LEMSTRA VAN DER KORST

BY REGULAR AND REGISTERED POST TO:

Avast Software s.r.o.
Pikrtova 1737/1a
Nusle
Prague 4
140 00 Czech Republic

Avast Software, Inc.
9300 Harris Corners Parkway
Suite 450
Charlotte NC 28269
United States

Avast Software B.V.
Databankweg 26
3821 AL Amersfoort

Avast Plc.
110 High Holborn
London WC1V 6JS
England

AVG Ecommerce CY B.V.
Databankweg 26
3821 AL Amersfoort

Avast Holding B.V.
Databankweg 26
3821 AL Amersfoort

J.H. Lemstra
Attorney-at-law

M.N. van Dam
Attorney-at-law

Prins Hendriklaan 16, 1075 BC Amsterdam
P.O. Box 75655, 1070 AR Amsterdam

tel.: +31 (0)20 20 50 531
mob.: +31 (0)65 31 50 917

mail: j.lemstra@lvdk.com
mail: m.vandam@lvdk.com
web: www.lvdk.com

Also by e-mail:
Ondrej.Vlcek@avast.com
John.Schwarz@avast.com
Trudy.Cooke@avast.com

Re	Letter and notification before action regarding various unlawful acts and request for the preservation of evidence
Ref.	5356
Date	29 August 2022
Place	Amsterdam

For the urgent attention of the Boards of Directors, General Counsel of the above entities

5356/1009833.6

Dear Mr. Ondřej Vlček, Mr. John G. Schwarz and (other) board members of the addressees of this letter,

INTRODUCTION

Our firm, together with our co-counsel Pels Rijcken Droogleever Fortuijn N.V., act on behalf of Stichting CUIC -- Privacy Foundation for Collective Redress (the "**Foundation**"). The Foundation has become aware of very serious unlawful acts committed by either or all of Avast Software s.r.o., Avast Plc., Avast Holding B.V., Avast Software B.V., AVG Ecommerce CY B.V., and Avast Software, Inc. ("**Avast**"), resulting from blatant disregard for both European and national (Dutch) privacy and consumer law.[1] Avast consistently represents itself as a trustworthy software developer, notably in the IT-security field. In fact, Avast has admitted to collecting and selling its customers' personal data, without their consent, for its own commercial benefit. Avast committed these continuous acts (at least) from 2015 at least until Avast has ensured that all unlawfully obtained data is irreversibly erased from its systems and all systems from third parties (the "**Relevant Period**").

The Foundation – established in accordance with article 3:305a Dutch Civil Code ("**DCC**") – is a non-profit foundation incorporated under the laws of the Netherlands, with a registered seat in Amsterdam, the Netherlands. The Foundation's members include the Dutch foundation Stichting Privacy First and the Austrian non-profit association *noyb* – European Center for Digital Rights, both of which have been active in the field of protecting the personal data and privacy of European citizens for many years.

The Foundation's statutory objective is to protect the personal data, privacy and other interests of European citizens. It pursues this inter alia by taking legal action against companies that violate data protection laws, the right to the protection of personal data and other rights, including the rights established by the General Data Protection Regulation ("**GDPR**"). In the case at hand, the Foundation represents the interests of all victims of the unlawful conduct committed by Avast, who reside or had residence in the Netherlands in the Relevant Period (the "**Avast Victims**"). The Foundation's means and objectives empower it to represent the interests of all Avast Victims. The Foundation and its endeavours to – inter alia – obtain compensation for the violations (as defined below in nr. 15 and further and nr. 40 and further (the "**Violations**"))

[1] I.e. failing to collect and process data consistent with the requirements of the Dutch Personal Data Protection Act ('*Wet bescherming persoonsgegevens')* ("**DDPA**"), the General Data Protection Regulation ("**GDPR**"), the GDPR Implementation Act ('*Uitvoeringswet AVG')* ("**GDPR Implementation Act**") and the Dutch Telecommunications law ('*Telecommuncatiewet'*) ("**DTA**"), as well as for violating the provisions of the Directive on Unfair Commercial Practices (2005/29/EC, *OJ* 2005, L149/22), as transposed into Dutch civil law, particularly article 6:193a DCC.

in favour of the Avast Victims, are supported by other Dutch and EU consumer and data protection organisations.

For the purpose of the Avast Victims, the Foundation holds Avast liable for (incurred and future) damages and seeks for adequate compensation for the damages caused in the Relevant Period by the Violations. The Foundation also seeks to receive information on all unlawfully obtained customer data held by Avast about each of the Avast Victims, with any such data held by Avast being subsequently destroyed, a list of all third parties to whom such data has been directly or indirectly shared is provided to the Avast Victims, and an undertaking obtained by Avast from each third party recipient of such data that it also has destroyed the same. In addition, the Foundation seeks to enter into a dialogue with Avast to prevent similar wrongdoing in the future and to ensure Avast's compliance with European and Dutch privacy and consumer law.

Before seeking legal remedies, the Foundation and its lawyers (Lemstra Van der Korst and Pels Rijcken) are committed to engaging in a constructive dialogue with Avast on these issues. Should Avast not choose to enter into such dialogue, the Foundation will – without further notice – initiate collective proceedings in the Netherlands.[2] Within these proceedings, the Foundation will seek the injunctive relief outlined above, a declaratory decision confirming Avast's unlawful conduct and a claim for damages.

In order to enable a meaningful dialogue in redressing Avast's wrongdoing, the grounds for the Foundation's and/or the Avast Victim's claims are set out below. The Foundation, however, expressly reserves its right to amend, increase and adjust the grounds for its claims at a later stage.

Additionally, this letter serves as a formal notice interrupting any applicable limitation period (*stuitingsbrief*, within the meaning of article 3:317 DCC) for any and all claims against Avast which result from the Violations.

FACTS

1. Avast is an international software producer, well-known for its antivirus and security software products and services. These products and services were offered to the public under the names Avast and AVG, for example Avast AntiVirus and AVG AntiVirus. In 2021 Avast had a worldwide revenue of US$ 941.1 million. During this period, over 435 million customers used its products worldwide.[3] Of those users, a substantial number reside in the Netherlands and comprise the Avast Victims.

[2] Under the Dutch Act on the Collective Settlement of Mass Claims (*Wet afwikkeling massaschade in collectieve actie*, referred to as "**WAMCA**").

[3] Avast plc annual report 2021, p. 2.

2. During the Relevant Period, Avast offered browser extensions under the name Avast Online Security for the Google Chrome, Mozilla Firefox, Microsoft Edge and Opera browsers.[4] During this period Avast also offered the Avast Secure Browser, a browser that included a pre-installed Avast Online Security extension (collectively, the "**Online Security Extension**").

3. Avast stated that the Online Security Extension offers "*protection against known phishing and malware sites, improving your browsing overall browsing [sic] experience with crowd source web reputation rating*."[5] The processing performed by the Online Security Extension was cloud-based. This means that all data that Avast collected, was sent to Avast's servers. For instance, when a user visited a website, the URL of that website was sent to Avast's servers in order to check if the website was malicious or otherwise unsafe to visit.

4. In 2013, Avast acquired the US-based company Jumpshot, a marketing analytics company.[6] According to information on the websites of Avast and Jumpshot, Jumpshot's services were used to examine consumer journeys in detail: "*examine every search, click, and buy. On every site*."[7] Jumpshot's data allowed customers to get a "*super-detailed view of every buy path, as it twists and turns*." [8] Jumpshot sold its customers very detailed and extensive information about online consumers' internet usage. The amount of information was limitless. Jumpshot advertised with the statement: "*All of the data with none of the walls. See it all, finally*." [9]

[4] See the internet archive of the wayback-machine (https://addons.mozilla.org/en-US/firefox/addon/avast-online-security/), e.g. captures of 5 December 2014, 30 July 2018 and 1 October 2018 (last visited 25 August 2022).

[5] https://addons.mozilla.org/en-US/firefox/addon/avast-online-security/, last visited 25 August 2022).

[6] https://press.avast.com/avast-software-acquires-jumpshot-to-work-magic-against-slow-pc-performance.

[7] See the internet archive of the wayback-machine (https://web.archive.org/web/20191127181613/https://www.jumpshot.com/, e.g. captures of 27 November 2019 (last visited 25 August 2022).

[8] Idem.

[9] See the internet archive of the wayback-machine (https://web.archive.org/web/20191205215055/https://www.jumpshot.com/product/clickstream-data) e.g. captures of 27 November 2019 (last visited 25 August 2022).

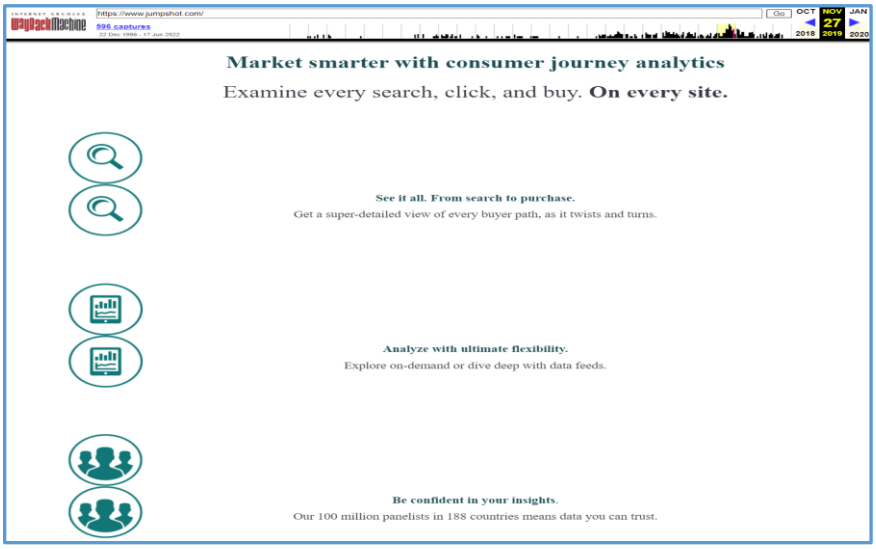


Figure 1: Source: internetwayback-machine (https://web.archive.org/web/20190621000418/https://www.jumpshot.com/), capture of Avast-landingpage, of 21 July 2019 (last visited 25 August 2022).

5. Jumpshot was marketed to two audiences, "*Data Lovers*" and "*Publishers & Advertisers*." Data Lovers were encouraged to use the tools to gain deeper analysis with unlimited "*granular data feeds*" that allowed them to "*follow user journeys at the atomic level*."[10] Publishers & Advertisers were encouraged to develop targeted campaigns based on "*real-life browsing*" and "*real behaviors*", again at the individual user level.[11]

[10] See the internet archive of the wayback-machine (https://web.archive.org/web/20191127181613/https://www.jumpshot.com/), e.g. capture of 27 November 2019 (last visited 25 August 2022).

[11] Idem.

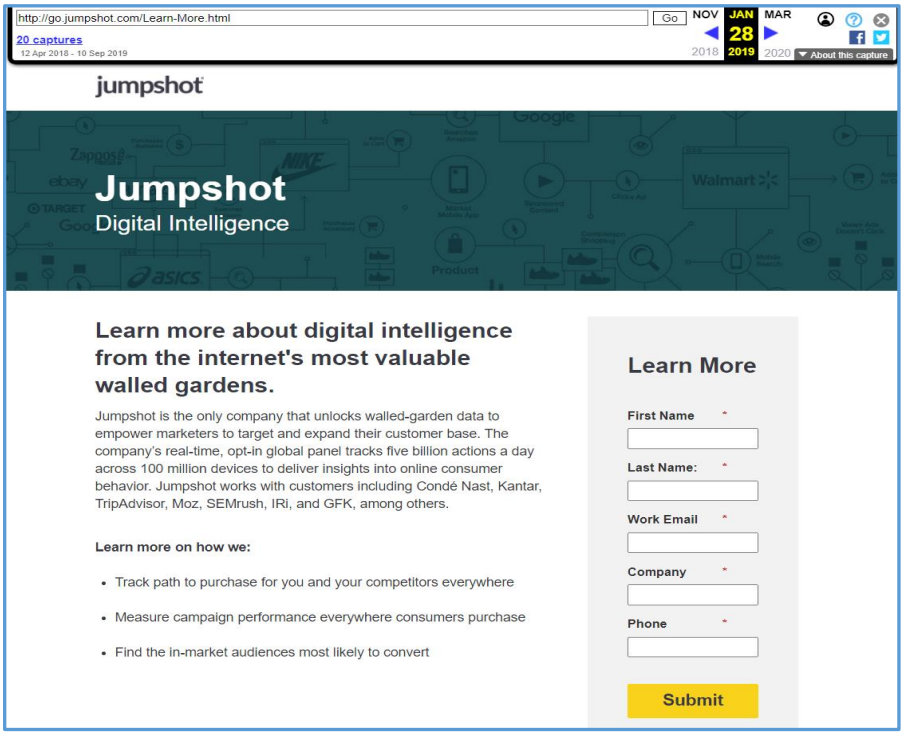


Figure 2: Source: internetwayback-machine (https://web.archive.org/web/20190128002855/http://-go.jumpshot.com/Learn-More.html), captures of Jumpshot web pages of 28 January 2019 (last visited 25 August 2022).

Figure 3: Source: internetwayback-machine (https://web.archive.org/web/20190621000418/https://¬www.jump-shot.com/), captures of Jumpshot-webpages of 21 July 2019 (last visited 25 August 2022).

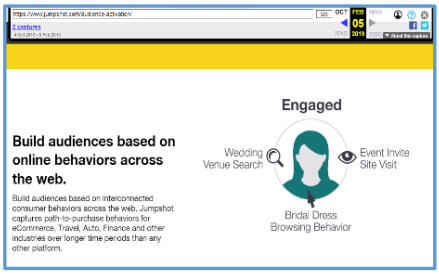


Figure 4: Source: internetwayback-machine (https://web.archive.org/web/20190205194940/https://¬www.jump¬shot.com/audience-activation/), captures of Jumpshot-webpages of 5 February 2019 (last visited 25 August 2022).

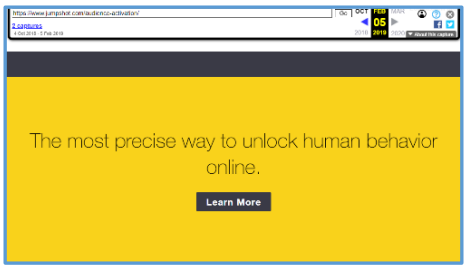


Figure 5: Idem.

6. Through Jumpshot, Avast offered three main services to advertising technology (Adtech) and other customers:

   (1) A feed of the top 10.000 domains that Avast users visited, that could be used to spot trends;

   (2) The "All Click Feed", which allowed clients to buy information on all clicks Jumpshot collected on a particular domain; and

   (3) The "Insight Feed", which offered a feed of live user data focused on cross-platform shopping user pathways and behaviour.[12]

All Clicks Feed

All Clicks Feeds are sold on a domain level (so for example, you could buy the feed for amazon.com) and can be run against our Full or Stable Panel. As the name indicates, what we are reporting on is every click event that we detected from our panel on a given domain. What we don't do is report on the Jumpshot Device ID that executed the clicks to protect against the triangulation of PII. We only provide a unique session ID for each session, sessions having a standard 30 minute timeout applied. The advantage of purchasing an All Clicks Feed is that if you are curious about the frequency of events that Jumpshot does not discover patterns for within our standard products, or you simply need a deeper understanding of activity on a domain without any filtering, All Clicks Feeds will let you see all of the activity, The downside if that you cannot use All Clicks Feeds to understand things like cross-visitation or repeat visitors. Because we don't utilize our Pattern Repository to identify events in this feed, it can be produced without any event discovery work on Jumpshot's part. As such, this is another product that relies purely on raw data.

Figure 2: Source: Vice Motherboard (https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation) internal Jumpshot document obtained by Motherboard and PCMag.

7. Among the many clients of Jumpshot were Google, Microsoft, Unilever, TripAdvisor, IBM, Yelp and Pepsi.[13] Needless to say, that – by acquiring

[12] https://martechseries.com/analytics/jumpshot-launches-enhancements-insights-platform-allowing-marketers-understand-online-shoppers-competitors-like-never/.

[13] See the internet archive of the wayback-machine (http://web.archive.org/web/20190621000418/https://www.jumpshot.com/), e.g. capture of 21 June 2019 (last visited 25 August 2022) ; https://samagame.com/en/avast-ensures-that-they-will-not-collect-more-customer-data-through-their-subsidiary-jumpshot-after-it-is-discovered-that-they-were-selling-them/.

Jumpshot – Avast created a commercial incentive within its group to collect and use data.

AVAST'S UNLAWFUL PRACTICES AT STAKE

8. Following several publications in 2019 – amongst others from Wladimir Palant[14] under the title "*Avast Online Security and Avast Secure Browser are spying on you*"[15] – it became clear that the commercial incentives within Avast prevailed over the legal rights of its consumer customers under European and national (Dutch) law.

9. According to these publications, the Online Security Extensions unlawfully collected data as follows: every time a webpage was visited, Avast collected (i) the full address of the page the user visited, (ii) the webpage title, (iii) the full address of the page the user came from, (iv) how the user came to the page (for instance by using a search engine or by entering the address), (v) whether the page was visited before (country code), (vi) several unique user IDs, (vii) the browser and operating systems used (both types and versions), (viii) the search results and other links included on search engine webpages, (ix) the user's approximate geographical location, (x) the assumed gender and age group of the user and (xi) user identifiers, names, email addresses and home addresses.[16]

10. Palant performed further research and discovered that the data Avast collected was transferred to Jumpshot.[17] The news was picked up by tech publications PCMag and Motherboard which were provided with documents showing that the Avast antivirus software installed on a personal device was collecting personal data and sending it to Jumpshot. Jumpshot then selected and amended the data by repackaging it into various different products that were sold to third parties. As confirmed by PCMag and Motherboard, despite Avast's claim that the data was "*fully de-identified and aggregated and cannot be used to personally identify or target you*", the data could, in fact, be linked

[14] Wladimir Palant operates the blog Almost Secure on palant.info. He posts blogs about security topics. Notably, he is also the original developer of popular anti ad/tracking web browser extension Adblock Plus, https://palant.info/about/.

[15] Wladimir Palant, Avast Online Security and Avast Secure Browser are spying on you, blogpost 28 October 2019, https://palant.info/2019/10/28/avast-online-security-and-avast-secure-browser-are-spying-on-you/.

[16] Wladimir Palant, Insights from Avast/Jumpshot data: Pitfalls of data anonymization, blogpost 18 February 2022, https://palant.info/2020/02/18/insights-from-avast/jumpshot-data-pitfalls-of-data-anonymization/.

[17] Wladimir Palant, Mozilla and Opera remove Avast extensions from their add-on stores, what will Google do? blogpost 3 December 2019, https://palant.info/2019/12/03/mozilla-removes-avast-extensions-from-their-add-on-store-what-will-google-do/.

back to individual Avast users and was personal data (i.e., and personal identifiable information) under GDPR.[18]

11. Following the publication of Palant's report, operators of the Firefox, Chrome and Opera browsers removed the Online Security Extension from their browser extension stores.[19] On 28 January 2020, Avast published its first official statement on the matter. According to Avast it had discontinued the processing of the personal data it had collected from its customers for purposes other than security, and had stopped sharing data with its subsidiary Jumpshot. According to Avast, no personal identifiable information was shared and users had the ability to opt-out of their data being shared with Jumpshot. Moreover, Avast claimed to have started transitioning to an opt-in mechanism for new downloads and subsequently for existing users.[20]

12. Two days later, on 30 January 2020, Avast's CEO, Ondrej Vlcek, apologized to the Avast customers for this unlawful data collection and processing and announced the winding down of Jumpshot and its activities of selling browser history data.[21]

13. On 11 February 2020, the Czech Data Protection Authority announced a preliminary investigation into these Jumpshot activities.[22]

14. Subsequently, according to Avast's 2020 annual report, claims were settled relating to the Jumpshot activities, with negotiations still ongoing. Avast

---

[18] The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks, PCMag 27 January 2020, https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks; Leaked Documents Expose the Secretive Market for Your Web Browsing Data, Motherboard 27 January 2020, https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation.

[19] Wladimir Palant, Mozilla and Opera remove Avast extensions from their add-on stores, what will Google do? blogpost 19 Dember 2019, https://palant.info/2019/12/03/mozilla-removes-avast-extensions-from-their-add-on-store-what-will-google-do/ ; Mozilla Removes Avast and AVG Firefox Extensions, PCMag December 4 2019, https://www.pcmag.com/news/mozilla-removes-avast-and-avg-firefox-extensions#:~:text=Avast%20has%20been%20harvesting%20user,from%20their%20add%2Don%20sites; Google removes Avast, AVG extensions from Chrome Web Store after data collection concerns, Google9to5 17 December 2019, https://9to5google.com/2019/12/17/chrome-avast-extensions-removed/.

[20] Avast Official statement on the recent news about privacy, 28 January 2019, https://forum.avast.com/index.php?topic=231828.msg1533674#msg1533674.

[21] Avast to Commence Wind Down of Subsidiary Jumpshot, press release 30 January 2020, https://press.avast.com/avast-to-commence-wind-down-of-subsidiary-jumpshot; Avast Is Going To Stop Selling Your Web Habits, Forbes 30 January 2020, accessible via https://www.forbes.com/sites/thomasbrewster/2020/01/30/avast-is-going-to-stop-selling-your-web-habits/?sh=5c63010289db; Antivirus company shuts down its data-harvesting arm after getting caught red-handed, TheVerge 30 January 2020, accessible via https://www.theverge.com/2020/1/30/21115326/avast-jumpshot-subsidiary-suspended-data-collection-selling-ceo-blog-post; Avast shutters Jumpshot subsidiary after user data harvesting.

[22] Statement of the Czech Office for Personal Data Protection on the current affair concerning Avast Software s.r.o., 11 February 2020, https://www.uoou.cz/en/vismo/dokumenty2.asp?id_org=200156&id=1896.

acknowledged that future claims and liabilities in respect of data protection matters could be forthcoming:

> "*Management has provided the Committee with regular updates on the status of the wind-down, which is substantially complete, and continues to receive updates in relation to developments with regard to the ongoing communications with relevant regulators and authorities in respect of certain data protection matters. Any potential future claims or liabilities arising out of communication with relevant regulators or authorities cannot at this time be quantified. For further details of the provisioning in relation to Jumpshot and the wind down, see page 178.*"[23]
>
> *"The majority of the claims in relation to Jumpshot have been successfully settled as of 31 December 2020. As further disclosure would prejudice the outcome of these negotiations, as permitted by IAS 37.92, we have not made any further disclosures about estimates in connection with the financial effects of, and disclosures about the uncertainty regarding the timing or amount of these.*"[24]

VIOLATION OF DATA PROTECTION RIGHTS UNDER THE GDPR AND THE DDPA

15. In the context of the activities described above, Avast collected and processed a vast amount of personal data about its users. In relation to Avast, the Online Security Extension and Jumpshot, the processing activities can be described as follows (together the "**Processing Activities**"):

- collecting personal data through Avast security software;
- transferring data to Jumpshot;
- selecting data or amending data for the purpose of selling it as (part of) specific products and services; and
- transferring data by Jumpshot to its customers.

16. The GDPR applies to the processing of personal data by Avast, as (a) Avast, according to its General Privacy Policy at the time, qualified as controller with respect to the Processing Activities,[25] and (b) Avast processed the personal data in the context of the activities of its establishments in the EU. Moreover, to the extent Avast processed the personal data before the GDPR became applicable, i.e. before 25 May 2018, the Dutch Data Protection Act ('*Wet bescherming persoonsgegevens*': "**DDPA**") applied.

---

[23] https://investors.avast.com/media/1401/annual-report-2020.pdf, p. 99.

[24] https://investors.avast.com/media/1401/annual-report-2020.pdf, p. 178.

[25] Avast General Privacy Policy, www.avast.com/en-gb/privacy-policy#pc.

17. As a direct result of its relation with Jumpshot's activities, Avast (continuously) violated several principles and provisions of the GDPR (and the DDPA), including, but not limited to:

(a) the principle of transparency (article 5(1)(a) GDPR) and the obligation of information (articles 12, 13 and 14 GDPR; articles 33-34 DDPA);

(b) the principle of lawfulness of processing (article 6 GDPR; article 8 DDPA);

(c) the principle of fairness (article 5(1)(a) GDPR; article 6 DDPA);

(d) the principle of purpose limitation (article 5(1)(b) GDPR; articles 7 and 9(1) DDPA);

(e) the principle of data minimisation (article 5(1)(c) GDPR: articles 10 and 11(1) DDPA) and data protection by design and by default (article 25 GDPR; article 11(2) DDPA); and

(f) the prohibition of processing special categories of personal data (article 9 GDPR; article 16 DDPA).

These violations are discussed below.

(a) Non-compliance with the principle of transparency (article 5(1)(a) GDPR) and the obligation of information (articles 12, 13 and 14 GDPR; articles 33-34 DDPA)

18. The principle of transparency (articles 5(1)(a) and 12-14 GDPR; articles 33-34 DDPA) requires, inter alia, that all processing of personal data should be made transparent to data subjects. Any information and communication relating to the processing of the personal data and its purposes must be easily accessible and understandable to the data subjects. [26]

19. The main document Avast used to inform data subjects was its privacy policy[27] ("**Privacy Policy**"). The information Avast provided in the Privacy Policy in connection to the Processing Activities was incomplete and inadequate for at least the following reasons:

- It did not provide concise and intelligible information. Due to the length of the Privacy Policy and the frequent use of terms such as "may", it was difficult, if not practically impossible, for the user to fully comprehend how Avast actually processed personal data and what

[26] WP29, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, nrs. 8-11.

[27] See the internet archive of the wayback-machine (https://web.archive.org/web/20190803204607/https://www.avast.com/privacy-policy), e.g. capture of 03 August 2019 (last visited 25 August 2022).

the risk for data subjects could be as a result of that processing. In any case, the information provided was not 'concise, transparent, intelligible and easily accessible', as required by article 12(1) GDPR and recital 58.[28]

- In any case, the privacy policy did not refer to relevant information, namely the fact that it continuously processed and sold information on customer browsing activity. This information was dispersed throughout the document in vague and/or misleading language, such as "*We pseudonymize and anonymize the Clickstream Data and re-use it for cross-product direct marketing, cross-product development and third-party trend analytics*."[29] This did not make it explicit that these "products" were not directly related with Avast or its activities – i.e. the products and services of Avast.
- It did not indicate what was the legal ground for its Processing Activities under Article 6 GDPR.
- No retention periods were provided. The Privacy Policy merely stated: "Reasons we might retain some data for longer periods of time include: (…) Direct communication with you and our authorized partners such as for service activation, billing, support, and marketing".[30]
- It did not include information about recipients. The Privacy Policy merely stated: "*We may publish or share that information with third parties that are not part of the Avast Group, but we will only ever do so after anonymizing the data*."[31] This statement also contradicted other parts of the Privacy Policy which suggested that pseudonymized information could be used or shared for marketing purposes. Pseudonymized data is not the same as anonymized data, and is still considered personal data.[32] More importantly, this statement contradicted the facts, as research shows that the data was not at all anonymized. The data was always attached to an individuating,

[28] WP29, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, nrs. 8-11.

[29] See the internet archive of the wayback-machine (https://web.archive.org/web/20190803204607/https://www.avast.com/privacy-policy), e.g. capture of 03 August 2019 (last visited 25 August 2022).

[30] Idem.

[31] See the internet archive of the wayback-machine (https://web.archive.org/web/20191127181613/https://www.jumpshot.com/) e.g. captures of 27 November 2019 (last visited 25 August 2022).

[32] Recital 26 GDPR.

unique and persistent identifier for each user.[33] Furthermore, third party recipients of Avast user data collected by Jumpshot also qualify as "controllers" and should have all been named in the information on recipients.

- It did not clearly mention the identity of the Avast controller and its Data Protection Officer ("DPO").

As a consequence, the Privacy Policy of Avast did not adequately inform data subjects. Therefore, Avast's processing activities in connection to the Jumpshot activities violated articles 5(1)a, 12 and 13 GDPR and articles 33 and 34 DDPA.

(b) Non-compliance with the principle of lawful processing (article 6 GDPR; article 8 DDPA)

20. A key principle under the GDPR is that personal data must be processed lawfully. Article 6 GDPR and article 8 DDPA contain both an exhaustive list of six grounds under which data may be lawfully processed. Consequently, a processing is unlawful in the event that the controller is not able to base its processing on one of these grounds. As it has no lawful ground for the processing of personal data as described above, Avast violated, and possibly still violates, article 6 GDPR and article 8 DDPA.

21. Furthermore, the controller must determine the ground for processing prior to the commencement of data processing, and is bound to this determination. The ground for processing cannot be changed retrospectively when the chosen ground turns out to be unlawful or insufficient, for instance when consent turns out to be invalid. Besides the fact that Avast never declared any ground for the Processing Activities, which already amounts to a violation of the transparency requirement [34], only two of these legal grounds could potentially be used for the Processing Activities:

- prior consent for the processing provided by the data subject (article 6(1)(a) GDPR; article 8(a) DDPA),
- the legitimate interest of the controller or others (article 6(1)(f) GDPR; article 8(f) DDPA).

No valid consent

22. It is clear that Avast had not obtained valid consent for processing personal data in relation to Jumpshot's activities.

[33] https://forum.avast.com/index.php?topic=171725.0 https://blog.avast.com/2015/05/29/avast-data-drives-new-analytics-engine/.

[34] See here under, section c).

23. According to Avast's own statements, it only began implementing an "explicit opt-in choice for all new downloads of our AV" as of July 2019. It also stated that it was "*now also prompting our existing free users to make an opt-in or opt-out choice*" and that this process would "*be completed in February 2020.*" The statements show that from the start of Jumpshot's activities in 2015, up until the winding down of Jumpshot in early 2020, Avast provided the vast majority of users only with an opt-out option and those users were automatically opted-in until they chose otherwise.[35] Such opt-out does not constitute adequate (i.e. unambiguous, informed and freely given) consent for processing personal data under the GDPR.[36]

24. Furthermore, even in cases where some Avast customers were offered an opt-in consent option, such consent was not valid as it could not have been 'specific' nor 'informed' as is the requirement under the GDPR (article 4(11) and recitals 32, 42 and 43). For example, Jumpshot was the "primary clickstream data" source for Hitwise, a data provider to Oracle, Salesforce, Taboola and a large array of third party data marketplaces who subsequently systemically on-shared that data. Jumpshot may have ceased operations in January 2020, but Avast is responsible for the loss of control of its customer data that still exists – and is still being processed by third parties in the Adtech ecosphere.

No legitimate interest

25. Furthermore, Avast cannot rely on the legal ground that the processing was necessary for a legitimate interest, because the purpose of the processing at hand is neither legitimate, nor does it pass the balancing test as required under article 6(1)(f) GDPR and article 8(f) DDPA.

26. Obviously, Avast cannot use this legal basis for its processing, as it processed the data for the purpose of an illegitimate interest, i.e. making a profit out of secretly selling vast amounts of unlawfully obtained personal data, without (adequately) informing data subjects.[37]

27. Given the questionable, illegitimate interest that is served, the severity of the processing, the fact that the processing was unexpected and hidden for data subjects, and that no safeguards were provided, the interests of data subjects

[35] Avast Official statement on the recent news about privacy, 28 January 2019, https://forum.avast.com/index.php?topic=231828.msg1533674#msg1533674.

[36] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679. version 1.1, adopted on 4 May 2020, para. 3-5.

[37] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, para III.3.3-III.3.5; Opinion of the AG of 19 December 2018 in Case C-40/17 (*FashionID*), ECLI:EU:C:2018:1039, nr. 122.

clearly outweigh the interests of Avast, Jumpshot and the buyers or users of the data (i.e. Jumpshot's customers).

Conclusion

28. In the absence of a valid legal basis of processing, Avast's operations in connection with the Jumpshot activities violated article 6(1) GDPR.

(c) Non-compliance with the principle of fairness (article 5(1)(a) GDPR; article 6 DDPA)

29. The principle of fairness entails that personal data may not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject.[38]

30. The fact that Avast collected, analysed and sold vast volumes of personal data from its users for other purposes than the security of their device –*i.e.* for commercial gain- was hidden from them. By keeping it hidden and by preventing opting out of such processing, Avast prevented these data subjects from exercising control over the use of their data. Avast customers were not and could not be aware of the Processing Activities, nor could they restrict them. Moreover, Avast did not just hide the Processing Activities from its own customers, it actively misled them, and abused their trust by making them believe that Avast, as their online security vendor was using their personal data only for security purposes, when it was creating and exploiting an ongoing security vulnerability for themselves. [39] Avast exploited the needs and vulnerabilities of its customers and was complicit in subjecting them to detrimental or even discriminatory use of their data.

31. As a result, Avast's processing operations in connection with Jumpshot's activities did not comply with the principle of fairness of article 5(1)(a) GDPR and, before 25 May 2018, of article 6 DDPA.

(d) Non-compliance with the principle of purpose limitation (article 5(1)(b) GDPR; articles 7 and 9(1) DDPA)

32. In this case, Avast initially claimed to collect personal data for security purposes. Avast subsequently used this data for commercial and marketing purposes, and sold it to third parties. These so-called secondary purposes are very different from the primary purpose and not related or compatible with

[38] Recital 39 GDPR.

[39] We note that this behaviour is similar to the instance where Twitter was fined by the US Federal Trade Commission for using personal information (email addresses and telephone numbers) for alleged "two-stage authentication" whereas they were sold to Adtech participants to profile its users. https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

each other.[40] Further processing can only be lawful if it meets, inter alia, the reasonable expectations that the data subject had when their data was collected, considering the context in which this happened.[41] The data subjects were not informed about the processing for the secondary purposes, nor about the large scale of the processing and number of recipients involved, and therefore could not reasonably expect this further processing. Indeed, one could say they are incompatible because by knowingly sending the personal identifying information of customers and users to multiple intermediaries for onward transmission, Avast causes the very security vulnerabilities its customers were seeking to avoid when contracting with it for its security and anti-virus products. This means the processing was incompatible and thus unlawful.

33. Therefore, the Processing Activities in connection to the Jumpshot activities violated article 5(1)(b) GDPR and articles 7 and 9 DDPA.

(e) Non-compliance with the principle of data minimisation (article 5(1)(c) GDPR; articles 10 and 11(1) DDPA) and data protection by design and by default (article 25 GDPR; article 11(2) DDPA)

34. Avast's Jumpshot activities were focussed on collecting and selling a data subject's entire web browsing activity: "*Market smarter with consumer journey analytics. Examine every search, click, and buy. On every site*".[42] No efforts were taken to minimise the collected data. The design of the processing operation was aimed at collecting more, rather than less, personal data. Furthermore, users could only opt-out by changing the settings and actively disabling data sharing. Considering that the default setting was configured in a way that meant all data was collected, this amounts to a violation of article 25 GDPR.

35. Therefore, the Processing Activities in connection to the Jumpshot activities infringed the principle of data minimisation and the rules regarding privacy by design and default in violation of articles 5(1)c and 25 GDPR and article 11(1) DDPA.

(f) Non-compliance with the prohibition for processing special categories of personal data (article 9 GDPR; article 16 DDPA)

36. The datasets collected by Avast were comprehensive and included special categories of personal data or allowed such information to be derived from it.

---

[40] Recital 50 GDPR; WP29 Opinion 03/2013 on purpose limitation adopted on 2 April 2013, p. 21-23.

[41] WP29 Opinion 03/2013 on purpose limitation Adopted on 2 April 2013, p. 12.

[42] See the internet archive of the wayback-machine (https://web.archive.org/web/20191205215055/https://www.jumpshot.com/product/clickstream-data) e.g. captures of 05 December 2019 (last visited 25 August 2022).

For example, when a data subject used a search engine to investigate symptoms of an illness, health data would have been derived from the search results Avast collected.[43] Furthermore, recording visits to certain websites would demonstrate religious beliefs or sexual preferences.

37. There is no exemption that Avast could rely upon for the processing of such data, except from explicit consent (article 9(2)a GDPR; article 23(1)(a) DDPA). As indicated above, Avast did not obtain consent, let alone explicit consent.

38. Therefore, Avast's processing operations in connection to the Jumpshot activities also violated article 9 GDPR and article 16 DDPA.

(g) Non-compliance with the prohibition to transfer personal data to third countries (articles 44-49 GDPR, article 78 DDPA)

39. The Foundation is concerned that a US subsidiary, Jumpshot Inc., was processing the Avast Victims' data in the United States, in violation of the rules pertaining to the transfer of personal data from the EU/EEA to third countries outside the EU/EEA, including the United States. The Foundation wishes to receive information as to how this data transfer lawfully took place, particularly which transfer mechanisms were used under the DDPA and the GDPR respectively, how users were informed of such transfers and what was the legal basis for the data transfers.

OTHER VIOLATIONS

40. With respect to its conduct in connection to the Jumpshot activities, Avast not only violated the data protection rights of users under the GDPR, but also violated other provisions in Dutch and European Union Law, including:

a. Telecommunications law;

b. Consumer law (including rules regarding unfair commercial practices);

c. Criminal law.

41. In addition, the Processing Activities imply and result in unjustified enrichment ('*ongerechtvaardigde verrijking*') by Avast.

(a) Telecommunications law (article 11.7a DTA)

42. Article 11.7a DTA contains strict rules for the use of technologies for storing of information on, or accessing information from, the terminal equipment of an end user (i.e. the end user's PC, laptop, tablet or smartphone and the like). Pursuant to the article, the use of technologies is only allowed with the end user's consent and after they have been provided with information.

[43] CJEU 1 August 2022, C-184/20, ECLI:EU:C:2022:601.

43. For the purposes described above Avast installed software on its customers' and users' devices and read data from them without obtaining informed consent. The DTA therefore applies to Avast's activities and Avast should have obtained its customers informed consent for this installation. As discussed above, Avast failed to obtain informed consent and therefore violated article 11.7a DTA for each Avast Victim during the Relevant Period.

(b) Unfair commercial practices (articles 6:193a-6:193d DCC)

44. In addition, Avast violated the rules on unfair commercial practices, as regulated by articles 6:193a-6:193d DCC, which implements the Unfair Commercial Practices Directive.[44] Particularly, Avast omitted essential material information regarding the processing of personal data related to its products,[45] by failing to mention that personal data would not solely be used for security purposes but would also be used for marketing and commercial purposes. It can be assumed that many consumers would not have used the products if they had been informed of these activities. By failing to include the essential information, Avast violated article 6:193d DCC.

45. Another unfair practice is offering a product for "free" while it is in fact not free (article 6:193g(t) DCC). According to the European Commission personal data have an economic value. Avast was offering a product for free, while in fact it was letting the users pay by secretly collecting and exchanging their personal data from the users. This conduct constitutes an unfair commercial practice [46] and consequently Avast's actions also qualify as an unfair commercial practice within the meaning of article 6:193g(t) DCC.

(c) Criminal law

46. Furthermore, Avast violated the Dutch Criminal Code ("DCrC") as it unlawfully accessed its users' devices and unlawfully shared non-public data.

---

[44] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149 11.6.2005, p. 22, as amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJ L 328, 18.12.2019, p. 7–28.

[45] See the internet archive of the wayback-machine (https://web.archive.org/web/20190803204607/https://www.avast.com/privacy-policy) e.g. captures of 03 August 2019 (last visited 25 August 2022).

[46] EC UCP Guidance, p. 88-89. See also decision of the Italian Competition Authority: https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes.

47. Article 138ab DCrC penalizes unlawful access to a device or computer breach ('*computervredebreuk*'), which entails purposefully and unlawfully accessing an electronic exchange system. Accessing a system under false pretences constitutes such an unlawful breach. If the breach is motivated by (financial) gain, for either the offender himself or another, this is considered an aggravating circumstance and the punishment is increased.

48. Article 138c DCrC penalizes purposefully and unlawfully collecting or transferring non-public data ('*overnemen niet-openbare gegevens*'). Even when initial access to data is lawful, collecting or passing on data can be considered unlawful. If the breach is motivated by (financial) gain, for either the offender or another, this is considered an aggravating circumstance, constituting ground for increasing the sanction.

49. Avast accessed the personal data of its users under false pretences. Avast pretended to access and use the data (only) for security purposes, but in fact used the data for secondary commercial purposes and sold this data to multiple third parties.[47] Avast has unlawfully collected and transferred non-public data, for its own commercial gain. Avast has thereby violated articles 138ab and 138c DCrC.

UNLAWFUL ACT AND UNJUSTIFIED ENRICHMENT (ARTICLES 6:162 AND 6:212 DCC)

50. By the facts and circumstances and conduct described above and (amongst others) the above-mentioned Violations, Avast committed a tort pursuant to article 6:162 DCC. Avast clearly acted unlawfully by breaching the rights of its users, disregarding its statutory duties and acting in conflict with what is generally accepted according to unwritten law.

51. By the facts and circumstances and conduct described in this letter, Avast benefitted from unlawfully and illegally collecting data at the expense of its customers, without them being made aware of this business model. Therefore, pursuant to article 6:212 (1) DCC, Avast has a duty to compensate its users for damages up to the amount of the enrichment (i.e. the value of the data it illegally collected and the profits it gained by commercially exploiting that data).

CLAIM FOR DAMAGES

52. The Foundation represents the interests of the Avast Victims (i.e. Dutch residents that have been the victim of the Violations). Avast claims to have

[47] Leaked Documents Expose the Secretive Market for Your Web Browsing Data, Motherboard 27 January 2020, https://www.vice.com/en/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation.

more than one million users in the Netherlands.[48] These users have suffered damages as a result of these Violations. Pursuant to article 82 GDPR and/or article 6:162 DCC, Avast is liable for any and all material and non-material damages suffered in relation to the Violations. The affected persons have the right to receive "*full and effective*" compensation and in this context the concept of damage must be interpreted broadly (recital 146 GDPR). The statutory liability includes the right to equitable relief ('*een naar billijkheid vast te stellen schadevergoeding*').

53. The Violations are substantial and serious. As set out in this letter, Avast violated core principles of inter alia the GDPR, DDPA, DTW and DCC, and consequently committed a tort and unjustifiably enriched itself, resulting in distress and serious and substantial damages for its customers. Many of the Avast Victims were security-conscious individuals, and Avast went to great lengths to advertise its products as a means to protect its customers, and indeed their children, whose browsing behaviour and other personal information was then collected and sold to third parties.

54. The damages caused by Avast are irreversible. A large volume of personal data of its customers has been collected and sold to numerous companies for commercial purposes over a significant period of time. In view of the nature, duration and severity of the Violations this constitutes an actual loss of control over that personal data, which obviously cannot be undone. In this regard, it is relevant that Avast played a key role in broader large scale data trading and profiling, and processes the data of vulnerable persons, such as minors. Furthermore, it is relevant that the illegal and unlawful data processing took place continuously during at least half a decade, and (allegedly) ended only after much controversy in 2020.

55. On behalf of the Foundation and for the purpose of the Avast Victims, we hereby:

- hold Avast Software s.r.o., Avast Plc., Avast Holding B.V., Avast Software B.V., AVG Ecommerce CY B.V., Jumpshot, Inc. and Avast Software, Inc. liable for all damages suffered by the Avast Victims as a consequence of the Violations of the GDPR, TCA, DCC and the DCrC;
- demand payment from Avast Software s.r.o. Avast Plc., Avast Holding B.V., Avast Software B.V., AVG Ecommerce CY B.V., Jumpshot, Inc. and Avast Software, Inc. of compensation for all damages suffered by the Avast Victims;

[48] https://investors.avast.com/media/1228/analyst-presentation-5-july-f.pdf.

- unequivocally reserve all rights and claims against Avast Software s.r.o.., Avast Plc., Avast Holding B.V., Avast Software B.V., AVG Ecommerce CY B.V., Jumpshot, Inc. and Avast Software, Inc. and any other organization within the Avast group of companies with regard to its conduct concerning Avast products and services, in particular with regard to the facts described in this letter and including but not limited to those rights and claims resulting from the Violations, and interrupts any statute of limitation currently accruing in respect of any of these rights and claims on behalf of or for the purpose of the Avast Victims and the Foundation itself.

56. Without any timely substantiated response to this letter proving otherwise, we assume that Avast Software s.r.o., Avast Plc., Avast Holding B.V., Avast Software B.V., AVG Ecommerce CY B.V. and Avast Software, Inc. are all involved in and responsible for the Violations described above and accountable for all damages caused by these Violations.

57. Please note that the Foundation acts on behalf of all persons affected which have or had habitual residence in the Netherlands (the Avast Victims) on the legal grounds of its competence as a class action legal entity pursuant to article 3:305a DCC. Moreover, the Foundation will also be entitled to claim damages and other forms of redress before a Dutch Court pursuant to – inter alia – articles 79(2) and 80 GDPR.

REQUEST FOR PRESERVATION OF EVIDENCE AND DISCLOSURE

58. During its further investigations in relation to this litigation and/or related litigation, the Foundation may seek disclosure pursuant to article 843a Dutch Code of Civil Procedure ("**DCCP**") or the applicable disclosure regimes in the EU and the United States of further relevant data in the possession of Avast. Avast is required to inform the court truthfully and to provide evidence when obliged to do so pursuant to articles 21 and 22 DCCP and therefore, we request that Avast cease all routine and/or merger-related deletion and further clean-up actions with respect to the Avast Victims' data as part of its ongoing operations. In order to enable the Foundation to further review and assess the Violations, it requests, and to the extent necessary it summons Avast, within 10 working days as of the date of this letter to (a) confirm that it will preserve and not delete and (b) provide the following information:

1. A full list of all products and services affected by the Violations, and over what exact period of time.

2. An exact breakdown of the schema of the data collected, how it was processed and where it was stored.

3. An exact count of the number of Dutch (former) residents affected.
4. A list of all Jumpshot customers that received user data, and over what periods of time.
5. All data sharing agreements with customers, so we can understand what restrictions were placed on those customers regarding the personal data.
6. Disclosure on what personal data Avast still has a copy of.
7. An account of revenue and profits generated from the Violations described.
8. The basis for EU-US data sharing.

59. In addition, the Foundation requests Avast to inform whether it has undertaken to the Czech DPA to keep all relevant records available during any pending or completed investigations into Avast's business practices in the context of the investigation in relation to the Violations or otherwise, and if so, whether such notification or statement applies to all data subjects involved within the European Union and the European Economic Area or to data subjects in the Czech Republic only.

60. We assume you will be notifying the Czech office for Personal Data Protection regarding this letter and request Avast to confirm this in writing to the undersigned.

THE NORTONLIFELOCK MERGER

61. The Foundation notes that Avast's proposed merger with Nortonlifelock, Inc. has been provisionally approved by the UK Competition and Markets Authority. The Foundation is concerned on behalf of or for the purpose of the Avast Victims about the sharing of unlawfully obtained customer data with Nortonlifelock, Inc. both as part of the due diligence process for this merger and ultimately under the merger itself, should it proceed to closing.

62. The Foundation therefore seeks assurances that this has not and will not take place, as well as apply for injunctive relief in relation to the same. The Foundation believes that it would be inappropriate that any value ascribed to Avast's admitted, systemic and unlawful behaviour that resulted in the Violations should rightfully belong to the Avast Victims and not flow to the shareholders of NortonLifelock, Inc. To this end, the Foundation requests, and to the extent necessary it summons Avast, within 10 working days as of the date of this letter to confirm that it will provide:

- the country location(s) and specific addresses of the legal entities NortonLifelock, Inc. that are proposed to hold and control the

personal data of the Avast Victims obtained as a result of the Violations;

- the actual or planned transfer date of any personal data of the Avast Victims from Avast to NortonLifelock, Inc.

63. Furthermore, the Foundation has serious reasons to believe that Avast will transfer personal data of Avast customers and users to the United States as part of the merger of Avast and NortonLifelock, Inc. Also with respect to this transfer the Foundation would therefore like to urgently receive details of the same to ensure that any transfer will be in accordance with all applicable laws and regulations. We assume that NortonLifelock, Inc. is aware of its obligations with respect to the same in the context of the merger and the due diligence relating to the same. We kindly ask you to confirm that the GDPR will be complied with.

INVITATION TO ENTER INTO NEGOTIATIONS

64. The Foundation primarily intends to resolve this matter amicably through settlement negotiations and therefore requests the entities addressed by this letter to enter into settlement discussions (article 3:305a (3)(c) DCC (recast)). On behalf of the Foundation, we hereby cordially invite Avast to enter into good faith negotiations with the Foundation regarding a fair compensation of damages.

65. The Foundation's legal status also enables it to seek enforcement before a Dutch Court pursuant to articles 79(2) and 80 GDPR. We draw your attention to the Dutch Act on the Collective Settlement of Mass Claims ('*Wet afwikkeling massaschade in collectieve actie'* or "WAMCA"), pursuant to which a settlement can be achieved that has binding effect on the individuals whose interests the Foundation aims to protect, unless they opt out. This act further allows a settlement beyond the Netherlands-based 'class' and, as such, can provide 'global peace' for Avast if and when a solution offered to Netherlands-based data subjects extends to individuals in other jurisdictions. This act has already proven successful in other large international settlements with very low opt-out percentages.

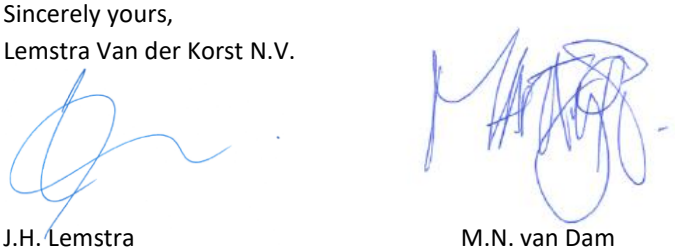
66. Obviously, this letter is without prejudice to the Foundation's and Avast Victims' rights and remedies, all of which are expressly reserved. In this respect, all rights are reserved and without limitation to the generality of the foregoing, the Foundation expressly reserves its rights to file a complaint with the relevant Czech, Dutch and other relevant European Data Protection Authorities, both in relation to the Violations and otherwise.

67. If Avast is willing to engage in settlement discussions as stated above, please confirm so by 20 September 2022 via e-mail to j.lemstra@lvdk.com and m.vandam@lvdk.com. Absent a timely, positive and meaningful response, the Foundation will serve a writ of summons upon Avast without further notice.

The Foundation reserves all rights and interrupts/tolls any statute of limitations ('*stuiting van de verjaring*') under any applicable law, including but not limited to Dutch law (article 3:317 DCC).

In order to ensure that you receive this letter in due time, we are sending you a copy both by e-mail and by registered mail.

Sincerely yours,
Lemstra Van der Korst N.V.



J.H. Lemstra M.N. van Dam