



Warszawa, 02-12-2024 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

VII.501.23.2023.PKR

Pan

Tomasz Siemoniak

**Minister Spraw Wewnętrznych
i Administracji**

**Ministerstwo Spraw Wewnętrznych
i Administracji
ePUAP**

Szanowny Panie Ministrze,

do Rzecznika Praw Obywatelskich wpłynęła skarga dotycząca przechowywania i przetwarzania danych osobowych w policyjnych bazach danych – Krajowym Centrum Informacji Kryminalnych (KCIK) oraz Elektronicznym Rejestrze Czynności Dochodzeniowo-Śledczych (ERCDS) po zatarciu skazania.

Jak wynika ze skargi, wobec Skarżącego został wydany wyrok, w którym uznano go za winnego zarzucanych mu czynów i wymierzono mu karę pozbawienia wolności, której wykonanie warunkowo zawieszono na okres próby oraz karę grzywny. Dodatkowo, Skarżący został zobowiązany do zapłacenia określonej kwoty tytułem wynagrodzenia wyrządzonej szkody. Skarżący karę wykonał, a skazanie uległo zatarciu z mocy prawa. W dalszej części skargi wskazano, że od czasu skazania upłynęło ponad 5 lat, natomiast od momentu popełnienia zarzucanych Skarżącemu czynów ponad 22 lata, od tego też czasu nie miał on żadnego konfliktu z prawem oraz nie było wobec niego prowadzone żadne postępowania karne ani przygotowawcze. Skarżący podkreśla także, że popełnione przez niego przestępstwo cechowało się niską społecznością

szkodliwością, o czym świadczy fakt zastosowania przez sąd instytucji warunkowego zawieszenia wykonania kary.

Mimo tego, że dane dotyczące skazania Skarżącego zostały usunięte z mocy prawa z Krajowego Rejestru Karnego, to nadal są przechowywane w policyjnych bazach danych – Krajowym Centrum Informacji Kryminalnych (KCIK) oraz Elektronicznym Rejestrze Czynności Dochodzeniowo-Śledczych (ERCDS). Skarżący wskazał, że dalsze przechowywanie jego danych w policyjnych rejestrach- KCIK oraz ERCDS uniemożliwia mu uzyskanie pracy z dostępem do danych niejawnych, wymagającej posiadania nieposzlakowanej opinii, a także możliwość poszukiwania zatrudnienia w krajach objętych systemem wizowym, w których konieczne jest udowodnienie niekaralności, tj. USA, Australii, Nowej Zelandii, Kanadzie oraz Wielkiej Brytanii. W ocenie Skarżącego, ustał cel przetwarzania jego danych osobowych w tych systemach.

Zgodnie z motywem drugim dyrektywy 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 uchylenia decyzji ramowej Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89, dalej jako: dyrektywa 2016/680), zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od ich obywatelstwa czy miejsca zamieszkania – przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych.

W myśl art. 4 ust. 1 dyrektywy 2016/680, państwa członkowskie zapewniają, by dane osobowe były:

- a) przetwarzane zgodnie z prawem i rzetelnie;
- b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;
- c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Natomiast w art. 5 dyrektywy 2016/680 wskazano, że państwa członkowskie zapewniają, by przyjęto odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych.

Przestrzeganiu tych terminów służą odpowiednie środki proceduralne.

Dyrektywa 2016/680 została wdrożona do polskiego systemu prawnego ustawą 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, dalej jako:

o.d.o.). W myśl art. 16 ust. 1 o.d.o. administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, regulujące działania właściwego organu, a jeżeli przepisy te nie określają terminu – nie rzadziej niż co 10 lat od dnia zebrania, uzyskania, pobrania lub aktualizacji danych. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane usuwa się, z zastrzeżeniem art. 17¹ (ust. 2).

Natomiast stosownie do art. 24 ust. 1 o.d.o. osoba, której dane dotyczą, może wystąpić z wnioskiem do administratora o niezwłoczne:

- 1) uzupełnienie, uaktualnienie lub sprostowanie danych osobowych – w przypadku, gdy dane te są niekompletne, nieaktualne lub nieprawdziwe;
- 2) usunięcie danych osobowych – w przypadku, gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów niniejszej ustawy.

Przepis art. 20 ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2024 r. poz. 145 ze zm.) stanowi, że w celu realizacji zadań ustawowych Policja jest uprawniona do

¹ Zgodnie z art. 17 o.d.o., dane osobowe uznane za zbędne można przekształcić w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo w taki sposób, że przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

przetwarzania informacji, w tym danych osobowych, z zachowaniem ograniczeń wynikających z art. 19. Danych osobowych, o których mowa w art. 14 ust. 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej (ust. 2c).

Krajowe Centrum Informacji Kryminalnych zostało utworzone ustawą z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (Dz.U. z 2024 poz. 376 ze zm.).

Zgodnie z art. 13 ustawy o przetwarzaniu informacji kryminalnych:

1. Zakres przetwarzanych informacji kryminalnych obejmuje następujące dane: 1) datę i miejsce popełnienia przestępstwa; 2) rodzaj popełnionego przestępstwa i kwalifikację prawną czynu; 3) sygnaturę akt, pod którą zostały zarejestrowane czynności lub postępowanie; 4) nazwę organu lub jednostki organizacyjnej prowadzącej czynności lub postępowanie oraz informację o sposobie nawiązania kontaktu z tym organem lub jednostką organizacyjną; 5) informacje o: a) osobach, przeciwko którym prowadzone jest postępowanie karne, w tym postępowanie w sprawach o przestępstwa skarbowe, lub w stosunku do których prowadzone są czynności operacyjno-rozpoznawcze, b) przedmiotach, w tym nieruchomościach, wykorzystanych do popełnienia przestępstwa, uzyskanych w wyniku przestępstwa lub utraconych w związku z przestępstwem, c) przedsiębiorcach, spółkach cywilnych, fundacjach, stowarzyszeniach, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa, zgromadzone w rejestrach prowadzonych na podstawie odrębnych przepisów, d) numerach rachunków bankowych lub rachunków papierów wartościowych, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa lub że gromadzone są na nich środki pochodzące z przestępstwa,

e) innych postępowaniach lub czynnościach prowadzonych na podstawie ustaw przez podmioty, o których mowa w art. 19 i 20, istotnych z punktu widzenia czynności operacyjno-rozpoznawczych lub postępowania karnego, w tym postępowania w sprawach o przestępstwa skarbowe.

2. Informacje, o których mowa w ust. 1 pkt 5 lit. a, obejmują: 1) dane personalne: a) nazwisko, b) imiona, c) imiona i nazwiska poprzednie, d) imiona rodziców i nazwisko rodowe matki, e) datę i miejsce urodzenia, f) płeć, g) pseudonim, h) adres miejsca zameldowania, i) adres miejsca pobytu, j) cechy dokumentów tożsamości: rodzaj dokumentu, datę wystawienia dokumentu, organ wystawiający dokument, numer,

serię dokumentu, k) numer ewidencyjny Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub obywatelstwo, w przypadku cudzoziemca nieposiadającego numeru PESEL, l) numer identyfikacji podatkowej NIP, m) numer identyfikacyjny REGON;

2) inne dane przekazane przez podmioty, o których mowa w art. 19 i 20, pozwalające na określenie tożsamości osoby, a w szczególności rysopis i przynależność do grupy przestępczej.

W art. 14 ust. 1 ustawy o przetwarzaniu informacji kryminalnych wskazano, że informacje kryminalne, o których mowa w art. 13 ust. 1 pkt 1-4 oraz pkt 5 lit. a i e, są przechowywane w bazach danych przez okres 15 lat. Natomiast w art. 25 wskazano, że informacje kryminalne podlegają usunięciu z baz danych, jeżeli:

- 1) ich gromadzenie jest zabronione;
- 2) zarejestrowane informacje kryminalne okazały się nieprawdziwe;
- 3) ustał cel ich gromadzenia;
- 4) upłyną okresy, o których mowa w art. 14 ust. 1-3;
- 5) jest to uzasadnione ze względu na bezpieczeństwo państwa lub jego obronność albo mogą spowodować identyfikację osób udzielających pomocy przy wykonywaniu czynności operacyjno-rozpoznawczych prowadzonych przez upoważnione do tego podmioty uprawnione.

W § 1 zarządzenia nr 31 Komendanta Głównego Policji z dnia 6 października 2020 r. w sprawie funkcjonowania Elektronicznego Rejestru Czynności Dochodzeniowo-Śledczych (Dz. Urz. KGP. z 2020 r. poz. 53, dalej jako: zarządzenie nr 31) określono, że Elektroniczny Rejestr Czynności Dochodzeniowo-Śledczych, zwany dalej "ERCDS" prowadzi się w Komendzie Głównej Policji w systemach teleinformatycznych Policji, jako system służący do przetwarzania w formie elektronicznej, w sposób zautomatyzowany, informacji i danych osobowych gromadzonych przez Policję w urządzeniach ewidencyjnych w ramach prowadzonych postępowań karnych, karnych skarbowych i w sprawach nieletnich.

Przepis § 25 zarządzenia nr 31 stanowi, że w ERCDS przetwarza się informacje i dane osobowe w odniesieniu do: 1) podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego; 2) podejrzanych (oskarżonych), wobec których w toku

postępowania karnego lub postępowania karnego skarbowego zastosowano środek zapobiegawczy w postaci oddania podejrzanego (oskarżonego) pod dozór Policji; 3) nieletnich dopuszczających się czynów zabronionych przez ustawę, jako przestępstwa ścigane z oskarżenia publicznego; 4) zawiadamiających o popełnieniu przestępstwa; 5) pokrzywdzonych, o których mowa w art. 49 k.p.k.; 6) biegłych i tłumaczach, o których mowa w rozdziale 22 k.p.k.; 7) referentów ERCDŚ; 8) użytkowników ERCDŚ.

2. Informacje, w tym dane osobowe osób, o których mowa w ust. 1 pkt 1-3, obejmują:

1) imiona, nazwiska, w tym nazwisko rodowe lub pseudonimy; 2) imiona i nazwiska rodowe rodziców; 3) datę i miejsce urodzenia; 4) oznaczenie i cechy identyfikacyjne dokumentu tożsamości; 5) obywatelstwo; 6) numer PESEL; 7) adres zamieszkania i adres pobytu; 8) dane kontaktowe (np. numer telefonu, adres poczty elektronicznej); 9) identyfikator KSIP osoby (OIO); 10) inne dane, za wyjątkiem danych wrażliwych, o których mowa w art. 14 ust. 1 UDODO.

W myśl § 34 zarządzenia nr 31, weryfikując informacje, w tym dane osobowe w ERCDŚ, pod kątem ich przydatności, uwzględnia się:

- 1) czas, który upłynął od wprowadzenia informacji, w tym danych osobowych, do ERCDŚ do momentu dokonywania oceny;
- 2) podstawy wprowadzenia informacji, w tym danych osobowych oraz ich prawdziwość;
- 3) aktualność przesłanek legalności oraz niezbędności dalszego przetwarzania informacji, w tym danych osobowych, do wykonania zadań ustawowych Policji;
- 4) powzięcie przez organ Policji wiarygodnej informacji, że:
 - a) czynu stanowiącego podstawę wprowadzenia informacji, w tym danych osobowych, do ERCDŚ nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia,
 - b) zdarzenie lub okoliczność, w związku z którymi wprowadzono informacje, w tym dane osobowe, do ERCDŚ nie ma znamion czynu zabronionego,
 - c) osoba, której dane dotyczą, została uniewinniona prawomocnym wyrokiem sądu.

W § 35 pkt. 2 zarządzenia nr 31 wskazano, że weryfikacji, o której mowa w § 33, kierownicy jednostek i komórek organizacyjnych Policji lub upoważnieni w tym zakresie policjanci i pracownicy Policji dokonują z wykorzystaniem informacji, w tym danych osobowych zawartych we wnioskach osób, których dane dotyczą, złożonych w trybie przepisów rozdziału 4 UDODO. Natomiast w § 36 zarządzenia przewidziano, że dane osobowe uznane za zbędne podlegają wyłącznie pseudonimizacji. Usunięciu podlegają jedynie dane, które zostały wprowadzone bezzasadnie lub są nieprawdziwe.

W zarządzeniu nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji (KSIP) (Dz. Urz. KGP. Z 2019 r. poz. 114, dalej jako: zarządzenie nr 70) wskazano, jakie systemy teleinformatyczne składają się na KSIP i jakie dane osobowe oraz informacje się w nich przetwarzają (§ 4-5 a). W rozdziale 15 zarządzenia nr 70, podobnie jak w przypadku systemu ERCDS, przewidziano procedurę weryfikacji i usuwania informacji, w tym danych osobowych z KSIP. Weryfikacji informacji, w tym danych osobowych, przetwarzanych w KSIP w celu ustalenia, czy istnieją informacje, których dalsze przechowywanie jest zbędne oraz w zakresie legalności, prawidłowości i aktualności przetwarzanych informacji, dokonują jednostki i komórki organizacyjne Policji, które zarejestrowały informacje w zbiorze danych KSIP (§ 104 ust. 1 zarządzenia nr 70).

W myśl § 105 ust. 1 zarządzenia nr 70, weryfikując informacje, w tym dane osobowe, przetwarzane w celu wykrywania przestępstw, pod kątem ich przydatności, uwzględnia się:

- 1) rodzaj i charakter popełnionego czynu wyczerpującego znamiona przestępstwa;
- 2) rodzaj i charakter dobra chronionego prawem naruszonego popełnionym przestępstwem;
- 3) formy sprawstwa i umyślności popełnienia przestępstwa;
- 4) postaci zamiaru i skutki czynu, w tym rodzaj i rozmiar wyrządzonej lub grożącej szkody;
- 5) zagrożenie sankcją karną za popełnione przestępstwo;
- 6) liczbę popełnionych przestępstw;
- 7) czas, który upłynął od momentu wprowadzenia informacji, w tym danych osobowych, do zbiorów danych KSIP do momentu dokonywania oceny;

- 8) inne przetwarzane w zbiorach danych KSIP informacje o osobie;
- 9) podstawy uzyskania, pobrania lub zgromadzenia informacji, w tym danych osobowych oraz ich prawidłowość;
- 10) aktualność przesłanek legalności oraz niezbędności dalszego przetwarzania informacji, w tym danych osobowych, do wykonania zadań ustawowych Policji;
- 11) wystąpienie okoliczności określonych w art. 16 ust. 2 zdanie drugie, art. 24 ust. 2 i 4 oraz art. 31 ust. 2 ustawy ODO przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz w przypadku:
 - a) danych daktyloskopijnych wystąpienie okoliczności określonych w art. 211 ust. 2 i art. 21m ustawy o Policji,
 - b) informacji dotyczących wyników analizy kwasu deoksyrybonukleinowego (DNA), wystąpienie przesłanek i okoliczności określonych w art. 21e ust. 2-4 ustawy o Policji,
 - c) informacji, w tym danych osobowych, przetwarzanych w rejestrze wykroczeń, wystąpienie przesłanek i okoliczności określonych w art. 20f ust. 14-16 ustawy o Policji;
- 12) powzięcie przez organ Policji wiarygodnej informacji, że:
 - a) czynu stanowiącego podstawę wprowadzenia informacji, w tym danych osobowych, do zbiorów danych KSIP nie popełniono albo brak jest danych dostatecznie uzasadniających podejrzenie jego popełnienia;
 - b) zdarzenie lub okoliczność, w związku z którymi wprowadzono informacje, w tym dane osobowe, do zbiorów danych KSIP, nie ma znamion czynu zabronionego;
 - c) osoba, której dane dotyczą, została uniewinniona prawomocnym wyrokiem sądu.

Dane z ERCDS, KSIP oraz KCIK mogą być udostępnione innym podmiotom (art. 16 ust. 2 i 3 ustawy o przetwarzaniu informacji kryminalnych, rozdział 12 zarządzenia nr 70, rozdział 8 zarządzenia nr 31).

Jakkolwiek Rzecznik Praw Obywatelskich rozumie potrzebę gromadzenia przez policję danych o osobach, które popełniły przestępstwo lub wykroczenie, to zaniepokojenie budzi fakt, że dane te są przechowywane w policyjnych systemach nawet po zatartiu skazania, kiedy ustał cel ich gromadzenia, zaś osobie uprawnionej nie przysługują

skuteczne środki prawne, które zobligowałyby administratora danych do ich usunięcia. Nie można również nie zauważyć, że zakres przechowywanych w tych systemach danych osobowych został określony bardzo szeroko.

Zaznaczenia przy tym wymaga, że w myśl art. 106 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2024 r. poz. 17 ze zm.), z chwilą zatarcia skazania uważa się je za niebyłe; wpis o skazaniu usuwa się z rejestru skazanych. Stosownie do art. 14 ust 1 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. z 2024 r. poz. 276) dane osobowe osób, o których mowa w art. 1 ust. 2 pkt 1, 3 i 7, oraz dane o podmiotach zbiorowych, o których mowa w art. 1 ust. 3, usuwa się z Rejestru, jeżeli z mocy prawa skazanie uległo zatarciu, a ponadto po otrzymaniu zawiadomienia o zarządzeniu zatarcia skazania przez sąd, na podstawie art. 107 § 2 oraz art. 337 Kodeksu karnego (pkt. 1).

Krajowe Centrum Informacji Kryminalnej służy przede wszystkim do wykrycia sprawcy przestępstwa, a więc nie powinno gromadzić wpisów o osobach, które za popełnienie określonego przestępstwa zostały skazane, a skazanie to uległo zatarciu. Skoro ustawodawca uznał, że po upływie określonego czasu od wykonania kary nie ma potrzeby przechowywania informacji o skazaniu w Krajowym Rejestrze Karnym, to niekonsekwencją byłoby, gdyby uznał jednocześnie, iż dane te należy przechowywać w rejestrze mającym na celu ułatwienie wykrywania przestępstw, gdyż w tym przypadku cel ten z pewnością został osiągnięty². Skoro zatem po zatarciu skazania następuje usunięcie wpisu o skazaniu z najbardziej powszechnego rejestru, jakim jest Krajowy Rejestr Karny, to niezrozumiałym jest dlaczego w unormowaniach dotyczących policyjnych systemów (KCIK, KSIP, ERCDS) fakt ten nie jest w ogóle brany pod uwagę.

Zdaniem Rzecznika, w świetle aktualnych unormowań dotyczących poszczególnych policyjnych systemów, można byłoby zaprzestać przetwarzania danych osobowych osoby, wobec której nastąpiło zatarcie skazania. Możliwość taką stwarzają przepisy: ustawy o przetwarzaniu informacji kryminalnych (art. 25 pkt. 3), zarządzenia nr 31 (§ 35 pkt 2 w zw. z § 34 pkt 3), zarządzenia nr 70 (§105 ust. 1pkt 10), zwłaszcza gdy z właściwym wnioskiem do administratora zwróci się zainteresowana osoba.

Dodatkowo, nie bez znaczenia dla przyjęcia takiej interpretacji jest art. 20 ust. 2c ustawy o Policji, gdzie wskazano, że danych osobowych, o których mowa w art. 14 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i

² D. Kwiatkowski, Obowiązek usunięcia z rejestrów wpisu o zatartym skazaniu, „Palestra” 2020, nr 3.

zwalczaniem przestępczości, nie pobiera się, w przypadku gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej.

W tym kontekście warto także zwrócić uwagę, że wykładnia przepisów ustawy o przetwarzaniu informacji kryminalnych, które przewidują, że dane usuwa się z rejestru, gdy ustał cel ich gromadzenia (art. 25 pkt 3), powinna prowadzić do wniosku, że dane te po zatarciu skazania podlegają usunięciu. Jednakże z niezrozumiałych przyczyn ww. przepis interpretuje się w ten sposób, że dobrowolne poddanie się karze i zatarcie skazania nie stanowią w myśl art. 25 ustawy z 2001 r. o przetwarzaniu informacji kryminalnych przesłanek do usunięcia informacji kryminalnych z baz danych KCiK³.

Warto również zwrócić uwagę na wyrok Trybunału Sprawiedliwości UE z dnia 30 stycznia 2024 r. w sprawie C 118/22. W sprawie tej, dane osobowe obywatela Bułgarii zostały wpisane do rejestru policyjnego w toku dochodzenia prowadzonego w sprawie popełnienia przez niego przestępstwa złożenia fałszywych zeznań. Po zakończeniu dochodzenia został on uznany za winnego i skazany na karę ograniczenia wolności. Po odbyciu kary i zatarciu skazania, złożył wniosek o wykreślenie wpisu w rejestrze policyjnym. Wniosek nie został uwzględniony, dlatego obywatel Bułgarii wniósł skargę do sądu. Wskazał, że przepisy bułgarskiego prawa są niezgodne z prawem UE, gdyż nie przewidują odpowiedniego terminu usunięcia danych osobowych. Stanowią, że wpis w rejestrze policyjnym, obejmujący dane wrażliwe (odciski palców, wizerunek, próbki pozwalające na ustalenie profilu DNA), może być usunięty, jedynie w przypadku gdy zarejestrowanie nastąpiło z naruszeniem prawa, postępowanie karne zostało umorzone lub zakończyło się uniewinnieniem, na podmiot danych nałożono karę administracyjną zamiast odpowiedzialności karnej, podmiot danych zmarł. Zatem dane osobowe osoby skazanej są przechowywane w bułgarskim rejestrze policyjnym zawsze aż do śmierci podmiotu danych. Sąd bułgarski zwrócił się do TSUE z pytaniami prejudycjalnymi dotyczącymi zgodności bułgarskiego prawa z dyrektywą 2016/680.

TSUE zauważył, że przechowywanie w rejestrze policyjnym danych dotyczących osób, które zostały prawomocnie skazane, może w niektórych przypadkach okazać się niezbędne, nawet po usunięciu tego skazania z rejestru karnego i gdy w konsekwencji skutki, jakie ustawodawstwo krajowe wiąże z tym skazaniem, zostają uchylone. Osoby te mogą bowiem brać udział w popełnieniu przestępstw innych niż te, za które zostały skazane, lub przeciwnie, zostać oczyszczone w drodze porównania danych

³ Decyzja PUODO z dnia 10 kwietnia 2019 r. sygn. ZSOŚS.440.23.2019.

przechowywanych przez te organy z danymi zebranymi podczas postępowań dotyczących tych innych przestępstw. Takie przechowywanie danych może przyczyniać się do realizacji celu interesu ogólnego wymienionego w motywie 27 dyrektywy 2016/680. W kontekście okresu przechowywania danych osobowych, TSUE zauważył, że jedynie w sytuacji prawomocnego skazania osoby, której dane dotyczą, za umyślne przestępstwo ścigane z oskarżenia publicznego przechowywanie wspomnianych danych zostaje utrzymane do chwili śmierci tej osoby, ponieważ w innych przypadkach ustawodawstwo krajowe przewiduje wykreślenie wpisów osób ściganych za takie przestępstwo. W tym względzie TSUE jednak stwierdził, że pojęcie „umyślnego przestępstwa ściganego z oskarżenia publicznego” ma wyjątkowo ogólny charakter i może mieć zastosowanie do znacznej liczby czynów zabronionych – niezależnie od ich charakteru i wagi. W orzeczeniu podkreślono, że w niektórych przypadkach, biorąc pod uwagę czynniki takie jak charakter i waga popełnionego przestępstwa lub brak powrotu do przestępstwa, ryzyko, jakie stanowi osoba skazana, niekoniecznie będzie uzasadniać utrzymanie do chwili jej śmierci dotyczących jej danych w przewidzianym w tym celu krajowym rejestrze policyjnym. W takich przypadkach nie będzie już niezbędnego związku między przechowywanymi danymi a zamierzonym celem. Ich przechowywanie, zdaniem Trybunału, nie będzie zatem zgodne z zasadą minimalizacji danych ustanowioną w art. 4 ust. 1 lit. c dyrektywy 2016/680 i będzie wykraczać poza okres niezbędny do celów, dla których są one przetwarzane, wbrew art. 4 ust. 1 lit. e tej dyrektywy.

TSUE zaznaczył, że w okolicznościach badanej sprawy zatarcie skazania, pociągające za sobą usunięcie wydanego wobec określonej osoby wyroku skazującego z rejestru karnego, nie może samo w sobie czynić zbędnym przechowywania jej danych w rejestrze policyjnym, ponieważ przechowywanie to służy celom innym niż dane o jej uprzedniej karalności we wspomnianym rejestrze karnym. Jednocześnie jednak Trybunał wskazał, że jeżeli, jak w przedmiotowej sprawie, na mocy przepisów mających zastosowanie do krajowego prawa karnego takie zatarcie skazania jest uzależnione od braku popełnienia nowego umyślnego przestępstwa ściganego z oskarżenia publicznego przez pewien okres po odbyciu kary, może ono stanowić wskazówkę co do mniejszego ryzyka, jakie stanowi osoba, której dane dotyczą, w świetle celów zwalczania przestępczości lub utrzymania porządku publicznego, a zatem element mogący skrócić niezbędny okres takiego przechowywania (pkt 58-61).

W świetle powyższego wyroku TSUE, w ocenie Rzecznika Praw Obywatelskich, zasadnym wydaje się zweryfikowanie przepisów o policyjnych bazach danych (KCIK, KSIP, ERCDS), w szczególności zaś ich wykładni i sposobu stosowania w praktyce i

rozważenie wprowadzenia takich zmian, które umożliwią usunięcie danych osobowych dotyczących osoby, wobec której nastąpiło zatarcie skazania lub pseudonimizację takich danych po zatarciu skazania, zwłaszcza jeśli przestępstwo było mniejszej wagi, zaś w kolejnych latach osoba taka nie popełniła kolejnego przestępstwa. Pozbawienie osoby, wobec której funkcja wychowawcza prawa karnego odniosła skutek możliwości pełnego korzystania ze swoich praw, z powodu pozostawienia jej danych osobowych w rejestrach policyjnych, mimo ustania celu i niezbędności przetwarzania tych danych, jest w ocenie Rzecznika Praw Obywatelskich stygmatyzujące.

W związku z powyższym, działając na podstawie art. 13 ust. 1 pkt 2 i art. 16 ust. 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r. poz. 1264 ze zm.), zwracam się do Pana Ministra o zajęcie stanowiska w przedmiotowej sprawie i powiadomienie Rzecznik Praw Obywatelskich o podjętych działaniach.

Z poważaniem

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Do wiadomości:

Pan insp. Marek Boroń

Komendant Główny Policji

mail: informacjapubliczna.kgp@policja.gov.pl