

Przetargi BIP

Od: lobbying.pl@icloud.com
Wysłano: piątek, 12 grudnia 2025 08:08
Do: WNIOSKI BIP; Sekretariat.BPM; Biuro Dyrektora Generalnego MON; baw; kontakt@mon.gov.pl
DW: listy@prezydent.pl; bprm; Biurorzecznika; poczta@abw.gov.pl; abw@abw.gov.pl; kontakt@mswia.gov.pl; skw@skw.gov.pl; punkt_konsultacyjny@sejm.gov.pl; marszalek@sejm.gov.pl; bbn@bbn.gov.pl; kancelaria@rcl.gov.pl; Włodzimierz.Czazasty@sejm.pl; karol.nawrocki@prezydent.pl; sygnal@cba.gov.pl; jan.pinski@wiesci24.pl; leszek.szymowski@gmail.com; kontakt@slw.com.pl; widzowie@tvn.pl; kontakt@pulstv.pl; aleksander berdowicz; sekretariat@tv-trwam.pl; lemon@lemonrecords.pl; kontakt@stopklatka.tv; kontakt@eska.tv; redakcja@ttv.pl; marcinski@proton.me; Grzegorz Braun; Grzegorz Braun; Piotr Grzegorzczak; Grzegorz Lichwa; Adam Kołaczek; "Paweł A. Fijałkowski"; Aleksandra Baron; Lobbyingo.cz; Lobbyingo IPM; Lobbyingo DE
Temat: WYSTĄPIENIE W TRYBIE LOBBINGOWYM do Ministra Obrony Narodowej

UWAGA: korespondencja spoza organizacji !

Liverpool, dnia 12.12.2025r

Minister Obrony Narodowej RP
Władysław Kosiniak Kamysz
ul. Klonowa 1
00-909 Warszawa

WYSTĄPIENIE LOBBINGOWE / WNIOSEK FORMALNY

o pełne ujawnienie Listu Intencyjnego MON – Palantir Technologies oraz wszystkich dotychczasowych dokumentów dotyczących współpracy i integracji technologicznej

ŻĄDANIE PEŁNEJ JAWNOŚCI

Działając jako zawodowy lobbysta wpisany do rejestru podmiotów wykonujących zawodową działalność lobbingsową pod numerem wpisu (00305), w imieniu własnym, Lobbyingo International Public Movement, jego klientów, podmiotów zależnych i powiązanych oraz przede wszystkim interesu publicznego narodu Polskiego, narodów unii europejskiej jak i pozostałej reszty świata życia uduchowionego oraz w związku z wpływem wdrażanej przez MON technologii o charakterze

podwójnego przeznaczenia (dual-use) na prawa i wolności obywateli, żądam niezwłocznego udostępnienia w formie elektronicznej (PDF) na adres e-mail oraz równolegle przez platformę ePUAP:

W PEŁNEJ, NIEZMIENIONEJ FORMIE

1. Oryginału podpisanego **Listu Intencyjnego MON – Palantir Technologies** wraz z:
 - wszystkimi załącznikami, aneksami, wersjami roboczymi, wersjami językowymi,
 - wszelkimi notatkami negocjacyjnymi, uzgodnieniami, protokołami,
 - listą uczestników negocjacji oraz materiałami, które do nich przekazano.
2. Pełnej dokumentacji współpracy MON – Palantir Technologies, obejmującej [m.in.](https://m.in.gov.pl):
 - korespondencję urzędową,
 - dokumenty techniczne i opisowe,
 - analizy prawne, DPIA, oceny ryzyka,
 - dokumenty finansowe,
 - raporty, briefingi, notatki z posiedzeń,
 - dokumenty zawarte z innymi agendami rządowymi w ramach tej współpracy,
 - wszelkie analizy dotyczące wprowadzenia technologii do służb porządku publicznego i cywilnych organów państwa.

UZASADNIENIE MERYTORYCZNE

1. Jawność technologii strategicznych w sektorze obronnym

Współpraca państwa członkowskiego NATO i UE z globalnym podmiotem prywatnym, takim jak Palantir Technologies, dotyczy technologii o charakterze strategicznym: integracji danych, analityki operacyjnej, sztucznej inteligencji, rozwiązań wsparcia dowodzenia, cyberinfrastruktury i logistyki wojskowej.

Z uwagi na znaczenie tych technologii dla bezpieczeństwa państwa zasadne jest zapewnienie:

- jawności zakresu współpracy,
- jawności jej podstaw prawnych,
- jawności kosztów w części nieobjętej ochroną informacji niejawnych,
- jawności decyzji dotyczących integracji zasobów państwowych z platformami firm trzecich.

Transparentność w tym obszarze ma charakter **strukturalny**, ponieważ wpływa na ocenę ryzyk:

- interoperacyjności systemów państwowych,
- cyberbezpieczeństwa,
- przepływu danych operacyjnych,
- zgodności z regulacjami UE i NATO.

2. Wymogi przejrzystości wynikające z członkostwa Polski w UE i NATO

Polska, jako członek NATO i Unii Europejskiej, jest zobowiązana do przestrzegania:

- zasad interoperacyjności technologicznej (NATO Standardization Office),
- zasad transparentności zakupu i wdrażania technologii obronnych (EU Defence Procurement Directive),

- zasad jawności i kontroli demokratycznej nad sektorem obronnym, wynikających z *acquis communautaire*,
- regulacji dotyczących ochrony danych, w tym **RODO** oraz **NIS2**, które nakładają obowiązek dokumentowania przepływów danych i dostawców infrastruktury cyfrowej.

Współpraca z prywatnym podmiotem amerykańskim musi pozostawać zgodna z:

- polityką bezpieczeństwa informacji NATO,
- europejską autonomią strategiczną w zakresie danych i infrastruktury,
- zasadą minimalizacji ryzyk związanych z transferem danych poza EOG.

Dostęp do dokumentów, o które wnoszę, jest niezbędny, aby dokonać oceny zgodności z tymi standardami i obowiązkami, co stanowi interes publiczny o wysokiej wadze.

3. Cyfrowa suwerenność państwa

Wdrażanie rozwiązań klasy Palantir ingeruje w:

- architekturę danych wojska,
- procesy dowodzenia i analizy,
- modele decyzyjne oparte na sztucznej inteligencji, jak obecnie testowane w Palestynie przez Izrael lub na Ukrainie,
- zależności technologiczne pomiędzy państwem a prywatnym podmiotem zewnętrznym.

Bez jawności i audytowalności dokumentów nie jest możliwa ocena wpływu tej współpracy na tzw. **cyfrową suwerenność państwa**, którą definiuje się jako zdolność państwa do:

- kontroli nad własnymi zasobami informacyjnymi,
- prowadzenia operacji niezależnie od infrastruktury obcych podmiotów,
- unikania vendor lock-in w systemach krytycznych,
- zachowania przejrzystości procesów decyzyjnych wspomaganych przez AI.

INTERES PUBLICZNY O CHARAKTERZE BEZSPRZECZNYM:

Technologia Palantir, jako system analityczny integrujący dane z wielu źródeł, według deklaracji Ministra Kominiaka Kamysza ma charakter **dual-use**, co oznacza:

- zastosowanie wobec żołnierzy, funkcjonariuszy, ale i **cywili**,
- potencjalne wykorzystywanie przez Policję i służby porządku publicznego,
- wpływ na prawa podstawowe obywateli (prywatność, wolność, bezpieczeństwo),
- konieczność pełnej jawności dokumentów podstawowych.

Interes społeczny wymaga pełnej kontroli demokratycznej nad architekturą technologii wdrażanej na terytorium RP.

TERMIN: 7 DNI

Żądam udostępnienia pełnych dokumentów **w terminie 7 dni** od doręczenia niniejszego wniosku na:

- e-mail: lobbingo.pl@icloud.com

Monstrualny i demoniczny charakter technologii i jej wejście w sferę cywilną uzasadnia skrócony termin.

ZASTRZEGA SIĘ:

Nie wyrażam zgody na:

- zaciemnienia,
- usuwanie jakichkolwiek fragmentów,
- powoływanie się na „częściowe udostępnienie”,
- odmowę na podstawie rzekomego „bezpieczeństwa państwa”.

Technologia wdrażana przez MON zgodnie z publicznymi wypowiedziami Ministra Kominiaka Kamysza ma docelowo trafić do **Policji, organów cywilnych, administracji publicznej oraz struktur bezpieczeństwa wewnętrznego**. Oznacza to, że:

MON nie może zasłaniać się wyłącznie bezpieczeństwem narodowym.

System, który będzie wykorzystywany wobec obywateli, nie może być objęty tajemnicą zważając na dokonania tej firmy w Palestynie i na Ukrainie.

PODSTAWA PRAWNA BEZWZGLĘDNEJ JAWNOŚCI

1. **Konstytucja RP — art. 61** (prawo do informacji publicznej),
art. 31 ust. 3 (proporcjonalność) — tajemność może być stosowana tylko, gdy konieczna i minimalna.

2. Ustawa o dostępie do informacji publicznej:

- art. 1 ust. 1 — informacją publiczną jest *każdy* dokument dotyczący funkcjonowania organu państwa,
- art. 6 ust. 1 pkt 3 lit. d — umowy i porozumienia z podmiotami prywatnymi,
- art. 5 — wyjątki interpretowane ściśle; brak podstawy do używania klauzul przy technologiach cywilnych,
- **art. 23** — odpowiedzialność karna za bezprawną odmowę lub utrudnianie dostępu.

3. RODO/GDPR:

Art. 5, art. 25, art. 35 — *obowiązek przejrzystości i dokumentowania wpływu technologii na prawa obywateli*.

Technologia Palantir obejmuje przetwarzanie danych dotyczących osób fizycznych — dlatego jawność jest bezwzględna.

4. **Karta Praw Podstawowych UE** — art. 7, 8, 11.

5. **AI Act / Data Governance Act / Data Act** — pełna audytowalność systemów wysokiego ryzyka.

6. **Standardy NATO i ONZ dotyczące demokratycznej kontroli technologii** — jawność elementów analitycznych stosowanych wewnątrz państwa.

SKUTKI BRAKU PEŁNEJ JAWNOŚCI:

W przypadku:

- braku odpowiedzi,
- odpowiedzi niepełnej,
- zaciemnienia dokumentów,
- zasłaniania się „częściowym dostępem”,
- odmowy niepopartej konkretnym i proporcjonalnym uzasadnieniem,

zostanie **natychmiast** wniesiona skarga do Wojewódzkiego Sądu Administracyjnego na bezczynność MON lub na odmowę. Skarga będzie obejmować również:

- żądanie nałożenia grzywny na organ,
- wniosek o zabezpieczenie w zakresie wstrzymania dalszych wdrożeń,
- zawiadomienia do Rzecznika Praw Obywatelskich, Prezesa UODO, Komisji Europejskiej oraz właściwych organów NATO.

Poniżej załączam pełny wykaz podstaw prawnych i precedensów na które się powołuję w dzisiejszym wystąpieniu. (Konstytucja RP, uDIP, uDIN, RODO, akty UE, standardy NATO).

Konstytucja RP

Art. 61 Konstytucji RP: prawo do informacji obejmuje działalność organów władzy publicznej, w tym MON, także w zakresie dokumentów, stanowisk, aktów wewnętrznych i przebiegu negocjacji, jeśli dotyczą spraw publicznych.

Art. 31 ust. 3: zasada proporcjonalności — każde ograniczenie jawności musi być konieczne i minimalne.

Art. 54 i Art. 2 (zasada demokratycznego państwa prawnego): brak jawności wobec technologii ingerującej w wolności obywateli narusza istotę ustroju.

Ustawa o dostępie do informacji publicznej

Obejmuje dokumenty MON, także niewprowadzające skutków prawnych (listy intencyjne, protokoły, notatki).

Art. 6 ust. 1 pkt 3 lit. d — Umowy i porozumienia z podmiotami prywatnymi.

Art. 5 — wyjątki muszą być wykładane ściśle; nie wolno utajniać „dla wygody”.

Art. 23 — sankcja karna za bezprawną odmowę.

Ustawa o działalności lobbingowej w procesie stanowienia prawa

Wskazuje [m.in.](#) obowiązek przyjmowania i rejestrowania wystąpień lobbingowych.

W tej sprawie podnosimy, że współpraca MON–Palantir ma wymiar **prawotwórczy** (technologia, która trafi do sfery cywilnej → nowy reżim prawny przetwarzania danych, integracji systemów, nadzoru operacyjnego).

Ustawa o ochronie informacji niejawnych

Art. 5 ust. 1 — nadanie klauzuli wymaga realnej szkody, a nie ogólnej wygody.

Art. 6 — można zdeklasyfikować w części; także wyłącznie fragmenty.

Art. 7 — zakaz nadużywania klauzul.

Dla technologii dual-use — jawność dominująca.

Ustawa o ochronie danych osobowych + RODO/GDPR

Technologia Palantir dotyczy:

- przetwarzania danych osobowych obywateli,
- możliwego profilowania ryzyka,
- interoperacyjnych systemów militarnych i cywilnych.

Art. 5 RODO — zasada przejrzystości.

Art. 25 RODO — privacy by design → bez jawności nie da się zweryfikować.

Art. 35 RODO — ocena skutków operacji przetwarzania (DPIA).

Art. 83 RODO — sankcje za naruszenia.

MON *nie może* wprowadzać technologii obejmującej dane obywateli bez jawnych informacji opisowych.

Prawo europejskie: Karta praw podstawowych UE

Art. 7 — prywatność.

Art. 8 — ochrona danych.

Art. 11 — wolność informacji.

Dual-use, który przenika do struktur cywilnych, wchodzi w zakres tych praw.

Prawo europejskie: Digital Services Act / Artificial Intelligence Act / Data Governance Act / Data Act

Wszystkie te akty regulują:

- przejrzystość algorytmiczną,
 - audytowalność,
 - podmiotowy dostęp,
- zasady współpracy administracji z podmiotami prywatnymi przy przetwarzaniu informacji.

Technologia Palantir jest **systemem wysokiego ryzyka** (AI Act).

To wymusza audyt, jawność architektury i opisu działania.

Prawo międzynarodowe ONZ: Zasady z Johannesburga

Standard ONZ dotyczący przejrzystości systemów bezpieczeństwa i ograniczeń tajemnicy państwowej.

Zabrania nadużywania „security exception” dla technologii cywilno-wojskowej.

Standardy NATO ([m.in.](#) BI-SC Directive 90-2, NATO Data Exploitation Framework)

NATO wskazuje zasadę:

- audytowalności,
- interoperacyjności,
- minimalizacji tajności dla systemów dual-use,
- kontroli demokratycznej nad architekturą danych.

Każdy kraj członkowski musi umożliwić społeczną kontrolę technologii wchodzących do sfery bezpieczeństwa wewnętrznego.

Orzecznictwo krajowe (WSA, NSA)

Najważniejsze tezy:

- jawność przeważa nad utajnieniem,
- list intencyjny to informacja publiczna,
- dokumenty wytworzone przez podmiot prywatny stają się informacją publiczną, jeśli dotyczą spraw publicznych,
 - można udostępniać dokument „prawie cały”, a zaciemnić tylko wrażliwe fragmenty,
 - odmowa musi być szczegółowo uzasadniona — inaczej jest bezprawna.

Orzecznictwo TSUE

Wyroki dotyczące:

- proporcjonalności ograniczeń jawności,
- konieczności przejrzystości technologii ingerującej w prawa podstawowe,
- zasady, że „algorytm nie może decydować w sposób niekontrolowany”.

W kontekście Palantir to fundament.

Soft-law UE, NATO, OECD

Zasady:

- demokratycznej kontroli technologii,
 - jawności architektury danych,
 - przejrzystości algorytmicznej,
- ochrony społeczeństwa przed nadużyciami systemów analitycznych.

Palantir, jego szef, podmioty z nimi powiązane i od nich zależne, to jest dokładnie ta technologia, której te zasady dotyczą.

TRYB DORĘCZENIA:

Proszę jednocześnie wszystkich odbiorców o publikację w BIP, przesłanie potwierdzenia drogą mailową przyjęcia niniejszego wystąpienia (czas, sygnatura), oraz o wskazanie osoby/osób kontaktowych (imię, stanowisko, bezpośredni adres e-mail i tel.) odpowiedzialnych za przygotowanie odpowiedzi.

Pozdrawiam,

Patryk Ryszard Pańkowski
Zawodowy Lobbysta / Pełnomocnik Publiczny

Lobbingo International Public Movement
94 Neston Gardens, Birkenhead
Merseyside, CH41 8AZ, United Kingdom
e-mail: lobbingo.pl@icloud.com

