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

Also per e-mail: privacy@palantir.com

Draft: December 17th, 2020
Our ref.: SOMI / PALANTIR
Your ref.: -

Dear Sir or Madam,

On behalf of Stichting Onderzoek Marktinformatie (translated to the 'Foundation for Market Information Research', hereinafter: '**SOMI**'), we hereby submit the following complaint letter regarding Palantir Technologies Inc. (hereinafter: '**Palantir**'). The complaint relates to several violations of the European Convention on Human Rights (hereinafter: '**ECHR**'), the General Data Protection Regulation (hereinafter: '**GDPR**') as well as a potential conflict of interest with the EU member states.

SOMI

1. SOMI is a knowledge center, think tank and consumer representative foundation that focuses on data security and privacy protection for all European citizens.

2. So far, over 10,000 participants have registered with SOMI to be informed about their digital rights and have their interests represented. They have authorized SOMI to act against the violation of their rights by Palantir, as described below, and to exercise the rights granted to them by the GDPR and other European laws.

The role of Palantir in the EU

3. Palantir is described as a controversial and secretive company that focuses on big data and data mining to provide services to government agencies and commercial corporations. Its tools are primarily aimed at surveillance and security and often involve the processing of large amounts of extremely sensitive or proprietary data.[1]

4. It was revealed that since 2016, Europol has been using the 'Palantir Gotham' software for operational analysis in an anti-terrorism task force.[2] This raised 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:[3]

[1] https://www.forbes.com/sites/bethkindig/2020/09/29/palantir-ipo-deep-dive-analysis/
[2] https://www.europarl.europa.eu/doceo/document/E-9-2020-000173-ASW_EN.html
[3] https://www.euractiv.com/section/digital/news/eu-commission-pressed-on-controversial-links-to-palantir/

"*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?*"[4]

5. Other European clients of Palantir include the French intelligence agency DGSI, the Danish national police, German police in Hesse and North Rhine-Westphalia[5], the Dutch police[6] as well as civic EU-institutions.[7] Neither Palantir nor agencies that use it are willing to share information about the nature and extent of these and other collaborations, but the use of Palantir software by these agencies remains controversial.

6. With its recent initial public offering (hereinafter: '**IPO**'), Palantir also aims to expand its horizon and attract more commercial corporations as clients. Currently Palantir already has some of Europe's biggest corporations as clients, such as Airbus, BP, Ferrari and Merck.[8] This list is only bound to grow due to the increased exposure following the IPO and the increased focus of corporations on big data.

Discrimination and bias in Palantir search algorithms

7. Palantir's software can have a significant impact on the European society and may lead to violations of basic human rights. Palantir's search algorithm facilitates discrimination and contains a bias regarding certain races or ethnicities, political opinions and religious beliefs. In the US, the use of Palantir software has already resulted in racial profiling and targeting of vulnerable communities.[9] Another example, is the role Palantir played in the deportation of immigrants by the ICE in the US and the separation of immigrant families.[10] This does not only show a lack of principles, it also constitutes a clear violation of article 14 ECHR, which prohibits discrimination on any ground, including race, religion and national origin.

8. Where other technology companies refuse morally rejectable contracts, Palantir seems the prioritize its relationship with the US government. Palantir's CEO, Alex Karp, has demonstrated this by claiming Google took a 'loser' position when Google ended its AI contract with the Pentagon because it could be used for lethal purposes,[11] as well as by its stance in the ICE discussion and its fear to damage its reputation with the US government.

[4] https://www.euractiv.com/wp-content/uploads/sites/2/2020/06/2020.06.10-Letter-to-Commission-Palantir.pdf
[5] https://digit.site36.net/2020/06/11/europol-uses-palantir/
[6] https://fd.nl/achtergrond/1359235/geen-belegger-weet-wat-databedrijf-palantir-eigenlijk-doet
[7] https://algorithmwatch.org/en/story/palantir-the-secretive-data-behemoth-linked-to-the-trump-administration-expands-into-europe
[8] https://www.sec.gov/Archives/edgar/data/1321655/000119312520230013/d904406ds1.htm (p. 162-163)
[9] https://futurism.com/lapd-documents-show-their-policing-algorithms-continue-to-target-minorities-and-past-offenders
[10] https://www.vice.com/en/article/pkeg99/palantirs-ceo-finally-admits-to-helping-ice-deport-undocumented-immigrants
[11] https://www.forbes.com/sites/bethkindig/2020/09/29/palantir-ipo-deep-dive-analysis/

9. It is also important to realize that Palantir is designed from the perspective of the US justice system. The EU justice system is, however, completely different and 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.

10. These considerations of SOMI are shared by many human rights organizations that have explicitly questioned Palantir's actions, including Privacy International, Open Rights Group, Big Brother Watch, medConfidential, Foxglove, No Tech For Tyrants and Amnesty International.[12]

Lack of transparency

11. Until now, no substantial information has been made available to the public on how Palantir's software exactly works, who is using it, what it is used for, how it handles sharing of sensitive data to non-EU jurisdictions and its compliance to applicable European laws, standards and principles.

12. European citizens are entitled to transparency from their governments as well as their government (sub-)contractors in public-private partnerships, in particular regarding its effects on their legal rights. The lack of transparency makes it virtually impossible to hold Palantir or its clients, accountable for their actions.

13. The obligation to process personal data in a transparent manner is laid down in article 5 GDPR. Articles 13 and 14 GDPR specify this obligation by stating that companies and authorities must inform data subjects of the personal data they process, the processing grounds etc. to ensure fair and transparent processing. Such information has never been provided by Palantir or its clients, who therefore are in breach of articles 5, 13 and 14 GDPR. For example, Palantir uses web-scraping tools and processes data from social media without informing the data subject or making them aware of such processing.[25]

14. It is also a well-known fact that Palantir builds profiles of data subjects for government authorities. Article 22 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.

15. Up to this date, Palantir never released any meaningful information regarding the logic behind its software, how it works, what results it delivers and how the company evaluates and appreciates such results. The only information available to the public so far, originates from leaked documents and statements from whistleblowers.

[12] https://privacyinternational.org/press-release/3732/press-release-10-questions-palantir-privacy-organisations, https://notechfortyrants.org/2020/10/22/whos-behind-palantir-uk-feat-what-are-they-doing-on-your-campus-report-supplement/, https://www.amnestyusa.org/wp-content/uploads/2020/09/Amnest-International-Palantir-Briefing-Report-092520_Final.pdf

Illegitimate processing and privacy violations

16. According to article 5 GDPR, personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with these purposes.

17. The principle of legitimate processing is further specified in articles 6 and 9 GDPR, which require legitimate grounds for processing personal data. Palantir or its clients never showed its processing grounds and based on the examples as mentioned above, SOMI concludes that Palantir has no lawful processing grounds for a lot of its processing activities.

18. For example, article 9 GDPR considers racial information and information about someone's religion a special category of personal data. Processing of such data is, in principle, forbidden. Palantir never demonstrated one of the exceptions as mentioned in article 9 GDPR to apply to its processing and therefore is already in violation of article 9 GDPR. SOMI also believes such exceptions cannot be reasonably applied to the large-scale processing of special categories of data by Palantir. European case law shows that reasons of substantial public interest (i.e. security) do not provide sufficient ground for unchecked large-scale processing of special categories of personal data. The processing must be proportionate to the aim pursued.[13]

19. Besides a breach of the GDPR, the large-scale processing of (special categories of) personal data and the lack of transparency also constitute a violation of article 8 ECHR. This article states the right to privacy and there is extensive case law by the European Court of Human Rights on the use of untransparent surveillance tools and big data by state and police authorities.[14]

Illegitimate transfer of personal data to the US

20. In the recent Schrems II decision, the European Court of Justice (hereinafter: '**ECJ**') invalidated the EU-US privacy shield for sharing personal data between EU and US entities, because the treaty provided insufficient safeguards against the "Foreign Intelligence Surveillance Act" (hereinafter: '**FISA**'). FISA means that, if warranted, all information on non-US citizens to which a US company can gain access, must be shared with US intelligence service.[15] In its decision, the ECJ made clear that the transfer of personal data to the US is not allowed without providing additional safeguards against unwanted interference from the US government.

21. As a US company, Palantir is subject to FISA. However, safeguards against unwanted interference from the US government have never been demonstrated by Palantir or its clients. Sharing personal data of EU data subjects with Palantir, therefore results in a violation of article 44 GDPR and undermines the GDPR.

[13] https://www.echr.coe.int/documents/guide_art_8_eng.pdf p. 49 -51.
[14] https://www.echr.coe.int/documents/guide_art_8_eng.pdf p. 49 -51.
[15] https://edri.org/our-work/german-big-brother-awards-one-winner-reacts-and-appears/

22. It is also important to note that Palantir has never masked its ambitions to provide its services to the US government.[16] In its early stages, Palantir has received significant funding from the CIA and it has been acknowledged that Palantir's most important customers are US law enforcement and intelligence agencies, such as the CIA, NSA, FBI, Department of Defense and Marine Corps.[17] What Palantir fears most, is that the US authorities consider Palantir an unreliable partner, as demonstrated by Palantir's fear of cancelling its infamous ICE-contract (see par. 8).[18] It is therefore likely that Palantir will easily share any data about EU data subjects with the US government, even without permission of its EU clients.

23. This is concerning as Palantir has access to large amounts of data and databases, filled with extremely sensitive and proprietary information about citizens and businesses within the EU. This information could be used to target, investigate and potentially discriminate European citizens and, thus, compromise the national security of EU member states.

Risk of losing ownership of sensitive and proprietary data

24. Once an agency or corporation gives Palantir access to their data, they are at risk of losing ownership of that data. The New York Police Department (NYPD) has already experienced this when they planned to cancel their contract with Palantir and asked for a readable version of the analytical data produced with the Palantir software. Palantir refused this request, claiming that sharing such data would threaten their intellectual property.[19]

25. A problem that subsequently arises is that extremely sensitive and proprietary datasets provided by government agencies, may no longer be 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 and has different interests compared to government agencies. The interests of Palantir are among others the interests of their shareholders, management executives and strategic clients, whereas the government's interest is the public interest.

26. Another risk to lose data lies in insufficient security measures to protect the data processed by Palantir. Article 32 GDPR requires appropriate measures to be implemented when processing personal data. There have been news reports of Palantir failing to provide such appropriate measures to protect personal data, for example a confidential police case being available for a prolonged duration to employees that should not have access to that case.[20]

[16] https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/
[17] https://www.businessinsider.nl/palantir-ice-explainer-data-startup-2019-7/
[18] https://www.nytimes.com/interactive/2020/10/21/magazine/palantir-alex-karp.html
[19] https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley
[20] https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/

Concluding

27. In view of all the above, SOMI concludes that Palantir violated and continues to violate various human rights as well as rights and obligations stated in the GDPR.

28. SOMI demands transparency from Palantir and agencies and corporations 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 collects, who analyses the data and the extent of its access to sensitive information.

29. On behalf of SOMI and all of its participants, we hereby summon you to:
    a. inform us of the receipt of this complaint and when Palantir will provide a substantive response to the complaint, within 5 working days after receipt of this complaint, and;
    b. inform us how Palantir intends to adequately resolve its violations of human rights and the GDPR.

    Failure to comply with our demands in a timely matter, will result in official complaints with European data protection authorities and possible further legal action.

Subject to all rights.

Your sincerely,

Drs. H.J.M.G. Franke LL.M	Dr. C.A.M. Wijtvliet
Stichting Onderzoek Marktinformatie	Stichting Onderzoek Marktinformatie