

Wnoszący petycję:

Adresat:

Minister Finansów i Gospodarki
za pośrednictwem Ministerstwa Rozwoju i Technologii
Plac Trzech Krzyży 3/5, 00-507 Warszawa

PETYCJA

w sprawie zmiany przepisów dotyczących publicznego udostępniania, ponownego wykorzystywania i masowego przetwarzania danych osobowych przedsiębiorców wpisanych do CEIDG oraz danych udostępnianych przez publiczne interfejsy API administracji

Na podstawie ustawy z dnia 11 lipca 2014 r. o petycjach, działając w interesie publicznym oraz własnym, zwracam się z wnioskiem o podjęcie prac legislacyjnych dotyczących zasad publicznego udostępniania danych osób fizycznych prowadzących działalność gospodarczą, w szczególności danych zawartych w Centralnej Ewidencji i Informacji o Działalności Gospodarczej oraz danych udostępnianych za pośrednictwem systemów i interfejsów programistycznych administracji publicznej, w tym Wykazu podatników VAT prowadzonego przez Szefa Krajowej Administracji Skarbowej.

Celem petycji nie jest ograniczenie możliwości weryfikacji przedsiębiorcy przez kontrahentów ani podważenie zasady przejrzystości obrotu gospodarczego. Postuluję natomiast dostosowanie obecnego modelu jawności danych przedsiębiorców do współczesnych możliwości technologicznych, które pozwalają na automatyczne pobieranie, kopiowanie, łączenie, wzbogacanie, profilowanie i rozpowszechnianie danych osobowych na skalę nieporównywalną z warunkami, w których tworzone obecny model publicznych rejestrów.

Najważniejsze postulaty

1. wprowadzenie możliwości zastrzeżenia publicznego udostępniania dokładnego adresu wykonywania działalności gospodarczej, jeżeli adres ten jest jednocześnie miejscem zamieszkania przedsiębiorcy;
2. wprowadzenie w CEIDG mechanizmu pozwalającego przedsiębiorcy określić, czy adres będący jednocześnie adresem zamieszkania może być publicznie prezentowany w nieograniczonym dostępie;
3. ograniczenie przekazywania dokładnych adresów zamieszkania osób fizycznych poprzez publiczne API administracji państwowej, jeżeli cel danego interfejsu może zostać osiągnięty bez ujawniania tak szerokiego zakresu danych;
4. rozdzielenie funkcji weryfikacyjnej publicznych rejestrów od funkcji umożliwiającej masowe budowanie baz osób fizycznych, tak aby możliwość sprawdzenia statusu konkretnego kontrahenta nie prowadziła automatycznie do możliwości tworzenia przez podmioty trzecie własnych kopii państwowych baz danych;
5. przeanalizowanie zakresu danych zwracanych przez API Wykazu podatników VAT, w szczególności w odniesieniu do osób fizycznych prowadzących działalność gospodarczą pod adresem zamieszkania;
6. wprowadzenie mechanizmów privacy by design i privacy by default w publicznych API, w szczególności poprzez zwracanie jedynie danych niezbędnych do realizacji określonego celu zapytania;
7. szczególne uregulowanie wtórnej publikacji danych pozyskanych poprzez API administracji publicznej, jeżeli podmiot trzeci przekształca usługę służącą weryfikacji kontrahenta w publiczną, indeksowaną przez wyszukiwarki bazę osób fizycznych;

8. przeanalizowanie zasad masowego i automatycznego łączenia danych pochodzących z CEIDG, Wykazu podatników VAT, GUS/REGON, KRS oraz innych rejestrów publicznych, jeżeli rezultatem jest tworzenie nowych, szczegółowych profili osób fizycznych;
9. ustanowienie dodatkowych gwarancji dotyczących komercyjnego ponownego wykorzystywania danych osobowych przedsiębiorców, w szczególności do budowania scoringów, ocen wiarygodności, profili biznesowych, map powiązań oraz baz przeznaczonych do sprzedaży lub odpłatnego dostępu;
10. przeanalizowanie problemu wykonywania przez podmioty wtórnie pozyskujące dane obowiązku informacyjnego z art. 14 RODO, w szczególności w sytuacji automatycznego pobierania danych z publicznych API;
11. ograniczenie publicznej dostępności danych osobowych po zawieszeniu lub zakończeniu wykonywania działalności gospodarczej, przy pozostawieniu możliwości uzyskania niezbędnych informacji przez uprawnione podmioty;
12. przeprowadzenie kompleksowej oceny skutków dla ochrony danych osobowych obecnego ekosystemu publicznych rejestrów i interfejsów API, z uwzględnieniem rozwoju sztucznej inteligencji, web scrapingu, automatycznego generowania stron oraz narzędzi do łączenia danych.

1. Zmiana technologiczna radykalnie zmieniała skutki publicznej dostępności danych

Jawność rejestru przedsiębiorców oraz publicznych wykazów administracji została ustanowiona przede wszystkim w celu zapewnienia bezpieczeństwa i przejrzystości obrotu gospodarczego. We współczesnej gospodarce cyfrowej dostępność informacji w rejestrze publicznym nie oznacza jednak już wyłącznie możliwości sprawdzenia danych konkretnego kontrahenta.

Rozwój interfejsów API, automatycznego pobierania danych, narzędzi typu web scraping, systemów sztucznej inteligencji oraz automatycznych systemów generowania treści umożliwia przetwarzanie bardzo dużych zbiorów danych, automatyczne ich łączenie i tworzenie na ich podstawie odrębnych baz oraz stron internetowych poświęconych konkretnym osobom.

Dane jednego przedsiębiorcy mogą zostać automatycznie pobrane z CEIDG, Wykazu podatników VAT, GUS/REGON, KRS oraz innych źródeł, a następnie przekształcone w rozbudowany profil osoby fizycznej. Powstają w ten sposób informacje, których żaden pojedynczy rejestr publiczny nigdy samodzielnie nie prezentował.

Problemem nie jest zatem wyłącznie jawność pojedynczego rekordu w rejestrze publicznym, lecz możliwość masowej agregacji, trwałego kopiowania oraz przekształcania danych publicznych w szczegółowe profile osób fizycznych. Publiczna dostępność źródła nie powinna być utożsamiana z nieograniczonym prawem do dowolnego przetwarzania zawartych w nim danych osobowych w każdym późniejszym celu.

- profile przedsiębiorców i historie zmian danych;
- zestawienia powiązań pomiędzy osobami i podmiotami;
- scoringi i oceny wiarygodności;
- automatyczne klasyfikacje i bazy marketingowe;
- agregaty danych przeznaczone do sprzedaży;
- strony profilowe indeksowane przez wyszukiwarki internetowe.

2. Szczególna sytuacja osób prowadzących jednoosobową działalność gospodarczą

Osoba prowadząca jednoosobową działalność gospodarczą znajduje się w szczególnej sytuacji w porównaniu z wieloma innymi uczestnikami obrotu gospodarczego. W przypadku JDG przedsiębiorca i osoba fizyczna są

tym samym podmiotem, a firma przedsiębiorcy obligatoryjnie zawiera jego imię i nazwisko. Nie istnieje więc rzeczywiste oddzielenie tożsamości przedsiębiorcy od tożsamości prywatnej osoby fizycznej.

Jeszcze poważniejszy problem występuje w przypadku osób, które prowadzą działalność gospodarczą we własnym mieszkaniu lub domu. Adres wykonywania działalności może być wówczas jednocześnie dokładnym miejscem zamieszkania przedsiębiorcy i jego rodziny.

W praktyce rozpoczęcie nawet niewielkiej jednoosobowej działalności gospodarczej może prowadzić do trwałego powiązania w Internecie imienia i nazwiska, działalności zawodowej, numerów identyfikacyjnych, statusu podatkowego, danych o działalności, rachunku firmowego oraz dokładnego adresu zamieszkania. Dane te mogą następnie być kopiowane przez kolejne portale, indeksowane przez wyszukiwarki i przechowywane niezależnie od źródłowego rejestru państwowego.

3. Szczególny problem publicznych API Ministerstwa Finansów

Ministerstwo Finansów udostępnia API Wykazu podatników VAT umożliwiające automatyczną komunikację systemów informatycznych z państwowym wykazem. Rozwiązanie to ma uzasadnione zastosowania gospodarcze, w szczególności do automatycznej weryfikacji statusu kontrahenta i rachunku bankowego.

Wykaz podatników VAT może jednak w odniesieniu do osoby fizycznej zawierać m.in. imię i nazwisko, NIP, REGON, status podatnika VAT, daty dotyczące rejestracji, wykreślenia lub przywrócenia, numery rachunków związanych z działalnością oraz adres stałego miejsca prowadzenia działalności, a w przypadku jego braku także adres miejsca zamieszkania.

Powstaje zatem pytanie o proporcjonalność technicznego udostępniania tak szerokiego zakresu informacji w sytuacji, gdy podstawowym celem określonego zapytania może być wyłącznie potwierdzenie statusu VAT albo zweryfikowanie numeru rachunku.

Szczególnie istotnym zjawiskiem jest wykorzystywanie publicznych API administracji państwowej nie tylko do wewnętrznej weryfikacji kontrahentów, ale jako jednego ze źródeł zasilających prywatne bazy danych. Dane takie mogą następnie być prezentowane w odmiennym kontekście, łączone z informacjami z CEIDG, GUS, KRS i innych źródeł oraz publikowane jako odrębne profile osób lub przedsiębiorców.

Istnieje zasadnicza różnica pomiędzy sytuacją, w której system księgowy sprawdza za pomocą API, czy kontrahent jest czynnym podatnikiem VAT i czy jego rachunek figuruje w wykazie, a sytuacją, w której podmiot komercyjny wykorzystuje API państwa jako źródło danych do budowy własnej publicznej bazy osób fizycznych, wzbogaca dane informacjami z innych rejestrów, publikuje je w Internecie, indeksuje w wyszukiwarkach i ewentualnie tworzy na ich podstawie scoring lub profil.

4. Publiczne API nie powinno automatycznie oznaczać prawa do stworzenia równoległego rejestru osób fizycznych

Fakt, że określone dane można zgodnie z prawem uzyskać z rejestru państwowego, nie powinien automatycznie prowadzić do wniosku, że każdy podmiot może bez dalszej analizy utworzyć ich trwałą kopię, zestawień je z danymi z szeregu innych źródeł, opublikować wynik w innym celu, wystawić go do indeksowania przez wyszukiwarki, tworzyć na jego podstawie dodatkowe wnioski o osobie, wykorzystywać go do profilowania i komercjalizować powstały profil.

Podmiot, który pobiera dane za pomocą API i następnie samodzielnie określa nowe cele oraz sposoby ich przetwarzania, powinien oceniać swoje obowiązki wynikające z RODO niezależnie od tego, że pierwotne źródło danych było publiczne. Szczególnego znaczenia nabierają zasady ograniczenia celu, minimalizacji danych, przejrzystości, prawidłowości, ograniczenia okresu przechowywania oraz rozliczalności.

5. Państwo powinno stosować zasadę minimalizacji również przy projektowaniu API

Jedną z podstawowych zasad RODO jest minimalizacja danych. Zasada ta powinna mieć odzwierciedlenie również w architekturze technicznej państwowych interfejsów API.

Jeżeli użytkownik systemu chce jedynie sprawdzić, czy określony NIP posiada status podatnika VAT czynnego, czy rachunek bankowy jest przypisany do konkretnego podatnika albo czy przedsiębiorca znajduje się w określonym rejestrze, do realizacji takiego celu nie zawsze musi być konieczne zwracanie dokładnego adresu jego miejsca zamieszkania.

Warto przeanalizować model różnych poziomów odpowiedzi zależnych od celu zapytania: odpowiedzi potwierdzającej określony status, podstawowych danych identyfikacyjnych oraz rozszerzonego zakresu danych dostępnego wyłącznie w przypadkach rzeczywistej potrzeby jego uzyskania. Szczególnej ochronie powinien podlegać dokładny adres osoby fizycznej, jeżeli jest to jednocześnie adres jej domu.

6. Zagrożenie dla prywatności i bezpieczeństwa przedsiębiorcy oraz jego rodziny

Powszechna publikacja adresu domowego wraz z imieniem i nazwiskiem oraz informacjami zawodowymi może zwiększać ryzyko natarczywego marketingu, oszustw i prób wyłudzeń, phishingu i socjotechniki, podszywania się pod przedsiębiorcę, nękania, stalkingu, grózb i szykan, ustalenia miejsca zamieszkania osoby aktywnej publicznie lub zawodowo oraz naruszenia prywatności członków rodziny mieszkających pod tym samym adresem.

Adres przedsiębiorstwa w przypadku JDG może być faktycznie adresem rodzinnego domu, w którym mieszkają również osoby niemające żadnego związku z prowadzoną działalnością gospodarczą. Ochrona tych osób powinna zostać uwzględniona przy ocenie proporcjonalności obecnego modelu jawności.

Problem powinien być analizowany w szczególności z punktu widzenia art. 47 Konstytucji RP dotyczącego ochrony życia prywatnego i rodzinnego, art. 50 dotyczącego nienaruszalności mieszkania, art. 51 dotyczącego informacji o osobie oraz konstytucyjnej zasady proporcjonalności.

7. Stanowisko Prezesa Urzędu Ochrony Danych Osobowych potwierdza systemowy charakter problemu

Problem opisany w niniejszej petycji został już dostrzeżony przez Prezesa Urzędu Ochrony Danych Osobowych.

W stanowisku z 25 czerwca 2025 r., sygn. DPNT.401.210.2025, Prezes UODO wskazał na potrzebę ponownej analizy fundamentów modelu powszechnej dostępności i jawności CEIDG, wymieniając wśród nowych ryzyk m.in. profilowanie, łączenie baz danych, wykorzystywanie danych przez podmioty trzecie w różnych celach oraz dostępność prywatnych danych adresowych osób prowadzących działalność gospodarczą w miejscu zamieszkania.

Następnie w wystąpieniu z 8 sierpnia 2025 r., sygn. DPNT.413.32.2025, Prezes UODO zwrócił się o działania legislacyjne mające na celu rewizję obecnego modelu powszechnej dostępności danych osobowych przedsiębiorców w CEIDG. Wśród możliwych rozwiązań wskazano m.in. możliwość zastrzeżenia danych adresowych, dobrowolność ich ujawniania, gdy adres działalności jest jednocześnie miejscem zamieszkania, oraz dostęp do danych adresowych w trybie wnioskowym.

Postulaty niniejszej petycji są więc zbieżne z kierunkiem wskazanym przez organ nadzorczy właściwy w sprawach ochrony danych osobowych.

8. Konieczne jest rozróżnienie jawności rejestru od masowego tworzenia komercyjnych baz osób fizycznych

Możliwość zweryfikowania przez klienta lub kontrahenta, czy określony przedsiębiorca faktycznie istnieje i prowadzi działalność gospodarczą, realizuje ważny interes publiczny. Nie wynika jednak z tego automatycznie, że realizacja tego interesu wymaga umożliwienia podmiotowi trzeciemu systematycznego pobierania bardzo dużej liczby rekordów, trwałego przechowywania ich poza systemem państwowym, łączenia danych pochodzących z różnych państwowych baz, publikowania profili przedsiębiorców w wyszukiwarkach internetowych, sprzedaży wyników takiego przetwarzania czy tworzenia scoringów i ocen dotyczących osoby fizycznej.

Z punktu widzenia ochrony prywatności istnieje zasadnicza różnica pomiędzy sprawdzeniem danych konkretnego kontrahenta a zbudowaniem masowej bazy umożliwiającej analizę i profilowanie znacznej części osób prowadzących działalność gospodarczą w Polsce. Prawo oraz techniczna konstrukcja państwowych systemów powinny tę różnicę uwzględniać.

9. Obowiązki wynikające z RODO nie znikają dlatego, że dane pochodzą ze źródła publicznego

Dane dotyczące osoby prowadzącej JDG pozostają danymi osobowymi. Ich pozyskanie z CEIDG, Wykazu podatników VAT, GUS, KRS lub innego publicznego źródła nie powoduje automatycznie wyłączenia stosowania RODO.

Znaczenie mają w szczególności zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości danych, ograniczenia okresu przechowywania oraz rozliczalności administratora. Podmiot tworzący własną bazę danych powinien posiadać odpowiednią podstawę prawną dla realizowanego przez siebie celu przetwarzania.

Szczególne znaczenie ma art. 14 RODO odnoszący się do sytuacji, w której dane nie zostały pozyskane bezpośrednio od osoby, której dotyczą.

10. Problem niewykonywania obowiązku informacyjnego z art. 14 RODO

W praktyce przedsiębiorca może odnaleźć swoje dane na stronach podmiotów, z którymi nigdy nie pozostawał w żadnej relacji i którym nigdy bezpośrednio nie przekazał swoich danych. Dane mogły zostać automatycznie pozyskane z CEIDG, API Ministerstwa Finansów lub innych publicznych źródeł i wykorzystane do utworzenia odrębnej bazy.

Pojawia się wówczas problem wykonania obowiązku informacyjnego określonego w art. 14 RODO. Niektóre podmioty mogą próbować powoływać się na przewidziany w RODO wyjątek związany z niewspółmiernie dużym wysiłkiem.

Szczególne problematyczna byłaby praktyka, w której przedsiębiorca podejmujący świadomą decyzję biznesową o zgromadzeniu danych setek tysięcy lub milionów osób mógłby następnie uzasadniać niewykonanie obowiązków informacyjnych wobec tych osób wyłącznie tym, że sam stworzył bazę danych o bardzo dużej skali. Prowadziłoby to do paradoksalnej sytuacji, w której wzrost skali przetwarzania danych zmniejszałby praktyczny poziom ochrony osób, których dane dotyczą.

Problem ten był przedmiotem postępowania dotyczącego spółki Bisnode, obecnie Dun & Bradstreet. W sprawie zakończonej wyrokiem Naczelnego Sądu Administracyjnego, sygn. III OSK 2538/21, NSA potwierdził obowiązek informacyjny wobec osób prowadzących działalność gospodarczą, których dane pozyskano z publicznych rejestrów, oraz wskazał na zawężającą interpretację wyjątku dotyczącego niewspółmiernie dużego wysiłku.

11. Profilowanie i scoring przedsiębiorców

Szczególnej uwagi wymagają podmioty, które nie ograniczają się do reprodukcji informacji z rejestru, lecz na podstawie danych publicznych tworzą nowe informacje dotyczące konkretnej osoby.

Połączenie wielu źródeł może pozwolić na automatyczne wnioskowanie o sytuacji zawodowej, historii gospodarczej, skali prowadzonej działalności, prawdopodobnej kondycji ekonomicznej, powiązaniach osobowych i gospodarczych, miejscu zamieszkania, otoczeniu zawodowym czy prawdopodobnej wiarygodności biznesowej.

Rezultatem może być scoring lub profil, który nigdy nie znajdował się w żadnym z rejestrów źródłowych. Tak utworzone informacje mogą następnie wpływać na sposób postrzegania przedsiębiorcy przez kontrahentów, klientów albo inne podmioty.

Rozwój sztucznej inteligencji dodatkowo obniża koszt przeprowadzania tego rodzaju analiz i pozwala wykonywać je automatycznie w stosunku do ogromnych zbiorów osób. Z tego względu ustawodawca powinien przeanalizować, czy obecny model udostępniania państwowych danych nie prowadzi do powstawania infrastruktury umożliwiającej nadmierną obserwację i profilowanie osób fizycznych prowadzących działalność gospodarczą.

12. Jawność nie powinna oznaczać utraty kontroli nad adresem własnego domu

Za szczególnie istotne uważam wprowadzenie rozwiązania pozwalającego przedsiębiorcy prowadzącemu działalność we własnym miejscu zamieszkania ograniczyć powszechną dostępność dokładnego adresu.

Możliwe jest zachowanie bezpieczeństwa obrotu gospodarczego bez publicznej ekspozycji dokładnego adresu mieszkania lub domu. CEIDG mogłaby publicznie prezentować np. miejscowość wykonywania działalności, podczas gdy dokładny adres byłby dostępny właściwym organom i podmiotom posiadającym odpowiednią podstawę prawną lub wykazującym prawnie uzasadnioną potrzebę uzyskania takiej informacji.

Analogicznie należałoby ocenić zasadność przekazywania adresu miejsca zamieszkania poprzez API Wykazu podatników VAT w sytuacjach, w których zapytanie ma służyć wyłącznie potwierdzeniu statusu podatnika lub rachunku bankowego.

13. Techniczny mechanizm ochrony przed masową redystrybucją

Postuluję przeanalizowanie możliwości wprowadzenia do państwowych rejestrów oznaczeń odnoszących się do danych osób fizycznych. Rozwiązanie takie nie powinno być rozumiane jako uzależnienie każdego zgodnego z prawem przetwarzania od zgody przedsiębiorcy.

Mogłoby jednak pozwolić na jednoznaczne i możliwe do odczytania maszynowo wskazanie, że dokładny adres przedsiębiorcy jest jednocześnie adresem jego zamieszkania, że adres podlega ograniczeniom w publicznym rozpowszechnianiu, że osoba wniosła sprzeciw wobec określonego przetwarzania opartego na prawnie uzasadnionym interesie albo że dane nie powinny być bez odrębnej podstawy prawnej wykorzystywane do dodatkowego profilowania lub scoringu.

Takie rozwiązanie ułatwiłoby administratorom zewnętrznych baz projektowanie systemów uwzględniających prawa osób już na etapie automatycznego pobierania informacji.

14. Problem trwałości kopii danych

Dodatkowym problemem jest kopiowanie danych przez wiele niezależnych serwisów. Zmiana albo usunięcie informacji w państwowym rejestrze nie powoduje automatycznej aktualizacji wszystkich prywatnych baz, które wcześniej pobrały dane.

W rezultacie w Internecie mogą przez wiele lat funkcjonować nieaktualne adresy, statusy działalności, informacje dotyczące VAT, dane kontaktowe, informacje o rachunkach lub powiązaniach. Z punktu widzenia osoby fizycznej powstaje praktycznie niemożliwa do kontrolowania sieć kopii danych.

Im więcej automatycznie generowanych serwisów powstaje, tym trudniejsze staje się ustalenie administratorów danych i skuteczne wykonywanie praw wynikających z RODO. Skala tego zjawiska może wzrastać wraz z dalszym rozwojem sztucznej inteligencji i automatycznych systemów generowania treści internetowych.

Wnioski końcowe

1. podjęcie prac legislacyjnych nad zmianą modelu publicznej dostępności danych osobowych przedsiębiorców;
2. objęcie analizą nie tylko CEIDG, lecz również publicznych API i innych systemów administracji udostępniających dane osób fizycznych prowadzących działalność gospodarczą;
3. przeprowadzenie kompleksowej oceny skutków obecnego modelu jawności i maszynowego dostępu do danych dla prywatności osób prowadzących JDG;
4. uwzględnienie stanowisk Prezesa UODO, w szczególności wystąpień DPNT.401.210.2025 oraz DPNT.413.32.2025;
5. przeanalizowanie możliwości zastrzeżenia dokładnego adresu działalności, gdy jest on jednocześnie miejscem zamieszkania przedsiębiorcy;
6. dokonanie przeglądu zakresu danych osobowych zwracanych przez API Wykazu podatników VAT, w szczególności zasadności udostępniania adresu miejsca zamieszkania osoby fizycznej;
7. rozważenie technicznego rozdzielania zapytań służących wyłącznie weryfikacji statusu lub rachunku od zapytań zwracających szerszy zakres danych przedsiębiorcy;
8. wprowadzenie przy projektowaniu państwowych API zasady minimalizacji danych oraz privacy by design i privacy by default;
9. przeanalizowanie możliwości ograniczenia masowego kopiowania i publicznej redystrybucji danych osobowych pobranych za pomocą państwowych interfejsów, zwłaszcza gdy prowadzi to do utworzenia równoległych publicznych baz przedsiębiorców;
10. uwzględnienie różnicy pomiędzy pojedynczą weryfikacją kontrahenta a masowym tworzeniem komercyjnych baz i profili osób fizycznych;
11. przeanalizowanie ryzyka wynikającego z automatycznego łączenia danych z CEIDG, Wykazu podatników VAT, KRS, GUS/REGON oraz innych źródeł;
12. przeanalizowanie problemu komercyjnego scoringu i profilowania osób prowadzących JDG;
13. wypracowanie mechanizmu zapewniającego skuteczniejsze wykonywanie przez wtórnych administratorów obowiązków wynikających z art. 14 RODO oraz praw osób określonych w art. 15-21 RODO;
14. ograniczenie sytuacji, w których państwowa infrastruktura techniczna przeznaczona do bezpieczeństwa obrotu gospodarczego może być wykorzystywana jako źródło zasilające komercyjne, publiczne bazy profilujące osoby fizyczne;
15. poddanie projektowanych rozwiązań konsultacji z Prezesem UODO, Rzecznikiem Małych i Średnich Przedsiębiorców, Rzecznikiem Praw Obywatelskich oraz organizacjami społecznymi zajmującymi się ochroną prywatności;
16. przedstawienie informacji, czy Ministerstwo prowadzi obecnie lub planuje prace dotyczące ograniczenia powszechnej dostępności prywatnych adresów przedsiębiorców, zasad masowego ponownego

wykorzystywania danych CEIDG, zakresu danych osobowych udostępnianych za pomocą API administracji publicznej oraz ochrony przedsiębiorców przed automatycznym profilowaniem na podstawie połączonych danych publicznych.

Podkreślam, że przedmiotem niniejszej petycji nie jest postulat likwidacji jawności rejestrów przedsiębiorców ani ograniczenia możliwości weryfikowania kontrahentów.

Postulatem jest przywrócenie proporcji pomiędzy uzasadnioną jawnością obrotu gospodarczego a konstytucyjnym i wynikającym z prawa Unii Europejskiej prawem osoby fizycznej do prywatności oraz ochrony danych osobowych.

Istnieje zasadnicza różnica pomiędzy udostępnieniem narzędzia pozwalającego zweryfikować przedsiębiorcę w konkretnej transakcji a stworzeniem technicznych warunków umożliwiających budowanie przez podmioty trzecie kompleksowych, publicznych i komercyjnych profili milionów osób fizycznych.

Fakt rozpoczęcia jednoosobowej działalności gospodarczej nie powinien oznaczać faktycznej rezygnacji z prawa do prywatności ani prowadzić do sytuacji, w której państwowe rejestry i API stają się techniczną podstawą do tworzenia przez nieograniczoną liczbę podmiotów kompleksowych profili konkretnego człowieka, obejmujących również dokładny adres jego domu.

Rozwój sztucznej inteligencji, automatyzacji i technologii agregacji danych powoduje, że koszt tego rodzaju profilowania gwałtownie maleje, a skala potencjalnego przetwarzania rośnie. Z tego względu problem wymaga interwencji ustawodawczej i technicznej, zanim masowa agregacja, automatyczne profilowanie oraz generowanie kolejnych kopii danych przedsiębiorców staną się zjawiskiem praktycznie niemożliwym do odwrócenia.

Proszę o rozpatrzenie niniejszej petycji oraz przedstawienie stanowiska w zakresie wskazanych postulatów.

Oświadczenie dotyczące publikacji danych: nie wyrażam zgody na ujawnienie na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego moich danych osobowych jako podmiotu wnoszącego petycję.

Z poważaniem,

Materiały źródłowe i odniesienia

Ustawa z dnia 11 lipca 2014 r. o petycjach - tekst jednolity, w szczególności art. 2-4

<https://eli.gov.pl/api/acts/DU/2018/870/text.html>

Prezes UODO, DPNT.401.210.2025 - stanowisko dotyczące modelu jawności CEIDG, profilowania i łączenia baz danych

<https://www.uodo.gov.pl/pl/138/3797>

Prezes UODO, DPNT.413.32.2025 - wystąpienie w sprawie jawności danych osobowych w CEIDG

<https://www.uodo.gov.pl/pl/138/3841>

UODO - informacja o wyroku NSA w sprawie Bisnode / Dun & Bradstreet, sygn. III OSK 2538/21

<https://sdt.uodo.gov.pl/pl/138/2827>

Krajowa Administracja Skarbowa - Informacje o Wykazie podatników VAT i zakresie danych

<https://www.gov.pl/web/kas/informacje-o-wykazie>

Krajowa Administracja Skarbowa - Jak korzystać z Wykazu podatników VAT, w tym API <https://www.gov.pl/web/kas/jak-korzystac-z-wykazu>

Krajowa Administracja Skarbowa - API Wykazu podatników VAT <https://www.gov.pl/web/kas/api-wykazu-podatnikow-vat2>

Ministerstwo Rozwoju i Technologii - informacje o składaniu petycji <https://www.gov.pl/web/rozwoj-technologia/zloz-petycje>

Uwaga: dokument został przygotowany jako projekt petycji do uzupełnienia danymi wnoszącego i podpisania przed wysłaniem. Stan źródeł sprawdzony: 24 września 2026 r.