



Warszawa, 08-10-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Sylvia Gregorczyk-Abram

VII.501.141.2026.KK

Pan

Władysław Kosiniak-Kamysz

Wiceprezes Rady Ministrów

Minister Obrony Narodowej

AE:PL-25597-80046-SIUIT-17

Szanowny Panie Premierze,

do Biura Rzecznika wpłynęło pismo od przedstawicieli inicjatywy „Nasze dane”, w którym Wnioskodawcy zwracają uwagę na współpracę nawiązaną przez Ministerstwo Obrony Narodowej (dalej: Ministerstwo) z amerykańską firmą Palantir Technologies Inc. (dalej: Palantir).

Zgodnie z informacją przedstawioną na stronie Ministerstwa¹, 27 października 2025 r. podpisany został list intencyjny dotyczący „partnerstwa na rzecz innowacji w obronności”, stanowiący kontynuację współpracy spółki z polskim wojskiem, zapoczątkowanej w dniu 23 grudnia 2024 roku podpisaniem „Memorandum of Understanding on Cybersecurity of Information Technology Cooperation”. Jak można się dowiedzieć ze strony Ministerstwa, firma Palantir specjalizuje się „w analizie danych na dużą skalę” i oferuje „zaawansowane oprogramowanie umożliwiające integrację, przetwarzanie, analizę i wizualizację ogromnych zbiorów danych – w szczególności dla potrzeb sektora publicznego, obronnego, wywiadowczego oraz

¹ <https://www.gov.pl/web/obrona-narodowa/list-intencyjny-mon--palantir-technologies-partnerstwo-na-rzecz-innowacji-w-obronnosci>

dużych firm przemysłowych”. Współpraca ma natomiast dotyczyć „obszarów sztucznej inteligencji (AI), technologii informacyjnych (IT) oraz cyberbezpieczeństwa”.

Niepokój Wnioskodawców budzi natomiast działalność firmy Palantir, w tym sposób przetwarzania i zakres wykorzystania danych, które według nich są wątpliwe etycznie. W piśmie otrzymanym przez Rzecznika wskazywane są przykłady rezygnacji ze współpracy z firmą Palantir państw takich jak Szwajcaria, Niemcy czy Francja, z uwagi na ryzyko udostępniania wrażliwych danych amerykańskiemu rządowi i służbom wywiadowczym czy stosowanie metod polegających na tworzeniu zaawansowanych profili poszczególnych osób i środowisk, w sposób niezgodny ze standardami konstytucyjnej ochrony prywatności. Wnioskodawcy podkreślają również, że Specjalna Sprawozdawczyni ONZ Francesca Albanese w swoim raporcie (A/HRC/59/23, 2025) stwierdziła, że istnieją „uzasadnione podstawy, by sądzić”, iż Palantir dostarczył technologię umożliwiającą zautomatyzowane podejmowanie decyzji na polu walki w ramach prowadzonej współpracy z izraelskim ministerstwem obrony.

O kontrowersjach piszą też polskie media², zwracając uwagę m.in. na niejasne okoliczności zawierania umów z Palantir przez europejskie rządy, ryzyko uzależnienia zdolności operacyjnych od zagranicznego dostawcy, powiązania Palantir z amerykańskimi służbami wywiadowczymi oraz imigracyjnymi, w tym ryzyko udzielenia dostępu do danych znajdujących się w dyspozycji firmy Palantir organom wywiadowczym rządu USA na podstawie tzw. CLOUD Act, czyli amerykańskiej ustawy federalnej z 23 marca 2018 roku upoważniającej władze USA do żądania od firm amerykańskich przekazania danych niezależnie od tego, czy znajdują się one na serwerach w Stanach Zjednoczonych czy poza ich granicami. Istotnym głosem w sprawie było też stanowisko Europejskiego Inspektora Ochrony Danych, który zwracał uwagę na cechy oprogramowania oferowanego przez Palantir uniemożliwiające ustalenie, jakie kategorie danych (w tym dane wrażliwe) podlegają przetwarzaniu.

W kontekście powyższych uwag chciałabym zwrócić uwagę na obowiązek szczególnej dbałości o zagwarantowanie zgodności potencjalnego przetwarzania danych osobowych z konstytucyjnym standardem ochrony prywatności. Jak wynika z art. 47 Konstytucji RP oraz art. 51 Konstytucji RP w zw. z art. 31 ust. 3 Konstytucji RP, konieczne jest istnienie wyraźnej ustawowej podstawy przetwarzania danych osobowych, a ich pozyskiwanie, gromadzenie i udostępnianie powinno odbywać się w sposób respektujący zasadę proporcjonalności, obejmując jedynie informacje

² Np. <https://oko.press/jeden-palantir-by-wszystkimi-rzadzic-tolkien-cia-i-europejska-suwerennosc>, <https://innpoland.pl/216629,mon-zaciesnia-wspolprace-z-kontrowersyjna-firma-czym-jest-palantir>.

niezbędne w demokratycznym państwie prawnym. Zgodnie z orzecnictwem Trybunału Konstytucyjnego oznacza to możliwość przetwarzania przez władze publiczne informacji o osobie wyłącznie w zakresie niezbędnym (koniecznym) – a nie „wygodnym” dla organów publicznych³.

Choć kwestie bezpieczeństwa narodowego i obronności znajdują się poza zakresem regulacji Unii Europejskiej, a w konsekwencji przetwarzanie danych osobowych dla tych celów – na podstawie art. 2 ust. 2 lit. a RODO⁴ czy motywu 14 Dyrektywy 2016/680⁵ – wyłączone jest spod gwarantowanych w tych aktach prawnych standardów ochrony prywatności i danych osobowych, należy jednak mieć na względzie konsekwentne akcentowanie przez Trybunał Sprawiedliwości Unii Europejskiej konieczności ochrony jednostki przed arbitralną ingerencją w jej prywatność wskutek działania organów władzy publicznej, jak również brak zgodności z prawem UE, w tym z art. 7 i 8 Karty Praw Podstawowych UE⁶, prewencyjnego, niezmieszanego i ogólnego gromadzenia danych obywateli⁷.

Uwzględniając powyższe uwagi, działając na podstawie art. 13 ust. 1 pkt 2 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r. poz. 1264 ze zm.), zwracam się do Pana Premiera z prośbą o zajęcie stanowiska w sprawie, w szczególności poprzez udzielenie odpowiedzi na następujące pytania:

1. Czy Ministerstwo przeprowadziło analizę współpracy z firmą Palantir pod kątem uwzględnienia ochrony prywatności zgodnie ze standardem konstytucyjnym i unijnym (jeśli tak – jakie były wyniki tej analizy)?
2. Czy została zawarta umowa wykonawcza pomiędzy Ministerstwem a firmą Palantir, w tym regulująca obszary współpracy i zasady ochrony przetwarzanych

³ Zob. wyrok Trybunału Konstytucyjnego z dnia 20 listopada 2002 r. (K 41/02), wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (K 23/11).

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.).

⁶ Karta praw podstawowych Unii Europejskiej (t.j. Dz. U. UE. C. z 2016 r. Nr 202, str. 389).

⁷ Zob. np. wyrok Wielkiej Izby TSUE z dnia 6 października 2020 r. (sprawy połączone C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i in. v Premier ministre i in.*), wyrok TSUE (w pełnym składzie) z dnia 30 kwietnia 2024 r. (sprawa C-470/21, *La Quadrature du Net II*).

danych (jeśli tak – jakie przyjęto rozwiązania w zakresie przetwarzania danych osobowych)?

3. Czy współpraca z firmą Palantir obejmuje również wsparcie w zakresie wykrywania przestępczości i innych zagrożeń dla bezpieczeństwa publicznego?
4. Czy Ministerstwo przewiduje upoważnienie firmy Palantir do samodzielnego pozyskiwania i agregowania danych (w tym danych osobowych), czy też współpraca obejmuje analizę danych otrzymanych ze źródeł udostępnionych przez właściwe organy (jeśli tak – jakie to będą zbiory danych)?
5. Czy współpraca będzie obejmowała prowadzenie przez firmę Palantir operacji na danych mających charakter zautomatyzowanego i generalnego przetwarzania?

Z poważaniem

Sylwia Gregorczyk-Abram

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Do wiadomości: Wnioskodawcy