PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 04-05-2026

DPNT.060.16.2026.WL.PM

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

Szanowna Pani Minister,

w związku z pismem z 24 kwietnia 2026 r. znak: DPiS.WWKS.002.33.1.2026, przekazującym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji **opisu założeń projektu informatycznego pn. „Generator Informacji Bezpieczeństwa Kolejowego (GIBK)”** – wnioskodawca: Kancelaria Prezesa Rady Ministrów, beneficjent: Urząd Transportu Kolejowego, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

Zgodnie z **pkt 1.1** „Identyfikacja problemu i potrzeb” opisu założeń projektu informatycznego, tworzony Generator Informacji Bezpieczeństwa Kolejowego (GIBK) ma zawierać m. in. moduł: „4. Moduł analityczny – wykrywanie anomalii i identyfikacja trendów z wykorzystaniem sztucznej inteligencji.” (str. 2). W **pkt 7.1** „Architektura” „Widok kooperacji aplikacji” „Lista systemów wykorzystywanych w projekcie” (str. 28) w odniesieniu do GIBK wnioskodawca zawarł następujący opis: „Moduł analityczny –

[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.), dalej: „rozporządzenie 2016/679”.
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

zaawansowane narzędzia analizy danych. System integruje się z krajowymi systemami teleinformatycznymi, takimi jak: CEIDG, PESEL, REGON, KRS, TERYT, Węzeł Krajowy, Węzeł Podpisu, e-Doręczenia, dane.gov.pl oraz Krajowy Rejestr Elektroniczny o Maszynistach i Prowadzących Pojazdy Kolejowe (KREMiPPK). GIBK współpracuje również z europejskimi systemami kolejowymi: ERADIS, EVR i OSS, prowadzonymi przez Europejską Agencję Kolejową, a także z systemami podmiotów rynku kolejowego.”.

Organ nadzorczy z uznaniem przyjmuje identyfikację przez wnioskodawcę **ryzyka nieprawidłowego zabezpieczenia danych osobowych**, które mogą być przetwarzane w GBIK – **pkt 5.1 „**Ryzyka wpływające na realizację projektu” (str. 18) opisu założeń projektu informatycznego, jak również założenie pozytywnego wyniku finalnego testu prywatności do końca lipca 2028 r. – **pkt 3 „**Kamienie milowe” opisu założeń projektu informatycznego (str. 14).

Prezes UODO prosi jednocześnie o wskazanie **jakie konkretne ryzyka związane z przetwarzaniem danych osobowych zostały zidentyfikowane przez wnioskodawcę**, w szczególności w obszarach takich jak nieuprawniony dostęp, utrata, wyciek lub nieuprawniona modyfikacja danych, a także jakie środki techniczne i organizacyjne będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków. Powstaje również pytanie **jakie dane osobowe będą przetwarzane w module analitycznym, który ma być częścią GBIK**. Jest to szczególnie istotne, gdyż jak zakłada wnioskodawca we wcześniej wspomnianym pkt 7.1 opisu założeń projektu informatycznego, GBIK będzie zintegrowany z szeregiem krajowych systemów teleinformatycznych, w większości o charakterze rejestrów publicznych w rozumieniu art. 3 pkt 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 ze zm.).

Dlatego też, wnioskodawca w toku planowanego testu prywatności, czyli **oceny skutków dla ochrony danych**, o której mowa w art. 35 ust. 1 rozporządzenia 2016/679[3], powinien przeprowadzić pogłębioną analizę modułu analitycznego wykorzystującego mechanizmy sztucznej inteligencji. Użycie tego typu rozwiązań w omawianym kontekście wiąże się z podwyższonym ryzykiem naruszenia praw i wolności osób fizycznych. Aby planowany projekt informatyczny uwzględniał ochronę danych w fazie projektowania (art. 25 ust. 1 rozporządzenia 2016/679[4]) konieczne jest przede **wszystkim skonstruowanie właściwej podstawy prawnej przetwarzania, gdyż dojdzie wtedy do zmiany celu**

[3] 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] 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.

przetwarzania w rozumieniu art. 6 ust. 4 rozporządzenia 2016/679[5] **w odniesieniu do danych z publicznych rejestrów teleinformatycznych: CEIDG, PESEL, REGON, KRS, TERYT, Węzeł Krajowy, Węzeł Podpisu, e-Doręczenia, dane.gov.pl oraz Krajowy Rejestr Elektroniczny o Maszynistach i Prowadzących Pojazdy Kolejowe (KREMiPPK), które będą wymieniać informacje z GBIK**.

Konieczne jest więc również przeprowadzenie oceny skutków dla ochrony danych, w ramach planowanych przez wnioskodawcę zmian legislacyjnych – art. 35 (ust. 1 [6] **i ust. 10** [7]**), dla stworzenia podstawy prawnej opowiadającej art. 6 ust. 1 lit. c rozporządzenia 2016/679**. Z uwagi na charakter modułów opartych na sztucznej inteligencji, obejmujących złożone operacje przetwarzania danych, w tym potencjalne profilowanie w rozumieniu art. 4 pkt 4 rozporządzenia 2016/679[8] oraz podejmowanie decyzji w sposób zautomatyzowany, analiza ta powinna stanowić integralny element

[5] Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; b)kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

[6] 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.

[7] 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.

[8] „Profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

oceny skutków dla ochrony danych (art. 22 rozporządzenia 2016/679[9]). **Brak wyraźnego uregulowania tej materii** może prowadzić do niewystarczającego uwzględnienia ryzyk dla praw i wolności osób fizycznych, a w konsekwencji do naruszenia z zasad dotyczących przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a)[10], ograniczenia celu (art. 5 ust. 1 lit. b)[11], minimalizacji danych (art. 5 ust. 1 lit. c)[12], rozliczalności (art. 5 ust. 2)[13] jak również wymogów ochrony danych w fazie projektowania.

W omawianym kontekście wnioskodawca powinien rozważyć, czy projektowany system nie powinien zostać także oceniony przez pryzmat zapewnienia stosowania Aktu w

[9] 1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. 2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą. 3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. 4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

[10] Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

[11] Zgodnie z zasadą ograniczenia celu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami.

[12] Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

[13] Zgodnie z zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie.

sprawie sztucznej inteligencji[14], z uwzględnieniem jego art. 27, także ust. 4 tej regulacji[15], **tj. oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych**.

Należy też podkreślić, że przepisy powszechnie obowiązującego prawa powinny ustanawiać adekwatne i jednoznaczne gwarancje ochrony praw jednostki w przypadku przetwarzania danych osobowych przez podmioty publiczne z użyciem systemów wykorzystujących sztuczną inteligencję, w szczególności w celu zapewnienia poszanowania prawa do ochrony danych osobowych (art. 8 Karty praw podstawowych UE), prawa do poszanowania życia prywatnego (art. 7 Karty praw podstawowych UE), a także prawa do dobrej administracji (art. 41 Karty praw podstawowych UE). Wiąże się to z koniecznością wprowadzenia odpowiednich gwarancji w prawie krajowym

Organ nadzorczy deklaruje jednocześnie swoje wsparcie eksperckie w ramach procesu oceny systemu SI2PEM.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

---

[14] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

[15] Przed wdrożeniem systemu AI wysokiego ryzyka, o którym mowa w art. 6 ust. 2, z wyjątkiem systemów AI wysokiego ryzyka przeznaczonych do stosowania w obszarze wymienionym w załączniku III pkt 2, podmioty stosujące będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) i c), przeprowadzają ocenę skutków w zakresie praw podstawowych, jakie może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące przeprowadzają ocenę obejmującą: a) opis procesów podmiotu stosującego, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem; b) opis okresu, w którym każdy system AI wysokiego ryzyka ma być wykorzystywany i opis częstotliwości tego wykorzystywania; c) kategorie osób fizycznych i grup, na które może mieć wpływ wykorzystywanie systemu; d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób fizycznych lub grupy osób zidentyfikowane zgodnie z lit. c) niniejszego ustępu, z uwzględnieniem informacji przekazanych przez dostawcę zgodnie z art. 13; e) opis wdrożenia środków nadzoru ze strony człowieka, zgodnie z instrukcją obsługi; f) środki, jakie należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym ustalenia dotyczące zarządzania wewnętrznego i mechanizmów rozpatrywania skarg. 2. Obowiązek ustanowiony w ust. 1 ma zastosowanie do wykorzystania systemu AI wysokiego ryzyka po raz pierwszy. W podobnych przypadkach podmiot stosujący może polegać na wcześniej przeprowadzonych ocenach skutków dla praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie wykorzystania systemu AI wysokiego ryzyka podmiot stosujący uzna, że którykolwiek z elementów wymienionych w ust. 1 uległ zmianie lub nie jest już aktualny, podmiot ten podejmuje niezbędne kroki w celu aktualizacji informacji. 3. Po przeprowadzeniu oceny, o której mowa w ust. 1 niniejszego artykułu, podmiot stosujący powiadamia organ nadzoru rynku o jej wynikach, przedkładając jako element tego powiadomienia wypełniony wzór, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące mogą zostać zwolnione z obowiązku dokonania powiadomienia. 4. Jeżeli którykolwiek z obowiązków ustanowionych w niniejszym artykule został już spełniony w wyniku oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, ocena skutków w zakresie praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, stanowi uzupełnieniem tej oceny skutków dla ochrony danych. 5. Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym spełnianie ich obowiązków wynikających z niniejszego artykułu w sposób uproszczony.

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan
Grzegorz Karpiński
Sekretarz stanu
Zastępca Szefa
Kancelarii Prezesa Rady Ministrów