DROP PALANTIR

An open letter from civil society to the World Food Programme on its partnership with Palantir Technologies

September 2026

To: Luke J. Lindberg, Executive Director, World Food Programme

Cc: Members of the WFP Executive Board; António Guterres, UN Secretary-General; Qu Dongyu, Director-General, Food and Agriculture Organization of the United Nations; Committee on World Food Security (CFS)

Dear Mr Lindberg,

We, the undersigned civil society organizations, digital rights advocates, humanitarian workers, food sovereignty activists, trade unions, researchers, and concerned citizens, call upon the World Food Programme (WFP) to end its partnership with Palantir Technologies. The WFP should withdraw from the contract with Palantir – renewed for a further five years this July – and commission a fully independent and public review of the partnership, as well as all partnerships with technology companies. We invite the WFP to put in place a concrete, time-bound plan to transition away from Palantir altogether, incorporating appropriate public accountability mechanisms to prevent the ethical and operational risks arising from partnerships with technology companies. We further urge the WFP to embrace technology and data infrastructural choices that are aligned with the ethos of public governance, and rooted in human rights and public interest.

Palantir Technologies is a US data-analytics company co-founded in 2003 by Peter Thiel and Alex Karp, and is today a major technology company. It received early seed funding from the CIA's venture arm, In-Q-Tel. Its business model rests on embedding its proprietary software platforms deep inside a client's operations through long-term contracts that create a dependency on Palantir's own engineers to keep systems running. Company leadership, notably CEO Alex Karp, has fiercely

advocated for a "moral debt" that he claims American tech companies owe to the United States, explicitly stating that the mission of his company is to “give an unfair advantage to America”.

This brazen allegiance of Palantir to the geopolitical power of the US is enough to give pause to any institution handing the company access to sensitive data.

Palantir’s financial structuring, and its importance to the US state apparatus, has also allowed it to engage in large-scale tax avoidance and cross-border value transfer: an analysis of its finances shows that Palantir achieved an effective global tax rate of just 1.4% in 2025, paying $22.7 million on $1.657 billion pre-tax profits. The company paid zero US federal income tax.

The WFP's relationship with Palantir began with a pilot in 2017, which turned into a ‘*pro bono*’ agreement reported to be worth around $45 million in 2019. According to data available on the United Nations Global Marketplace portal, the WFP has also contracted Palantir $2.5 million in related support between 2017 and 2024. Built on Palantir's Foundry platform, the WFP's Digital Operations and Transformation System (DOTS) is now embedded across the large majority of the WFP's global logistics and supply-chain operations. A leaked internal audit by the WFP's own Office of the Inspector General, dated August 2025, rated the partnership's privacy and risk-management failures “high priority”, and found that “key privacy concerns raised by both internal and external stakeholders regarding the use of DOTS have not been adequately addressed” since the partnership began. Rather than pause to address these findings, the WFP is renewing and expanding the relationship.

We believe that the partnership should end now, and exhort the WFP to take immediate actions to uphold its own mandate and the public interest. Our concerns include the following aspects:

1. The Palantir partnership contradicts the WFP's own mandate

Palantir's largest and most consequential customers are the US military, intelligence agencies, and immigration enforcement. The company has a long-standing role supporting US Immigration and Customs Enforcement's operations, and it entered into a formal strategic partnership with Israel's Ministry of Defense in January 2024. Human rights organizations and UN experts have raised serious concerns, including corporate complicity in war crimes and the role of military and surveillance technology providers in Gaza. Given this profile and proximity to a single member state's military and enforcement apparatus, Palantir is a poor fit to hold the data backbone of the world's largest humanitarian agency whose mandate is based on international human rights and humanitarian law frameworks. The WFP’s credibility depends on its actual and perceived independence and impartiality. In fact, the WFP's own guidelines, and the wider UN system's commitments on digital human rights, exist precisely to prevent such transgression.

2. The Palantir partnership poses a high risk for human rights and territorial sovereignty

The areas where the WFP works — including active conflict zones, displacement crises and famine-affected regions — are the very sites in which the US government has direct military and strategic interests. Civil society worldwide and even allied governments are citing risks that Palantir poses with regard to national sovereignty. Furthermore, granular data about population movement or food supply logistics in locations with vulnerable populations carries potential risks to their civic-political and socio-economic freedoms. As the world's largest humanitarian agency, the WFP has the greatest responsibility to protect the data it stewards from vested interests of military contractors like Palantir and the state power that the company seeks to serve, with resultant risks to both human rights and the sovereignty of states in the international order.

3. Transparency, a non-negotiable baseline, is completely absent in the Palantir partnership

In some cases, civil society and journalists have been able to challenge Palantir's other public contracts largely because Freedom of Information laws forced key details into the open. The UN is not subject to equivalent disclosure obligations, and the WFP has treated transparency about this partnership as optional. Without access to the actual contract – disclosing what permissions the WFP has granted (or conceded to) Palantir – no entity outside the WFP can fully assess the risk or hold the organization to account. A 2020 legal audit reportedly flagged contract language allowing Palantir to "utilise data for performance improvement", raising the possibility that the WFP's operational data could be used to train Palantir's commercial products. The 2025 audit also found no "clearly defined exit strategy" for the partnership. We should not have to rely on leaks to know such vital facts; information about the WFP's technology partnerships should be available *a priori* for public scrutiny.

The data flowing into the WFP's Palantir-built systems concerns the supply chain of food aid, including what food aid is moved, where it originates, its route, obstacles along the way, who transports it, which partners distribute it, who receives it, and where distribution happens. Data, metadata, or software improvements built through this partnership could well be of value beyond humanitarian logistics, enabling Palantir to develop products and services for its other enterprise clients — both military and commercial.

Also, data about population movement, the roads and obstacles that shape access, and food availability and distribution patterns is precisely the kind of information that could inform strategies aimed at controlling or constraining civilian access to food.

There is currently no proof that this has occurred, but the WFP's opacity prevents public monitoring and the identification of potential misuse. The emerging consensus is that auditability across the data value chain is essential for pre-emptive harm prevention. Therefore, transparency about data systems and infrastructures, and the burden of proactive disclosure on this should rest with the WFP; investigating a data harm post facto is simply against the public interest.

4. Humanitarian data is not a commodity; it needs the greatest care

Humanitarian sector agencies are stewards of some of the most sensitive data collected about the world's most vulnerable people. Gaza remains the starkest illustration of how civilian data in the hands of powerful mercenary corporations can end up feeding systems that perpetuate the most horrific human rights abuses and war crimes. As AI becomes a dual-use technology and the race to build AI systems drives an unprecedented hunger for data, handing over data from sensitive humanitarian settings without public disclosure of the terms is nothing short of criminal negligence. It is entirely antithetical to integrity and humanity, both core values of the WFP as a UN agency.

5. The WFP's public reassurances do not match its own reporting

During a session of the UN Committee on World Food Security, in response to a question from the Civil Society and Indigenous Peoples' Mechanism (CSIPM), the WFP's Jean-Martin Bauer, Director of the WFP's Food Security and Nutrition Analysis Service, stated on the record: "I want to emphasize that there is no beneficiary data, no personal identifying information processed through the Palantir software we have at WFP", adding, "there's no beneficiary information transiting through that software". This statement was reiterated in a recent management letter sent to all staff.

Independent research undertaken by Tech for Bad in June 2026, drawing on the WFP's own reporting, found that DOTS is listed among the "key digital applications used within the WFP's SCOPE [the WFP's beneficiary information management platform] ecosystem" for "data reconciliation". In so far as there is no publicly available information or transparent communication of the data flows between the WFP's beneficiary-facing applications (SCOPE and others) and DOTS, the processing of aid recipients' data remains a black box, and the WFP's public assurances remain difficult to trust. The clarification provided to the CSIPM query is hence unsatisfactory and incomplete, silent as it is on what the WFP considers beneficiary data and how it plans to address any possible risks of re-identification via quasi-identifiers in aggregate-level data reconciliation processes.

Whether aid recipients, other affected populations, suppliers, transporters, and partners know, and can meaningfully consent to, data use and reuse is critical for all local to global public data infrastructures.

Only full transparency regarding the WFP's data definitions and infrastructural workflows and protocols, along with effective monitoring and accountability mechanisms, can ensure trust in the WFP and effectively safeguard the people it is meant to serve.

Our demands

We call on the World Food Programme to:

1. Rescind its contract and terminate the partnership with Palantir Technologies.
2. Guarantee that the WFP-led UN80 integrated supply-chain initiative for humanitarian aid does not extend Palantir's footprint across the UN system.
3. Publish the full text of all current and prior WFP-Palantir contracts and data-sharing agreements, including provisions on data use, intellectual property, and any rights Palantir holds to use WFP data, or derivatives of it, to train or improve its own products.
4. Commission an independent, external human rights and data protection audit of DOTS, including its linkages to and integrations with other platforms, conducted with meaningful, resourced participation of affected communities, civil society organizations and frontline WFP staff, and publish it in full.
5. Establish clear, accessible mechanisms for beneficiaries and partner organizations to know when their data is processed through Palantir's systems or those of other technology providers, and to consent to, withdraw from, or wholly decline, such processing without losing access to assistance or funding.
6. Provide public clarification on the disjuncture between the WFP's statement that no beneficiary data is processed through Palantir software and its own reporting on aggregate-level beneficiary data reconciliation in DOTS, and adopt a robust human rights-based definition of what its beneficiary data safeguards actually cover.
7. Ensure that adequate and effective mechanisms are in place to prevent risks to human rights and data sovereignty, stemming from partnerships with technology companies, including strict conflict of interest policies and effective monitoring, accountability, and access to information mechanisms.
8. Set out and fund a concrete, time-bound plan to transition away from Palantir and other technology corporations towards public-interest-oriented data infrastructure built on open-source, interoperable and federated architectures grounded in a public governance ethos, with scaffolding for human rights and public interest.
9. Work with governments to fund the transition out of Palantir to public alternatives and ensure that future technology funding for the WFP does not carry conditionalities that impede its autonomy and integrity.
10. Publish, and develop if not already existing, a procurement policy for technology infrastructure and services for the WFP. This policy should ensure that concerns such as those raised above are addressed through regular, publicly available reporting.

Such an approach would align with the 2017 guidelines for international organizations, particularly within the UN system, recommended by the UN Special Rapporteur on Freedom of Expression and Access to Information.

The World Food Programme was created to protect and assist people and communities, not to become a test-bed for the technology of surveillance and control. We ask the WFP to meet this moment with the responsibility, transparency, caution, and accountability that the world's most vulnerable people deserve. We look forward to a substantive, public response, and remain attentive and open to discussions towards co-building tech infrastructure policies adequate to sustainable futures for all.

See all endorsers here.

Endorse the letter by filling out the form here.