



**PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH**

**Mirosław Wróblewski**

Warszawa,

**DPNT.413.18.2026**

**Pan  
Marcin Kierwiński  
Minister Spraw Wewnętrznych  
i Administracji**

Szanowny Panie Ministrze,

działając na podstawie art. 52 ust. 2 ustawy o ochronie danych osobowych<sup>1</sup> **zwracam się do Pana Ministra z uprzejmą prośbą i wnioskiem o podjęcie prac legislacyjnych prowadzących do odpowiednich zmian przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji<sup>2</sup> i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2020 r.<sup>3</sup>, celem dostosowania ich do standardów wynikających z zasad ochrony danych osobowych, standardów wynikających z Konstytucji RP oraz orzecznictwa Trybunału Sprawiedliwości UE.**

Zgodnie z art. 20 ust. 1l ustawy o Policji, od funkcjonariuszy oraz pracowników Policji wykonujących czynności służbowe związane z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego pobierane są odciski linii papilarnych lub wyciski ze słuzówki policzków. Dane te są przetwarzane wyłącznie w celu eliminacji śladów pozostawionych przez te osoby z materiału dowodowego zgromadzonego w toku postępowań. Jednocześnie, zgodnie z art. 20 ust. 1m ustawy o Policji, minister właściwy do spraw wewnętrznych określa, w drodze rozporządzenia, tryb pobierania wskazanych danych, sposób dokumentowania tych czynności, katalog uprawnionych służb policyjnych do korzystania ze zbiorów danych oraz sposób ich zabezpieczenia, uniemożliwiający identyfikację funkcjonariusza lub pracownika Policji przez osoby nieupoważnione.

<sup>1</sup> Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

<sup>2</sup> Dz. U. z 2025 r. poz. 636 ze zm.

<sup>3</sup> Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2020 r. w sprawie pobierania odcisków linii papilarnych oraz wycisków ze słuzówki policzków od funkcjonariuszy i pracowników Policji, Dz. U. z 2020 r. poz. 1347 ze zm., dalej jako: rozporządzenie.

Zakres przetwarzanych danych obejmuje w szczególności dane biometryczne w postaci odcisków linii papilarnych palców i dłoni oraz profili DNA uzyskanych z wymazów ze śluzówki policzków, a także dane identyfikacyjne, m.in. takie jak imię i nazwisko, imiona i nazwiska rodowe rodziców, data i miejsce urodzenia, numer PESEL, adres zamieszkania, obywatelstwo i płeć, jak również informacje związane z czynnościami służbowymi, w tym oznaczenie i numer sprawy oraz miejsce i powód daktyloskopowania, stosownie do art. 21h ust. 2 pkt 2 i 3 ustawy o Policji oraz art. 21b ust. 2 w zw. z art. 21d ust. 1 ustawy o Policji.

Administratorem zbiorów danych biometrycznych oraz danych DNA jest Komendant Główny Policji, który prowadzi zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (DNA), Centralną Registraturę Daktyloskopijną oraz zbiory automatycznie przetwarzające dane biometryczne, zgodnie z art. 21a ust. 1 oraz 21h ust. 1 ustawy o Policji. Przetwarzanie danych odbywa się przez uprawnione jednostki organizacyjne Policji, natomiast ich wprowadzenie do zbiorów danych DNA następuje na podstawie wniosku właściwego miejscowo organu Policji przed podjęciem pierwszych czynności służbowych związanych z ujawnianiem, zabezpieczaniem lub badaniem śladów związanych z podejrzeniem popełnienia czynu zabronionego, zgodnie z art. 21b ust. 2 ustawy o Policji, zaś do zbiorów danych biometrycznych – na podstawie wniosku organu prowadzącego postępowanie lub poszukiwanie osoby zaginionej, stosownie do art. 21i ustawy o Policji. Dane te mogą być udostępniane nieodpłatnie organom prowadzącym postępowania karne, czynności wykrywcze lub identyfikacyjne, zgodnie z art. 21j oraz art. 21c ustawy o Policji.

Przetwarzanie wskazanych danych odbywa się wyłącznie w celach określonych w ustawie o Policji, tj. w szczególności w celu prowadzenia czynności wykrywczych i identyfikacyjnych, a w odniesieniu do funkcjonariuszy i pracowników Policji – przede wszystkim w celu eliminacji pozostawionych przez nich śladów, zgodnie z art. 21d ust. 1 i 2 oraz art. 21k ust. 3 ustawy o Policji.

Z przepisów art. 21e ust. 1 oraz art. 21l ust. 1 ustawy o Policji wynika, że w weryfikacji danych zgromadzonych w zbiorze danych DNA oraz zbiorze danych biometrycznych, o której mowa w art. 16 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, uczestniczą jednostki organizacyjne Policji, służby, instytucje państwowe lub organy władzy publicznej, które przekazały informacje, w tym dane osobowe, do zbiorów danych DNA oraz biometrycznych.

Zgodnie z art. 21e ust. 2 pkt 4 oraz art. 21l ust. 2 pkt 3 ustawy o Policji, dane przetwarzane na podstawie art. 20 ust. 1l ustawy o Policji podlegają usunięciu w przypadku utraty ich przydatności eliminacyjnej, nie później jednak niż po upływie 5 lat od dnia ustania stosunku służbowego lub pracy osoby, której dane dotyczą. W odniesieniu do danych zgromadzonych w zbiorze danych DNA ich usunięcia oraz zniszczenia próbek biologicznych dokonuje komisja powołana przez Komendanta Głównego Policji, sporządzając z tych czynności stosowny protokół, zgodnie z art. 21e ust. 5 ustawy o Policji.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2020 r. określa tryb pobierania od funkcjonariuszy i pracowników Policji, o których mowa w art. 20 ust. 1l ustawy o Policji, odcisków linii papilarnych lub wymazów ze śluzówki policzków, sposób przeprowadzania i dokumentowania czynności związanych z ich pobieraniem, rodzaje służb policyjnych uprawnionych do korzystania ze zbiorów danych biometrycznych i zbioru danych DNA, o których mowa w art. 21a ust. 1 oraz art. 21h ust. 1 ustawy o Policji, a także sposób zabezpieczenia tych zbiorów. Zgodnie z § 3 rozporządzenia decyzję o pobraniu danych, weryfikacji zasadności ich dalszego przetwarzania oraz poinformowaniu dyrektora CLKP<sup>4</sup> o konieczności ich usunięcia podejmuje kierownik właściwej jednostki organizacyjnej Policji, któremu przyznano kompetencję w tym zakresie i który dokonuje oceny na podstawie zakresu zadań wynikających z karty opisu stanowiska pracy, przy czym Komendant Główny Policji, na wniosek właściwych komendantów, może polecić odstąpienie od pobrania danych albo ich usunięcie i zniszczenie. Stosownie do § 4 i § 5 rozporządzenia odciski linii papilarnych oraz wymazy ze śluzówki policzków pobierane są przez przeszkolonych funkcjonariuszy lub pracowników Policji, a następnie wraz z wymaganą dokumentacją i wnioskiem przekazywane do CLKP, który dokonuje ich weryfikacji, analizy DNA oraz wprowadzenia danych do właściwych zbiorów. Zgodnie z § 6 rozporządzenia dyrektor CLKP informuje o wprowadzeniu lub odmowie wprowadzenia danych do zbiorów, a stosowna dokumentacja podlega włączeniu do akt osobowych. Na podstawie § 7 rozporządzenia dostęp do zbiorów posiadają uprawnione służby policyjne, w szczególności służba kryminalna, śledcza, spraw wewnętrznych oraz zwalczania cyberprzestępczości. Korzystanie ze zbiorów zawierających odciski linii papilarnych lub profile DNA funkcjonariuszy lub pracowników polega na dostępie do informacji, w tym danych osobowych, przetwarzanych w tych zbiorach. Natomiast zgodnie z § 8 rozporządzenia przetwarzanie danych odbywa się wyłącznie przez przeszkolony personel CLKP z zastosowaniem środków zabezpieczających, w tym pseudonimizacji oraz systemów teleinformatycznych wyposażonych w mechanizmy uwierzytelniające użytkownika oraz uniemożliwiające dostęp do tych danych osobom nieuprawnionym.

Za niewykonanie polecenia przełożonego w przedmiocie pobrania odcisków linii papilarnych oraz wymazów ze śluzówki policzków przez policjanta grozi odpowiedzialność dyscyplinarna<sup>5</sup>.

Przetwarzanie danych osobowych na podstawie art. 20 ust. 1l ustawy o Policji, polegające na pobieraniu od funkcjonariuszy i pracowników Policji odcisków linii papilarnych lub wymazów ze śluzówki policzków w celu eliminacji pozostawionych przez nich śladów w toku czynności związanych z ujawnianiem, zabezpieczaniem lub badaniem śladów czynów zabronionych, co do zasady podlega pod reżim stosowania dyrektywy 2016/680<sup>6</sup>, albowiem zasadniczym celem tego przetwarzania jest realizacja

---

<sup>4</sup> Centralne Laboratorium Kryminalistyczne Policji.

<sup>5</sup> Zob. wyrok WSA w Lublinie z 20 grudnia 2022 r. III SA/Lu 455/22.

<sup>6</sup> 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

czynności wykrywczych i dowodowych związanych ze ściganiem przestępstw. Jednocześnie **w zakresie, w jakim dane te są przetwarzane dla celów administracyjnych i kadrowych, w szczególności w związku z dokumentowaniem wykonania obowiązku służbowego, prowadzeniem dokumentacji dotyczącej pobrania materiału biologicznego lub daktyloskopijnego, przechowywaniem informacji w aktach osobowych funkcjonariusza lub pracownika Policji oraz administrowaniem bazą danych od strony organizacyjnej i kadrowej, zastosowanie znajdują przepisy rozporządzenia 2016/679<sup>7</sup>.**

Zasady przetwarzania danych osobowych określone w art. 5 rozporządzenia 2016/679 obejmują m.in. zasadę zgodności z prawem (art. 5 ust. 1 lit. a), zasadę minimalizacji danych (art. 5 ust. 1 lit. c) oraz zasadę ograniczenia przechowywania (art. 5 ust. 1 lit. e). Zasada zgodności z prawem wymaga, aby przetwarzanie danych osobowych odbywało się wyłącznie na podstawie jednej z przesłanek wskazanych w art. 6 rozporządzenia 2016/679 oraz w sposób rzetelny i przejrzysty wobec osoby, której dane dotyczą. Oznacza to konieczność zapewnienia wyraźnej podstawy prawnej przetwarzania, a także zagwarantowania, że zakres i sposób wykorzystywania danych pozostają adekwatne do realizowanego celu i nie naruszają zaufania osób, których dane dotyczą.

Zasada minimalizacji danych nakłada obowiązek przetwarzania wyłącznie takich danych osobowych, które są adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do realizacji określonych celów. W konsekwencji niedopuszczalne jest gromadzenie danych „na zapas” lub w zakresie wykraczającym poza rzeczywiste potrzeby związane z wykonywaniem danego zadania. Każdorazowo należy ocenić, czy zamierzony cel może zostać osiągnięty przy wykorzystaniu węższego zakresu danych. Natomiast zasada ograniczenia przechowywania wymaga, aby dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do realizacji celu, dla którego zostały zebrane. Po osiągnięciu tego celu dane powinny zostać usunięte lub poddane anonimizacji, chyba że obowiązek ich dalszego przechowywania wynika z odrębnych przepisów prawa.

W tym kontekście należy wskazać, że art. 20 ust. 11 ustawy o Policji co do zasady zapewnia podstawę prawną przetwarzania danych biometrycznych i genetycznych funkcjonariuszy Policji, odpowiadając wymogom legalności przetwarzania danych osobowych wynikającym z art. 6 ust. 1 lit. c i e rozporządzenia 2016/679. Przetwarzanie tych danych znajduje bowiem umocowanie w przepisach prawa krajowego, które określają cel ich pobierania oraz wiążą ten obowiązek z realizacją ustawowych zadań Policji związanych z ujawnianiem i zabezpieczaniem śladów w postępowaniach dotyczących czynów zabronionych. Nie przesądza to jednak o pełnej zgodności przyjętych rozwiązań z wymogami ochrony danych osobowych. Wątpliwości budzą bowiem niektóre elementy konstrukcji ustawowej, w szczególności dotyczące zakresu i czasu przechowywania

---

ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, str. 89 ze zm.), dalej jako: dyrektywa 2016/680.

<sup>7</sup> 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 04.05.2016, str. 1, z późn. zm.; dalej jako: rozporządzenie 2016/679.

danych, które należy oceniać także przez pryzmat zasady minimalizacji danych oraz wymogu ograniczenia przetwarzania do przypadków bezwzględnie niezbędnych.

Zgodnie z orzecznictwem Trybunału Konstytucyjnego ograniczenia prawa do prywatności i autonomii informacyjnej jednostki wymagają ustawowej formy<sup>8</sup>. Należy podkreślić, że art. 51 ust. 1 Konstytucji RP stanowi, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Ponadto zgodnie z zasadą proporcjonalności, ograniczenia w zakresie korzystania z konstytucyjnych praw i wolności, w tym prawa do ochrony prywatności (art. 47 Konstytucji RP) i ochrony danych osobowych (art. 51 Konstytucji RP) mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw (art. 31 ust. 3 Konstytucji RP).

W kontekście danych przetwarzanych w bazie danych DNA i bazie danych biometrycznych warto także zwrócić uwagę na bogate orzecznictwo Trybunału Sprawiedliwości UE. Orzecznictwo to odnosi się co prawda do zasad wynikających z dyrektywy 2016/680, jednakże w drodze analogii można je również odnieść do przedstawionego w przedmiotowym piśmie problemu.

W wyroku w sprawie C- 371/24 Comdribus, TSUE przypomniał, że art. 10 dyrektywy 2016/680 przewiduje, że przetwarzanie szczególnych kategorii danych osobowych (w tym danych biometrycznych i genetycznych) jest dopuszczalne wyłącznie w ściśle określonych przypadkach przewidzianych prawem Unii lub państwa członkowskiego oraz pod warunkiem spełnienia dodatkowych wymogów. Obejmują one zapewnienie odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, a także wykazanie, że przetwarzanie jest bezwzględnie niezbędne. Warunek „bezwzględnej niezbędności” należy interpretować w świetle zasad określonych w art. 4 lit. a)-c) i 8 dyrektywy. Oznacza to, **że przetwarzanie musi służyć konkretnym, wyraźnym i prawnie uzasadnionym celom, a zakres danych powinien być adekwatny, stosowny i ograniczony do niezbędnego minimum (zasada minimalizacji). Ponadto przetwarzanie jest zgodne z prawem wyłącznie wtedy, gdy jest konieczne do realizacji zadań właściwych organów, a przepisy krajowe muszą precyzyjnie określać cele, zakres oraz podstawy przetwarzania. Ocena „bezwzględnej niezbędności” powinna być szczególnie rygorystyczna i odnosić się do ściśle określonych, konkretnych celów przetwarzania, odróżnianych od ogólnych powodów jego prowadzenia.** Wymaga ona także weryfikacji, czy zamierzony cel nie może zostać osiągnięty w równie skuteczny sposób przy użyciu mniej wrażliwych danych. Dodatkowo należy uwzględnić wagę celu przetwarzania, w szczególności w kontekście zapobiegania przestępczości, ścigania czynów zabronionych lub ochrony bezpieczeństwa publicznego, a także okoliczności konkretnej sprawy. Państwo członkowskie może zapewnić zgodność z dyrektywą 2016/680 poprzez zobowiązanie właściwych organów do każdorazowej oceny spełnienia wymogu „bezwzględnej

---

<sup>8</sup> Zob. wyrok TK z 18 grudnia 2014 r., sygn. akt K 33/13, wyrok TK z 30 lipca 2014 r. o sygn. akt K 23/11.

niezbędności” przetwarzania danych wrażliwych albo poprzez ustanowienie w przepisach szczegółowych kryteriów takiej oceny. W tym drugim przypadku kryteria te muszą w pełni odpowiadać wszystkim wymogom wynikającym z tego warunku<sup>9</sup>.

W wyroku w sprawie C-57/23 JH vs Policajni prezidium TSUE wskazał, że **brak maksymalnego okresu przechowywania danych biometrycznych i genetycznych nie jest sam w sobie sprzeczny z dyrektywą 2016/680, o ile przepisy krajowe przewidują mechanizmy okresowej kontroli zasadności dalszego przechowywania oraz zapewniają ocenę jego bezwzględnej niezbędności**<sup>10</sup>.

Natomiast w sprawie C-118/22<sup>11</sup>, gdzie przedmiotem sporu była kwestia dopuszczalności bezterminowego przechowywania danych osobowych – w tym danych biometrycznych i genetycznych – osób skazanych, pomimo zatarcia skazania, Trybunał wskazał, że **państwa członkowskie powinny ustanowić odpowiednie okresy usuwania takich danych lub mechanizmy ich regularnej weryfikacji pod kątem dalszej potrzeby przechowywania, a także zapewnić skuteczne procedury gwarantujące przestrzeganie tych zasad**.

Obowiązujące przepisy ustawy o Policji przewidują usuwanie odcisków linii papilarnych i wymazów ze służówki policzków po upływie pięciu lat od ustania stosunku służbowego lub pracy, co wynika z art. 21l ust. 2 pkt 3 w zw. z art. 21h ust. 1 oraz art. 21e ust. 2 pkt 4 w zw. z art. 21a ust. 1 ustawy o Policji. W odniesieniu do danych DNA ustawodawca przewidział dodatkowo procedurę ich usuwania oraz niszczenia próbek biologicznych przez komisję powoływaną przez Komendanta Głównego Policji. Regulacje te realizują częściowo standardy wynikające z orzecznictwa TSUE, w szczególności zakaz bezterminowego przechowywania danych oraz wymóg okresowej weryfikacji ich dalszej przydatności. Nie zmienia to jednak faktu, że przyjęty model retencji nadal budzi zastrzeżenia z perspektywy zasady minimalizacji danych i wymogu „bezwzględnej niezbędności” przetwarzania danych biometrycznych i genetycznych. **Pięcioletni okres przechowywania został określony w sposób sztywny i abstrakcyjny, bez obowiązku indywidualnej oceny dalszej potrzeby przetwarzania danych po ustaniu służby lub zatrudnienia.** Co prawda ustawa przewiduje możliwość wcześniejszego usunięcia danych w razie utraty ich „przydatności eliminacyjnej” w toku weryfikacji prowadzonej na podstawie art. 16 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości<sup>12</sup>, jednak **kryterium to ma charakter niedookreślony i ocenny. Jednocześnie sama procedura weryfikacyjna nie ma charakteru automatycznego ani cyklicznego, lecz zależy od praktyki organizacyjnej organów Policji.** W konsekwencji skuteczność mechanizmu ograniczania retencji danych pozostaje uzależniona od sposobu i częstotliwości inicjowania takich weryfikacji.

---

<sup>9</sup> Wyrok TSUE z 19 marca 2026 r. w sprawie C 371/24, pkt 24-34 i przytoczone tam orzecznictwo.

<sup>10</sup> Wyrok TSUE z 20 listopada 2025 r. w sprawie C-57/23 JH vs Policajni prezidium.

<sup>11</sup> Wyrok TSUE z 30 stycznia 2024 r. w sprawie C-118/22, Direktor na Glavna direktsia „Natsionalna politisia” pri MVR – Sofia, pkt 43-44.

<sup>12</sup> Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2023 r. poz. 1206 ze zm.).

Trzeba również zauważyć, że samo pobieranie od funkcjonariuszy i pracowników Policji odcisków linii papilarnych oraz wymazów ze słuzówki policzków znajduje podstawę w przepisach ustawowych, o tyle kwestie dotyczące wyboru osób, od których dane te mają zostać pobrane, zostały uregulowane na poziomie aktu wykonawczego. Zgodnie z § 3 ust. 1 pkt 1 rozporządzenia decyzję o „typowaniu” konkretnego funkcjonariusza lub pracownika Policji podejmuje kierownik jednostki organizacyjnej Policji właściwej ze względu na miejsce pełnienia służby lub zatrudnienia. Decyzja ta ma być poprzedzona analizą zakresu obowiązków wynikających z karty opisu stanowiska pracy (§ 3 ust. 1 *in principio* rozporządzenia). W praktyce oznacza to, że przesłanki decydujące o objęciu określonej kategorii osób obowiązkiem przekazania danych biometrycznych i genetycznych zostały pozostawione do uregulowania w akcie podustawowym.

Takie rozwiązanie budzi istotne wątpliwości konstytucyjne. Upoważnienie zawarte w art. 20 ust. 1m ustawy o Policji nie obejmuje bowiem kompetencji do określania materialnych przesłanek pobierania danych, w szczególności warunków ich pozyskiwania od określonych grup funkcjonariuszy i pracowników Policji. Materia ta, jako dotycząca zakresu ingerencji w prawo do prywatności oraz ochrony danych osobowych, powinna zostać uregulowana bezpośrednio w ustawie. Tymczasem rozporządzenie w praktyce współkształtuje zakres podmiotowy obowiązku przekazywania danych, a więc ingeruje w materię zastrzeżoną dla ustawodawcy. Wątpliwości w tym zakresie podnosił również Rzecznik Praw Obywatelskich, wskazując, że prowadzi to do niedopuszczalnej modyfikacji normy ustawowej przez akt wykonawczy, pozostającej w sprzeczności zarówno z konstytucyjną hierarchią źródeł prawa (art. 87 ust. 1 Konstytucji RP), jak i z granicami delegacji ustawowej określonymi w art. 92 ust. 1 Konstytucji RP<sup>13</sup>. W toku prac legislacyjnych nad projektem rozporządzenia uwagi co do zgodności § 3 ust. 2 Konstytucją RP zgłaszało również Rządowe Centrum Legislacji<sup>14</sup>.

**Analiza obowiązujących regulacji prowadzi zatem do wniosku, że obecny model przetwarzania danych biometrycznych i genetycznych funkcjonariuszy oraz pracowników Policji nie zapewnia pełnej zgodności z zasadami ochrony danych osobowych oraz standardami wynikającymi zarówno z Konstytucji RP, jak i orzecznictwa TSUE.** Zastrzeżenia dotyczą w szczególności oparcia części materialnych przesłanek przetwarzania danych na regulacji podustawowej, mimo że powinny one wynikać bezpośrednio z ustawy, a także niewystarczającego urzeczywistnienia zasad minimalizacji i ograniczenia retencji danych poprzez przyjęcie sztywnego pięcioletniego okresu przechowywania bez obowiązku indywidualnej i regularnej oceny dalszej konieczności przetwarzania danych.

Dlatego też, w ocenie Prezesa UODO, podjęcia wymagają prace legislacyjne w zakresie doprecyzowania przepisów ustawowych odnoszących się do zasad przetwarzania danych biometrycznych i genetycznych funkcjonariuszy oraz pracowników Policji, w szczególności poprzez ustawowe określenie materialnych przesłanek ich przetwarzania oraz zapewnienie zgodności zasad retencji danych z wymogami

---

<sup>13</sup> Zob. <https://bip.brpo.gov.pl/pl/content/szef-mswia-nieprawidlowo-okreslil-zasady-pobierania-odciskow-linii-papilarnych-policjantow>

<sup>14</sup> Zob. <https://legislacja.gov.pl/docs//513/12321958/12598843/12598846/dokument437661.pdf>

minimalizacji i okresowej oceny niezbędności dalszego przetwarzania, a także dostosowanie rozporządzenia MSWiA do standardów konstytucyjnych.

W tym miejscu trzeba również zauważyć, że Prezes UODO – oceniając skutki wyroku TSUE w sprawie C-57/23<sup>15</sup> – sygnalizował, że usuwanie danych osobowych ze zbiorów danych daktyloskopijnych odbywa się na takich samych zasadach jak usuwanie danych ze zbioru DNA, a weryfikacja zasadności dalszego przetwarzania danych następuje w trybie art. 16 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (art. 21e ust. 1 oraz 21l ust. 1 ustawy o Policji). Jednocześnie przepisy ustawy o Policji nie precyzują przesłanek usuwania danych ani pojęcia „zbędności dalszego przetwarzania danych”, pozostawiając administratorowi szeroką swobodę decyzyjną, co uzasadnia potrzebę ustawowego doprecyzowania tych przesłanek.

Mając na uwadze powyższe, uprzejmie proszę Pana Ministra o odniesienie się do tego wystąpienia na piśmie, **w terminie 30 dni** od daty jego otrzymania.

W przypadku podjęcia prac legislacyjnych w związku z przedstawionym powyżej zagadnieniem Prezes UODO deklaruje swoje wsparcie eksperckie celem wypracowania rozwiązań uwzględniających przepisy o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski  
Prezes Urzędu  
Ochrony Danych Osobowych

---

<sup>15</sup> Pismo do Sekretarza Stanu w MSZ z 14.01.2026 r. znak DOL.0623.9.2023.