21. There was also no need to process the data. The provision of anti-virus and anti-malware services clearly does not require the collection of such a large amount of personal data, including special personal data, as Avast did at the time. There were and are several alternative, less far-reaching practices.

4.22. Finally, the interests of users have been disproportionately affected, when considering the relevant factors:

- Avast collected data on a very large scale. The covert data collection by Avast continued for years, so Avast probably collected from many users their entire browsing history over all those years.
- The users did not know that this personal data was being collected, nor that the data was being provided to Jumpshot. Instead, the users had precisely turned to Avast as an anti-virus and anti-malware service provider for the purpose of *protecting* their privacy interests. The fact that Avast of all parties secretly collected data for commercial purposes was beyond any reasonable expectation. Avast wrongly failed to take into account the reasonable expectations of data subjects.

- The consequences of Avast's unlawful actions for users can be serious and far-reaching. After all, marketing and analytics tools reveal interests, preferences and beliefs at an individual level. As such, these tools should be seen as means by which influence can be exerted on users. Furthermore, the loss of control over personal information can lead to feelings of irritation, anxiety and stress, and self-censorship, among users.
- Avast processed detailed data on its users' entire browser history, including special personal data. This provided insight into the behaviour and mental state of the person concerned over an extended period of time. The users included extra vulnerable groups such as minors.

4.23. All this means that Avast's commercial interests cannot override the legitimate interests of users in the protection of their (special) personal data and privacy, as regulated by law.

Re (iv): Avast processed special personal data in breach of the processing ban

4.24. Since Avast collected users' integral browser history, it by definition also processed special personal data with the help of its products. For example, if users want to look up information about a particular chronic disease, they will generally do so via the internet. Similarly, Avast could establish through the visited website that the user purchased certain products, such as medicines or medical devices, with a certain frequency. The same applies to visits to websites with political, religious or sexual content.

4.25. Avast was only allowed to process special personal data insofar as it could and can prove that users had explicitly consented to it and/or to the extent that users themselves had clearly disclosed the special data, but this is not the case.

4.26. Avast had not sought or obtained any consent from its users for the data processing at all until July 2019, and in an absolutely inadequate manner from July 2019 onwards.

4.27. People who use the internet to search for information or to take of matters, do so on the assumption that their actions will remain private, or at least not be shared publicly, meaning that there is evidently no question of disclosure, let alone that the users intended to disclose their entire browsing history and other personal data.

Re (v): Avast transferred personal data to Jumpshot in violation of the prohibition on transfer

4.28. It is undisputed that Avast provided personal data to Jumpshot in the US. According to data protection legislation, the transfer of personal data to third countries, i.e. countries outside the EU/EEA, may not compromise the level of protection guaranteed by that legislation. For this reason, the transfer of personal data to these third countries is in principle prohibited, unless one of the exceptions can be successfully relied on. That is not the case here.

4.29. In the Relevant Period, there was no valid adequacy decision as referred to in article 45 GDPR. Two consecutive adequacy decisions, in which the Commission claimed that the US ensured an adequate level of protection ("Safe Harbor" and "Privacy Shield") have both been invalidated by the highest European court, after it found that the level of protection of US law is insufficient. These are the *Schrems I*[3] and *Schrems II* judgments.[4]

4.30. To the extent that Avast argues that it transferred personal data on the basis of *standard contractual clauses* as referred to in article 46 GDPR, it did not make clear, contrary to articles 13 and 14 GDPR, what additional measures it had taken to achieve the required level of protection. In view of the accountability requirement of articles 5(2) and 14(1) GDPR, Avast must be able to demonstrate this. It may therefore be assumed that Avast failed to take any additional measures at all. Even if Avast had done so, there was no appropriate additional measure in fact available that prevents the US government from accessing the data. Since Jumpshot made or sold the data available to third parties, no other conclusion can be drawn than that Jumpshot either received the data unencrypted or that it could decrypt it. Access by the US government was then not prevented. Any additional measures were therefore ineffective.

4.31. As far as the Foundation can ascertain, Avast did not have any *binding corporate rules* approved. If Avast did use approved *binding corporate rules*, it failed to publish these.

Re (vi): Avast's conduct is an unfair trade practice

4.32. Avast did not inform its users, or at least did not inform them sufficiently clearly, about the operation of its products. There is nothing to show that Avast would collect a large amount of personal data via its products and would make these available to third parties and/or sell them via Jumpshot.

4.33. This information (not shared with consumers) was essential for the users. Consumers made purchasing decisions without this essential information. It is likely that, if the users had known this, many of them would not have

[3] CJEU 6 October 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems I*).
[4] CJEU 16 July 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).

used Avast's products, at least not under the same conditions. This constitutes a misleading omission within the meaning of article 193d (2) or (3) of Book 6 DCC. The burden of proof that this would be otherwise rests on Avast.

Avast has unjustly enriched itself

4.34. Avast has unjustly enriched itself with its unlawful acts at the expense of the Members within the meaning of article 212 of Book 6 DCC.

4.35. Benefiting by Jumpshot from the covertly collected personal data has been extremely lucrative for Avast. Avast's enrichment is unjustified. This is because Avast's acts and omissions have violated data protection laws, including cookie rules, on a large scale, while it has also been guilty of misleading business practices. Avast's enrichment arises directly from these violations. As there is no justification for the enrichment, it is unjustified.

4.36. As a result of these violations the Members have been impoverished. Indeed, Avast's users, including the Members, unknowingly provided a large amount of personal data to Avast and thus lost control over that personal data. It is well established that personal data has (economic) value. This directly benefited Avast. There is thus a causal link between Avast's enrichment and the Members' impoverishment.

5. DAMAGE SUFFERED BY THE MEMBERS SHOULD BE COMPENSATED BY AVAST

5.1. Avast's conduct has resulted in both material and non-material damages on the part of the Members. Avast should compensate the damages suffered by the Members.

Material damage

5.2. Personal data is worth money. However, Avast did not pay the constituency for the data. The improper use of the Members' personal data enabled Avast to make a profit. The Foundation requests the District Court to assess the material damage suffered by the Members, in accordance with article 104 of Book 6 DCC, in the amount of the profits realized by Avast in the Netherlands as a result of its unlawful actions in the Relevant Period.

Non-material damage

5.3. On a structural and long-term basis, Avast has been deliberately and unlawfully processing (special) personal data of the Members and providing it to Jumpshot, which made it available or sold it to third parties, while the Members wanted to protect their personal data with Avast's products against unlawful use by third parties and against online risks in general,

and the products were also advertised as such by Avast. As a result, the Members have lost control over their personal data. Loss of control is explicitly mentioned in the GDPR as one of the types of harm that can result from a privacy breach.

5.4. That provision to Jumpshot and an unknown quantity of third parties undoubtedly led to profiling and influencing the (choice) behaviour and perceived 'online world' of users, with potentially undesirable and even discriminatory consequences, which are also listed in the GDPR as types of harm that can arise from a privacy violation.

5.5. In addition, as a result of the transfer to Jumpshot in the US, the personal data of the Members has been exposed to US legislation, which does not provide a level of protection that is essentially equivalent to that in the EU. In practice, this means that the Members' personal data may be subject to surveillance by US government agencies.

5.6. It is plausible that the breach of standards led to feelings of distrust, indignation and concern, as well as self-censorship, among the Members. This is all the more true as they used Avast's software to enjoy protection, when in reality this put their data on the street. This too results in non-material damage that is eligible for compensation.

5.7. Given the various criteria considered in Dutch case law, Avast's breach of standards is so far-reaching that adverse effects on the Members must be assumed.

5.8. In these proceedings, the Foundation proposes an approach whereby those affected by Avast's breaches of standards are awarded the same amount of damages. This approach, a standardisation in the form of fixing the same amount, is in line with Supreme Court case law and is also advocated in the literature. To the extent that individual circumstances justify a 'surcharge' on the amount of damages, for example in situations where the breach of standards has led to (even) more far-reaching consequences for a specific person than the consequences for the collective, the system of the WAMCA offers a solution for this in the form of the opt-out possibility of article 1018f DCCP.

5.9. The Foundation believes that, given the relevant circumstances and the various aspects of the breaches of standards, compensation of EUR 1,000 per Member is reasonable and appropriate. In the alternative, the Foundation requests the District Court to assess the non-material damages at EUR 200 for each year or part of a year in the Relevant Period that a Member used (one of) Avast's products.

Joint and several liability

5.10. The various Avast entities are jointly and severally liable for the damage suffered by the Members, because they are joint controllers within the

meaning of article 1(b) Wbp and article 4(7) GDPR. After all, the Avast entities were part of the Avast group and acted as one business unit providing one service to data subjects worldwide, operated one globally applicable privacy policy and implemented changes in policy, goals and means centrally and globally. These circumstances indicate that the legal and actual decision-making power with respect to the processing of the personal data also lay with Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V., as well as with Avast Ltd., as found by the FTC.

5.11. The basis for this collective action is article 305a of Book 3 DCC, as amended with effect from 1 January 2020 when the WAMCA entered into force. This case concerns a continuous wrongful act by Avast during the Relevant Period, or at least a series of events that took place both before and after 15 November 2016, so that the WAMCA is applicable under article 119a New Civil Code Transitional Act.

6. CLAIM FOR RELIEF

6.1. Inserted below is the full claim for relief as contained in the summons.

6.2. The Foundation requests the court, by provisionally enforceable judgment to the extent possible:

1. To designate the Foundation as exclusive representative as referred to in article 1018e DCCP.

2. To rule that this collective action seeks to protect users and former users of services and products of Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. at any time during the period 1 January 2014 - 30 January 2020 (the Relevant Period), not acting in the conduct of a profession or business, in so far as they were residing in the Netherlands at the time of the use of these services (the Members).

3. To rule that, in accordance with article 1018f (1) DCCP, any Member residing or domiciled in the Netherlands may, within one month of the announcement pursuant to article 1018f (3) DCCP of the decision designating the exclusive representative, notify the registry of the court, by written communication, that he or she no longer wishes his or her interests to be represented in this collective action.

4. To rule that, in accordance with article 1018f (5) DCCP, any Member who is not residing or domiciled in the Netherlands may, within one month of the announcement pursuant to article 1018f (3) DCCP of the judgment appointing the exclusive representative, notify the registry of the court, by written communication, that he or she consents

to having his or her interests represented in this collective action and that his or her interest is not represented in a collective or individual claim based on similar issues of fact and law for the same event or events against the defendants in another EU or EEA Member State.

5. On the grounds set out in this writ of summons, to rule that Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. jointly and/or each of them individually during the Relevant Period have and/or has acted in an unlawful manner towards the Members and/or have been and/or has been unjustly enriched and are and/or is liable for the damage suffered and yet to be suffered by the Members as a result.

6. To order Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. jointly and severally to pay compensation for the Members' material damage, to be assessed in accordance with article 104 of Book 6 DCC at the amount of the profits which Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. have enjoyed as a result of their unlawful actions, for each Member to be increased by the statutory interest from the moment the Member in question started to use the product, or first product, of the defendants, or in any case from date of this summons, or at least the date of passing judgment, until the day full payment is made.

7. To order Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. jointly and severally to pay compensation for non-material damage, to be assessed at an amount of EUR 1,000 per Member, or in any case (in the alternative) at EUR 200 per Member, for each year or part of a year in the Relevant Period that he or she used all or one of Avast's products, or at least (as a second alternative) to rule that this damage shall be assessed further in separate follow-up proceedings and shall be settled in accordance with the law: and (both principally and in the alternative): for each Member to be increased by the statutory interest from the moment the Member in question started to use the product, or first product, of the defendants, or in any case from date of this summons, or at least the date of passing judgment, until the day full payment is made.

8. To rule that the collective settlement of claims will (primarily) be structured in a manner to be determined by the Foundation, or at least (in the alternative) as the court deems advisable on the basis of proposals for the collective settlement of claims to be submitted by

the Foundation and the defendants pursuant to article 1018i DCCP in the proper administration of justice.

9. To order that Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. shall, within four weeks of the judgment to be rendered in this matter:

   (i) Destroy all user data unlawfully collected by Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. en AVG Ecommerce CY B.V., to the extent that they still retain such data.

   (ii) Inform any third parties (outside the Avast group) who have received users' data that the defendants have unlawfully collected, that the provision of data was unlawful and that further use of the data, including storing it, by the third parties is unlawful, and to request those third parties (a) to destroy such data and (b) to inform the defendants and the Members of the identity of all the other parties to which the data has also been transferred.

   (iii) Inform each Member (a) what data Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. and/or other entities within the Avast group have collected about him or her, (b) when and for how long this was done, (c) with which persons and/or legal entities this data has been shared and (d) whether, and if so when, this data has been destroyed.

   (iv) Create a website (or allocate a part of their website) so as to enable the Members to have access to the information referred to in 9 (iii) of the claim for relief.

   (v) Grant an independent auditor, such as Deloitte, E&Y or PwC, access to the IT facilities of Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. (including, but not limited to, remote servers at third parties providing services to the defendants) and otherwise provide all the assistance required for the purpose of conducting an independent investigation into compliance with the orders referred to in 9 (i) - (iv) of the claim for relief.

10. To appoint Deloitte, E&Y or PwC or a similar party to be determined by the district court in the proper administration of justice as independent investigators as referred to in 9 (v) of the claim for relief.

11. To order Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. jointly and severally to reimburse the Foundation for the reasonable and proportionate legal costs and other costs of these proceedings, consisting of: (a) the full legal costs incurred by the Foundation pursuant to article 1018l (2) DCCP, or at least the legal costs actually incurred pursuant to article 237 DCCP, plus the statutory interest from the date judgment was given until the date payment in full is made; (b) the full (extrajudicial) costs incurred by the Foundation pursuant to article 96 of Book 6 DCC, plus the statutory interest from the date judgment was given until the date payment in full is made; (c) the agreed fee to be paid by the Foundation to the litigation funder pursuant to article 96 of Book 6 DCC and article 1018l (2) DCCP; and (d) the full costs of settling the damage, all this as to be assessed further.

12. To order Avast Software s.r.o., Avast Ltd., Avast Holding B.V., Avast Software B.V. and AVG Ecommerce CY B.V. jointly and severally to pay the costs of the proceedings incurred by the Foundation, to be increased by the subsequent costs amounting to EUR 178 without service, or EUR 270 in the event of service having to be made, all this to be paid within fourteen days from the date of the judgment, and - in the event that the costs, or subsequent costs, are not paid within the period stipulated - to be increased by the statutory interest on the (subsequent) costs, to be calculated from the aforementioned period for payment until the date payment is made in full.

This case is being handled by:
J.H. Lemstra and M.N. van Dam
Lemstra Van der Korst N.V., PO Box 75655, 1070 AR Amsterdam
and:
Prof. G.J. Zwenne
Pels Rijcken N.V., P.O. Box 11756, 2502 AT The Hague