REGISTERED MAIL
Palantir Technologies Inc.
Attention: Legal Department
100 Hamilton Ave., Suite 300
Palo Alto, CA 94301

Draft: November 18, 2020
Our ref.: SOMI / PALANTIR
Your ref.: -

Dear Sir or Madam,

On behalf of the Foundation for Market Information Research (hereinafter: '**SOMI**'), we are hereby submitting a complaint letter regarding your organization (Palantir Technologies Inc., hereinafter: '**Palantir**'). The complaint relates to the lack of transparency surrounding Palantir software and data processing practices, as well as Palantir's potential conflict of interest with the EU member states. Since November 16, 2020, European consumers have participated in this initiative and authorized SOMI to exercise their rights accordingly with the GDPR and European laws, in relation to your company.

Before formulating and further explaining this complaint, I will first provide below additional information on SOMI and the identified practices of Palantir.

SOMI

1. SOMI is a knowledge center and think tank as well as a consumer representative organization. With its advocacy, SOMI contributes to data security and privacy protection for all European citizens.

2. So far, over 10,000 participants have registered with SOMI to be inform about their digital rights and have their interests represented. These individuals have become victims of privacy violations by Palantir as a result of the following practices.

Palantir practices

3. It was revealed that since 2016, Europol has been using Palantir 'Gotham' software for operational analysis in an anti-terrorism task force[1]. This raises concern among members of the European Parliament, such as the Dutch MP Sophie in 't Veld, who questions the risk of data processed by Palantir[2].

> *"Does the commission […] consider a company with the track record of Palantir, and subject to US jurisdiction, an appropriate partner for the European Union and suitable to be entrusted with the most sensitive personal data of European citizens*[3]

[1] https://www.europarl.europa.eu/doceo/document/E-9-2020-000173-ASW_EN.html
[2] https://www.euractiv.com/section/digital/news/eu-commission-pressed-on-controversial-links-to-palantir/
[3] https://www.euractiv.com/wp-content/uploads/sites/2/2020/06/2020.06.10-Letter-to-Commission-Palantir.pdf

4. Other European clients of Palantir include the French intelligence agency DGSI[4], the Danish national police[5], German police in Hesse and North Rhine-Westphalia[6] and the Netherlands police[7]. Neither Palantir nor agencies that use it are willing to share information about the nature and extent of these and other collaborations.

5. In spite of Palantir having made a record in the transparency register with the European Commission, no records appear to have been kept of the meetings between President von der Leyen and Mr. Alex Karp as CEO of Palantir, most notably, but not limited to, the one during the World Economic Forum in Davos on 22 January 2020[8].

6. SOMI demand transparency from Palantir and agencies who employ the service of Palantir either through the company itself, or its sub-contractors. The public needs to know about the effectiveness of the Palantir software, the amount of information it is collecting, who has the capabilities to analyze the data, and the extent of its access to sensitive information.

Palantir's close ties with the US government and intelligence agencies.

7. Palantir has never masked its ambitions to provide its services to the US government[9]. Not only Palantir got on its feet with CIA funding, it has been reported that Palantir has also worked domestically for US law enforcement and intelligence agencies such as NSA, FBI, Department of Defense, Marine Corps[10].

8. Moreover, as a US company, Palantir is subject to US jurisdiction in all aspects of doing business, including being subjected to the notorious "Foreign Intelligence Surveillance Act" (FISA). That means that all information on non-US citizens to which Palantir can gain access, must be shared with US intelligence service, if warranted[11].

9. This raises concern about the fact that Palantir has access to large numbers of databases filled with sensitive information about citizens and businesses within the European Union. Given the sensitive nature of the data it processes, such information could be used to target and discriminate European citizens and, thus, compromise the national security of the European member states.

Palantir's intellectual property and data ownership dispute

10. As early as 2017, the New York Police Department (NYPD) has been in a dispute with Palantir over access to analytic data the company produced[12]. The lawsuit stems from NYPD's plans to cancel its contract with Palantir as NYPD was transitioning to

[4] https://www.bfmtv.com/tech/cyberdefense-la-france-peut-elle-couper-les-ponts-avec-palantir_AN-201809290009.html
[5] https://edri.org/our-work/new-legal-framework-for-predictive-policing-in-denmark/
[6] https://digit.site36.net/2020/06/11/europol-uses-palantir/
[7] https://fd.nl/achtergrond/1359235/geen-belegger-weet-wat-databedrijf-palantir-eigenlijk-doet
[8] https://www.euractiv.com/section/data-protection/news/commission-kept-no-records-on-davos-meeting-between-von-der-leyen-and-palantir-ceo/
[9] https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/
[10] https://www.businessinsider.nl/palantir-ice-explainer-data-startup-2019-7/
[11] https://edri.org/our-work/german-big-brother-awards-one-winner-reacts-and-appears/
[12] https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency

software from another company. According to Buzzfeednews, Palantir has declined to hand over a readable version of the data to the NYPD, claiming that doing so would threaten its intellectual property[13].

11. A larger problem that subsequently arises is that datasets of greatest interest to government agencies may no longer government-owned or produced. Instead of being owned and managed by European agencies, they would since then be created and owned by a US-listed company, which has financial incentive over the ownership of data, specifically, when this would endanger the interests of their shareholders, management executives or strategic clients. Such conflict of interest may include prolonging security threats for financial reasons, instead of preventing them.

Several reports of the problems with Palantir software, including exposing sensitive data.

12. In 2013, Joint Regional Intelligence Center (JRIC) was tasked with tracking down an ex-LAPD officer who had embarked on a series of shootings targeting law enforcement officers. "We used Palantir extensively to address that [and] were active 24/7 until he was caught or killed," according to Sergeant Peter Jackson from JRIC "We found that processing clues was a big challenge."[14] In fact, on two separate occasions, it was reported that police shot at trucks misidentified as belonging to suspect, injuring three civilians[15].

13. In 2014, a police officer in the Long Beach drug squad marked a case confidential in the Palantir data analysis system. He expected key details to remain hidden from unauthorized users. This is important because it often involves protecting witnesses or undercover officers or keeping upcoming operations secret. Yet not long after, another officer working in different division ran a car license plate mentioned in his case and was able to read the entire confidential file[16].

14. Other reports that disqualify Palantir include "spiraling prices, hard-to-use software, opaque terms of service, and failure to deliver products".[17]

Palantir conducts that does not align with the European values.

15. In comparison to the US, the EU investigates, interprets, acts and judges differently with regard to fundamental principles of law and the rights of individual citizens, in particular including equal treatment and the presumption of innocence.

16. We believe Palantir may strongly emphasize discrimination and bias regarding race or ethnicity, political opinions and religious beliefs. In the US, Palantir software was used to a tool to target vulnerable communities[18], demonstrating the company's lack of principles in privacy and human rights.

---

[13] https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley
[14] https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/
[15] https://www.ocregister.com/2013/02/08/police-confuse-truck-for-dorners-shoot-at-3-in-torrance/
[16] https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/
[17] https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/
[18] https://futurism.com/lapd-documents-show-their-policing-algorithms-continue-to-target-minorities-and-past-offenders

17. These considerations of SOMI may be shared or may have been shared over the years by many human rights organizations that have explicitly questioned Palantir's actions, including Privacy International, Open Rights Group, Big Brother Watch, medConfidential, Foxglove[19], No Tech For Tyrants[20] and Amnesty.

Lack of transparency as to how Palantir's software works

18. Until now, no substantial information has been made available to the public on how Palantir's software exactly works, who is using it, and what their problems are or may be with it in the future. Even more importantly, with regards to the use of algorithms and the transport and sharing of sensitive data to jurisdictions outside the EU, as well as with regard to its compliance to applicable European standards and principles, no information, explanation or accountability if any, has been made available to the public.

19. European citizens deserve transparency from their governments as well as their government (sub-)contractors in public-private partnerships, in particular with regard to its effects on their legal rights. "The inability of EU citizens to review and debate the EU's dealings with a highly controversial actor like Palantir makes a mockery of the EU's commitment to transparency and only further reinforces the company's shadowy reputation."[22]

Complaint

20. These practices prompt SOMI and its participants to file this complaint. The complaint is that Palantir has violated the privacy of European citizens in numerous ways. We believe Palantir software violates several articles of the General Data Protection Regulation ('**GDPR**', under Dutch legislation: AVG). These applicable articles of the GDPR are listed below, with an indication as to how they have been possibly violated by Palantir.

Breach of Article 5 GDPR – *Principles relating to the process of personal data*

21. In accordance with the Article 5 GDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It shall only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

22. While Palantir claims that clients remain in control of their data, the reports in fact show that Palantir strives to convince its clients to share data in anonymized format, in order to improve its offering towards all other customers[23]. This action is in direct

[19] https://privacyinternational.org/press-release/3732/press-release-10-questions-palantir-privacy-organisations
[20] https://notechfortyrants.org/2020/10/22/whos-behind-palantir-uk-feat-what-are-they-doing-on-your-campus-report-supplement/
[21] https://www.amnestyusa.org/press-releases/palantirs-contracts-with-ice-raise-human-rights-concerns-around-direct-listing/
[22] https://notechfortyrants.org/2020/07/14/notechfor-eu/
[23] https://algorithmwatch.org/en/story/palantir-the-secretive-data-behemoth-linked-to-the-trump-administration-expands-into-europe/#:~:text=While%20Palantir%20claims%20that%20clients,its%20offering%20towards%20all%20customers.&text=Palantir%20refused%20to%20release%20the,holding%20it%20de%20facto%20hostage.

23. violation to the principles of purpose limitation and data minimization as according to the GDPR.

24. Moreover, due to the lack of transparency surrounding Palantir's practices, it is unclear whether its data has been processed in a manner that ensures appropriate security of the personal data or whether this data is still accurate or up to date.

Breach of Article 9 GDPR – *Processing of special categories of personal data*

25. Article 9 GDPR requires suitable measures to be implemented when processing special categories of personal data, including related to racial or ethnic origin, political opinions, religious beliefs, trade union membership as well as genetic, biometric, health or sexual orientation information.

26. The aforementioned reports of the problems with Palantir software illustrate that there is reason to suspect that Palantir has been failing to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, possibly resulting in quite sensitive data being exposed.[24]

Breach of Article 13 GDPR – *Information to be provided where personal data were collected from the data subject*

27. The controller should provide the data subject with information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data are processed.

28. As Palantirs' data processing includes data from social media, for instance, we believe the data subject most likely has not been informed or made aware of such processing.[25] According to Article 13 GDPR, where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences where he or she does not provide such data.

29. Moreover, the GDPR dictates that in case of profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequence of such processing, should be available to the data subject when the data is collected and when the data subject requests further information.

30. Up to this date, Palantir never release any meaningful information regarding the logic behind its software, how it works, what results it delivers and how the company advises on processing, evaluating and appreciating such results. The only information available to the public so far originated leaked documents and statements from whistleblowers.

Breach of Article 22 GPDR – *Automated individual decision-making, including profiling*

[24] https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/
[25] https://www.vox.com/recode/2020/7/16/21323458/palantir-ipo-hhs-protect-peter-thiel-cia-intelligence

31. In accordance to Article 22 GDPR, suitable measures must be implemented when processing special categories of personal data in order to safeguard the data subject's rights and freedoms and legitimate interests.

32. As mentioned before, we suspect that Palantir did not take any suitable measures to process special categories of personal data in pursuant to Article 9 GDPR.

Conclusion complaint

33. In view of all of the above, SOMI believes there have been and still are ongoing violations by Palantir of privacy rights and corresponding GDPR breaches.

Completion

34. On behalf of SOMI and all of its participants, I hereby request you to process this complaint and to inform us accordingly about the receipt of this complaint and how Palantir intents to handle it. We would also like to be informed on the earliest date, ultimately within 5 working days after receiving this letter, when Palantir will materially respond to the complaint.

Your sincerely,

Mr. drs. H.J.M.G. Franke

Stichting Onderzoek Marktinformatie

Dr. C.A.M. Wijtvliet

Stichting Onderzoek Marktinformatie