



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, **18 września 2026**

DPNT.060.111.2026.WL

**Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu do spraw Cyfryzacji**

Ministerstwo Cyfryzacji

Szanowna Pani Minister,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 16 września 2026 r., znak: DPIS-WWKS.002.184.1.2026, dotyczącym **opisu założeń przedsięwzięcia informatycznego „Polska Tarcza PNT – Moduł 1”**, dalej: OZPI, (wnioskodawca: Minister Finansów i Gospodarki, beneficjent: Główny Urząd Geodezji i Kartografii, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², Prezes Urzędu Ochrony Danych Osobowych zwraca uprzejmie uwagę na następujące kwestie.

Celem przedsięwzięcia informatycznego **„Polska Tarcza PNT – Moduł 1”** – jak wskazano w opisie – jest stworzenie narzędzia pozwalającego na analizę cyberodporności państwa w obszarze usług pozycji, nawigacji i czasu jako krytycznych komponentów procesów cyfrowych, administracyjnych, gospodarczych, naukowych i obronnych (geodezji, transportu, energetyki, komunikacji, lotnictwa, zarządzania kryzysowego, infrastruktury krytycznej i obronności).

W tym celu zakłada się budowę i modyfikację systemów i modułów analitycznych, API, usług statusowych, alertowych i raportowych oraz platformy integracyjnej Polska

¹ 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. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

Tarcza PNT. Umożliwi to wczesne wykrywanie, klasyfikację i ocenę wpływu incydentów, tj. obrazu sytuacji w zakresie jakości sygnałów GNSS. Pozwoli to na uzyskanie szybkiego rozpoznania, czy dane zdarzenie (zakłócenie sygnałów) ma charakter lokalny, sektorowy, transgeniczny, przypadkowy czy potencjalnie wrogi.

Analizując **pkt. 2.4 OZPI „Produkty końcowe projektu”**, należy zwrócić uwagę, że wnioskodawca **przewiduje przeprowadzenie inicjalnego testu prywatności**, z którego raport ma zostać przedstawiony w grudniu 2026 r., co należy ocenić pozytywnie, gdyż należy:

- zweryfikować wpływ przedsięwzięcia na procesy przetwarzania danych osobowych,
- ocenić ryzyka dla tych danych, a także
- prawidłowość sporządzonej oceny otoczenia prawnego (OZPI nie zakłada jego zmian) przez wnioskodawcę.

Test zawierający ocenę skutków dla ochrony danych powinien spełniać wymogi art. 25 ust. 1 ³ i art. 35 (w szczególności ust. 1 ⁹ oraz ust. 10 ⁴) rozporządzenia 2016/679. W ocenie tej i na jej podstawie wnioskodawca i beneficjent powinni:

- zdiagnozować ryzyka dla praw i wolności podmiotów danych wynikające z wdrażanych rozwiązań,
- wypracować konkretne środki zaradcze oraz techniczno-organizacyjne minimalizujące zidentyfikowane zagrożenia,
- przeanalizować i dokonać przeglądu ukierunkowany na ustalenie związku zachodzącego pomiędzy realizacją przedsięwzięcia informatycznego na proces i zakres przetwarzanych danych osobowych.

Wnioskodawca w **punkcie 6 „Otoczenie prawne”** nie dostrzega konieczności zmiany żadnych aktów prawnych, co wymaga **powtórnej analizy** w zakresie:

- przeanalizowania zagadnień związanych z otoczeniem prawnym – **czy na pewno**

3 Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. ⁹ Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

4 Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

analiza nie prowadzi do potrzeby uzupełnienia podstaw prawnych przetwarzania danych osobowych (pkt 6 OZPI), w szczególności biorąc pod uwagę wskazane wyżej ryzyka i wnioski z testu prywatności, jak również konstytucyjną zasadę praworządności, dotyczące przetwarzania danych osobowych zasady: zgodności z prawem, rzetelności i przejrzystości oraz rozliczalności (art. 5 ust. 1 lit a i ust. 2) i aspekty wynikające z art. 6 ust. 3 rozporządzenia 2016/679⁵.

Mając na względzie znaczenie projektowanego przedsięwzięcia dla strategicznych interesów państwa w podnoszeniu odporności państwa poprzez stworzenie systemu analitycznego i operacyjnego umożliwiającego wczesne wykrywanie, klasyfikację i ocenę wpływu incydentów na jakości sygnałów GNSS, organ nadzorczy deklaruje swoje eksperckie wsparcie w zakresie zapewnienia zgodności projektowanych rozwiązań z rozporządzeniem 2016/679, w tym także w przypadku przedstawienia do zaopiniowania projektu przepisów ustawy wdrażającej projektowane rozwiązania.

Łączę wyrazy szacunku,
Miroslaw Wróblewski
Prezes
Urzędu Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

⁵ Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.