PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 17.05.2024 r.

DOL.0623.10.2022

Pan
Adam Szłapka
Minister do spraw Unii Europejskiej

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa

Szanowny Panie Ministrze,

w odpowiedzi na korespondencję z dnia 26 lutego 2024 r. dotyczącą skutków wyroku Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE) z dnia 30 stycznia 2024 r. w sprawie o **sygn. C- 118/22 *Direktor na Glavna direktsia „Natsionalna politsia" pri Ministerstvo na vatreshnite raboti - Sofia* (ochrona danych osobowych – przetwarzanie danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości)** uprzejmie informuję, że w ocenie Prezesa Urzędu Ochrony Danych (dalej jako: organ nadzorczy) wyrok ten pociąga za sobą konieczność rozważenia zmiany ustawy z dnia 6 kwietnia 1990 r. o Policji[1] w zakresie przepisów regulujących działanie Krajowego Systemu Informacyjnego Policji.

W sentencji wyroku TSUE uznał, że:

[1] Ustawa o Policji z dnia 6 kwietnia 1990 r. (Dz. U. z 2024 r. poz. 145).

Art. 4 ust. 1 lit. c) i e) dyrektywy 2016/680[2] w zw. z art. 5 i 10, art. 13 ust. 2 lit. b) oraz art. 16 ust. 2 i 3 tej dyrektywy i art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej[3] należy interpretować w ten sposób, iż stoi on na przeszkodzie ustawodawstwu krajowemu przewidującemu przechowywanie przez organy policji do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, danych osobowych, w szczególności danych biometrycznych i genetycznych, dotyczących osób, które zostały prawomocnie skazane za umyślne przestępstwo ścigane z oskarżenia publicznego, aż do chwili śmierci osoby, której dane dotyczą, w tym w przypadku zatarcia skazania tej osoby, **bez nałożenia na administratora obowiązku okresowego przeglądu, czy takie przechowywanie jest nadal niezbędne, ani przyznania wspomnianej osobie prawa do usunięcia tych danych**, od chwili gdy ich przechowywanie nie jest już niezbędne do celów, dla których były one przetwarzane, lub w stosownym przypadku do ograniczenia ich przetwarzania.

Trybunał wskazał przy tym (pkt 39 wyroku), że gwarantowane w art. 7 i 8 Karty Praw Podstawowych UE prawa do poszanowania życia prywatnego i ochrony danych osobowych nie mają charakteru absolutnego, niemniej wszelkie ograniczenia w korzystaniu z nich powinny być przewidziane ustawą i szanować ich istotę oraz zasadę proporcjonalności. Na podstawie tej ostatniej zasady ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Powinny one mieścić się w granicach tego, co absolutnie konieczne, a uregulowanie dotyczące rozpatrywania ograniczeń musi zawierać jasne i precyzyjne zasady regulujące zakres i stosowanie tych ograniczeń (podobnie wyrok z dnia 22 czerwca 2021 r., Latvijas Republikas Saeima w sprawie C-439/19, EU:C:2021:504, pkt 110 i przytoczone tam orzecznictwo).

Przed dalszymi rozważaniami należy podkreślić, że omawiany wyrok został wydany w stanie faktycznym i prawnym, w którym dane o skazaniu były przetwarzane w bazach policyjnych bez ograniczenia czasowego a osoba, której dane dotyczą, nie miała przyznanego prawa podmiotowego do żądania usunięcia tych danych. Jedynym przypadkiem, w którym ustawodawstwo krajowe przewidywało usunięcie danych o skazaniu była śmierć osoby skazanej.

W polskim prawie przetwarzanie danych przez organy Policji dotyczących skazania odbywa się na podstawie przepisów ustawy o Krajowym Rejestrze Karnym[4] (dalej jako: „ustawa o KRK”), ustawy o przetwarzaniu informacji kryminalnych (dalej

---

[2] 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 uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.5.2016, str. 89 ze zm.).

[3] Dz. Urz. UE C 202 z 7.6.2016, str. 389.

[4] Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2024 r., poz. 276).

jako: „ustawa o PIK")[5] oraz ustawy o Policji, regulującej funkcjonowanie Krajowego Systemu Informacyjnego Policji (dalej jako: „KSIP").

Jak wskazuje przepis art. 1 ust. 2 pkt 1 ustawy o KRK, w rejestrze gromadzi się dane o osobach prawomocnie skazanych za przestępstwa lub przestępstwa skarbowe. Zgodnie z art. 14 ust. 1 ustawy o KRK dane osobowe osób prawomocnie skazanych za przestępstwa lub przestępstwa skarbowe usuwa się z rejestru, jeżeli z mocy prawa skazanie uległo zatarciu.

W ocenie Prezesa Urzędu Ochrony Danych obecnie **ustawa o KRK nie zawiera przepisów, które nie spełniają standardów prawnych wynikających z przedmiotowego wyroku TSUE**, gdyż z jej przepisów wynika, że administrator danych zawartych w KRK po zatarciu skazania z mocy samego prawa zobowiązany jest do usunięcia danych osobowych osób prawomocnie skazanych. Podmiot danych nie musi występować z wnioskiem.

Fakt zatarcia skazania nie jest natomiast przesłanką usunięcia danych z bazy danych prowadzonej w Krajowym Centrum Informacji Kryminalnych (dalej jako „baza KCIK"). Na zasadach określonych w ustawie o PIK informacje kryminalne przetwarza się w celu wykrywania i ścigania sprawców przestępstw oraz zapobiegania i zwalczania przestępczości. Informacje kryminalne przetwarza się bez wiedzy i zgody osoby, której dane dotyczą, oraz z zachowaniem zasad ich ochrony określonych w przepisach o ochronie informacji niejawnych (art. 2 ust. 1 i 2 ustawy oPIK).

Zgodnie z przepisem art. 13 ustawy o PIK zakres przetwarzanych w bazie danych informacji kryminalnych obejmuje takie dane jak: 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 wykorzystanych do popełnienia 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.

---

[5] Ustawa z dnia 6 lipca 2001 r. o przetwarzaniu informacji kryminalnych (Dz. U. z 2022 r. poz. 2448).

Jak wskazuje przepis art. 13 ust. 2 ustawy o PIK, informacje o 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, obejmują dane personalne tych osób takie jak: nazwisko, imiona, imiona i nazwiska poprzednie, imiona rodziców i nazwisko rodowe matki, datę i miejsce urodzenia, płeć, pseudonim, adres miejsca zameldowania, adres miejsca pobytu, cechy dokumentów tożsamości: rodzaj dokumentu, datę wystawienia dokumentu, organ wystawiający dokument, numer, serię dokumentu, numer ewidencyjny Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub obywatelstwo. W przypadku cudzoziemca nieposiadającego numeru PESEL- numer identyfikacji podatkowej NIP, numer identyfikacyjny REGON. Przetwarzaniu podlegają również 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.

Przepis art. 14 ustawy o PIK przewiduje terminy przetwarzania powyższych danych w rejestrze. Wskazany przepis stanowi, 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 (ust. 1). Informacje kryminalne, o których mowa w art. 13 ust. 1 pkt 5 lit. b, c i d, są przechowywane w bazach danych przez okres 5 lat (ust. 2). W szczególnie uzasadnionych przypadkach Szef Centrum może przedłużyć okres, o którym mowa w ust. 2, do lat 15 (ust. 3).

Informacje kryminalne, zgodnie z art. 25 ustawy o PIK, podlegają usunięciu z baz danych, jeżeli ich gromadzenie jest: 1) 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.

Przestrzeganie rzetelności usuwania informacji z bazy KCIK wymuszone jest także przepisem art. 44 ustawy o PIK, który stanowi, iż kto, wbrew przepisom ustawy, nie zarządza usunięcia bądź nie usuwa informacji kryminalnej z bazy danych Centrum, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

W świetle treści przepisów regulujących prowadzenie bazy KCIK uznać należy, że **przepisy regulujące retencję danych w tej bazie nie są sprzeczne z analizowanym orzeczeniem TSUE.** Ustawa wyłącza możliwość usuwania danych na wniosek osoby zainteresowanej z uwagi na charakter niejawny tego zbioru, jednakże zawiera przepisy nakładające na administratora bazy obowiązek usuwania danych po upływie ustawowych terminów retencji danych (art. 14 i art. 25 ustawy o PIK).

Przechodząc do rozważań dotyczących przepisów regulujących funkcjonowanie KSIP, wskazać należy, że TSUE w wielu wyrokach zajął stanowisko, zgodnie z którym wszelkie ograniczenia w korzystaniu przez jednostkę z praw podstawowych, w tym gwarantowanych w art. 7 i 8 Karty Praw Podstawowych Unii

Europejskiej praw do poszanowania życia prywatnego i ochrony danych osobowych, muszą zgodnie z art. 52 ust. 1 Karty być przewidziane ustawą i szanować zasadę proporcjonalności. Jednocześnie uregulowania prawne dotyczące tych ograniczeń powinny zawierać jasne i precyzyjne zasady normujące zakres i stosowanie tych ograniczeń[6].

Prowadzenie KSIP regulowane jest w ustawie o Policji. Przepis art. 21nb przewiduje, że Komendant Główny Policji prowadzi Krajowy System Informacyjny Policji, będący zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych (ust. 1). W odniesieniu do informacji, w tym danych osobowych, przetwarzanych w KSIP Komendant Główny Policji jest administratorem w rozumieniu przepisów o ochronie danych osobowych (ust. 2).

Przepis ten jest jedyną regulacją o charakterze ustawowym dotyczącą KSIP. Nie nakłada on na Komendanta obowiązku okresowego przeglądu danych zawartych w KSIP pod kątem potrzeby ich dalszego przetwarzania, ani też nie przyznaje podmiotowi danych prawa do ich usunięcia.

W takim przypadku zastosowanie znajdują przepisy art. 16 i 24 ust. 1 pkt 2 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[7] (dalej jako „ustawa ODO").

W odniesieniu do kwestii weryfikacji danych w KSIP wskazuje się, że zastosowanie ma art. 16 ustawy ODO, zgodnie z którym 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. (ust. 1). Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane usuwa się, z zastrzeżeniem art. 17 (ust. 2). Zauważyć w tym miejscu należy, że **wskazany w art. 16 ust. 1 dziesięcioletni termin weryfikacji danych, który ma mieć zastosowanie do KSIP, nie może być uznany za odpowiedni w świetle analizowanego wyroku**. Art. 5 dyrektywy 2016/680 nakłada na państwa obowiązek przyjęcia odpowiednich terminów weryfikacji danych i w razie spełnionych warunków, usuwania ich oraz przyjęcia odpowiednich środków służących sprawdzeniu przestrzegania tych terminów. Przepis ten ma na celu zapobieżenie, zgodnie z art. 4 ust. 1 lit. e tej dyrektywy, przechowywaniu danych osobowych przez okres dłuższy niż jest to faktycznie niezbędne. Odpowiedni charakter terminu wymaga, aby zgodnie z art. 4 ust. 1 lit. c i e dyrektywy w świetle postanowień ww. art. 52 ust. 1 Karty Praw Podstawowych przyjęty termin umożliwiał w danym przypadku usunięcie danych, które są w ogóle zbędne lub takie się stały z punktu widzenia celu ich przetwarzania. W świetle tych uwag **przyjęty w art. 16 ust. 1 ustawy termin nie może być uznany**

---

[6] Wyrok z 22 czerwca 2021 r., Latvijas Republikas Saeima, sygn. akt C- 439/19, (pkt 105); wyrok z 16 lipca 2020 r., Facebook Ireland i Schrems, sygn. akt C-311/18 (pkt 172–176).

[7] 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).

za odpowiadający standardom ochrony danych osobowych, wynikającym z prawa UE.

Szczegółowe zasady wykonywania zadań związanych z prowadzeniem i funkcjonowaniem KSIP zostały uregulowane w zarządzeniu Nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji[8].

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).

Przesłanki stanowiące o przydatności przetwarzanych danych zostały określone w § 105 zarządzenia Nr 70, zgodnie z którym weryfikując informacje, w tym dane osobowe, przetwarzane w celu wykrywania przestępstw, pod kątem ich przydatności, uwzględnia się szereg wymienionych w tym przepisie przesłanek. Niemniej zarządzenie Komendanta Głównego Policji stanowi jedynie regulację o charakterze wewnętrznym, która nie należy do źródeł prawa powszechnie obowiązującego w rozumieniu art. 87 Konstytucji Rzeczypospolitej Polskiej.

W polskim prawie wymienione przesłanki usunięcia danych osobowych w art. 24 ust. 1 pkt 2 ustawy ODO nie zostały wskazane. Stosownie do treści art. 24 ust. 1 pkt 2 ustawy ODO, żądanie (wniosek) usunięcia danych będzie skuteczne, w przypadku gdy dane te zostały zebrane lub są przetwarzane z naruszeniem przepisów niniejszej ustawy. Co istotne, przepis ten nie przesądza jak rozumieć „naruszenie przepisów ustawy", np. nie wyjaśnia, czy chodzi o każdy rodzaj naruszenia (np. brak spełnienia obowiązków informacyjnych). Taka wykładnia prowadziłaby oczywiście do absurdu. Wątpliwość interpretacyjna wynika z błędnej implementacji art. 16 ust. 2 dyrektywy 2016/680. Wskazany przepis dyrektywy wyraźnie przesądza, o jaki stopień niezgodności chodzi. Stosownie do treści tego przepisu, państwa członkowskie nakładają na administratora wymóg usunięcia bez zbędnej zwłoki danych osobowych i zapewniają, by osoba, której dane dotyczą, miała prawo uzyskać od administratora usunięcie bez zbędnej zwłoki jej danych osobowych, jeżeli przetwarzanie narusza przepisy przyjęte na podstawie art. 4, 8 i 10, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienia obowiązku prawnego ciążącego na administratorze[9]. **Praktyka orzecznicza organu do spraw ochrony danych osobowych wskazuje, że osoba występująca z wnioskiem do administratora o usunięcie danych z KSIP uzyskuje odpowiedź o charakterze ogólnym, wskazującą na ogólnie przedstawianą potrzebę dalszego przetwarzania danych i zgodność przetwarzania z przepisami prawa.** Wyroki sądów administracyjnych, które zapadają w tego rodzaju sprawach wskazują, że

---

[8] Zarządzenie Nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji (Dz. Urz. KGP z 2019 r., poz. 114).

[9] P. Kozik, M. Gumularz, Komentarz do art. 24, w: A. Grzelak (red.), Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz, Warszawa 2019, Legalis. Nb. 9-10.

przepisy ustawy ODO wymagają jedynie od administratora zgodności działania z przepisami regulującymi wykonywanie ustawowych zadań Policji i to do administratora należy ostateczna ocena potrzeby dalszego przetwarzania danych w KSIP[10]. Dlatego też **uzasadniony jest wniosek zmiany regulacji prawnych odnoszących się do sposobu weryfikacji przez administratora zasadności dalszego przetwarzania danych w KSIP, tak aby zapewnić podmiotowi danych realne prawo do żądania ich usunięcia, a nie jedynie kontrolę administratora o charakterze formalnym.**

Dodatkowo należy wskazać, że przepis art. 24 ust. 5 ustawy ODO nie nakłada na administratora danych obowiązku informowania podmiotu danych o przyczynach odmowy sprostowania lub usunięcia danych, co jest niezgodne z wdrażanym art. 16 ust. 4 dyrektywy 2016/680 stanowiącym, iż państwa członkowskie zapewniają by administrator informował pisemnie osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy. Polski ustawodawca w art. 24 ust. 6 ustawy ODO (w myśl art. 16 ust. 4 dyrektywy 2016/680) zobowiązał administratora, aby komunikat w sprawie odmowy realizacji praw z art. 24 ustawy ODO zawierał także informacje o możliwości wniesienia skargi. W doktrynie wskazuje się, że **przepis art. 24 ust. 6 ustawy ODO nie wskazuje wprost na możliwość wniesienia skargi do właściwego organu nadzorczego**[11], **przez co unormowanie to należy uznać za mogące ograniczać prawa podmiotowe jednostki do skutecznego żądania usunięcia przetwarzanych danych osobowych**.

Ze wskazanych wyżej powodów **w ocenie organu nadzorczego regulacja podstaw prawnych funkcjonowania KSIP nie spełnia standardów wynikających dla przepisów prawa krajowego z omawianego orzeczenia C-118/22**.

Dodatkowo zauważyć należy w odniesieniu do KSIP, że przepisy ustawy o Policji nie określają zakresu przetwarzanych danych (jest to przedmiotem regulacji zarządzenia KGP), jak i dopuszczalnych maksymalnych okresów ich przetwarzania. Przetwarzanie danych przez organy ścigania karnego może mieć miejsce na podstawie przepisów prawa, które powinny jednak spełniać określone warunki. Ze względu na charakter danych przetwarzanych w KSIP wskazać należy zarówno na przepisy art. 13, jak i art. 14, jak i art. 24 ODO. Zgodnie z art. 13 ust. 1 ODO właściwe organy przetwarzają dane osobowe wyłącznie w zakresie niezbędnym dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Z kolei art. 14 ust. 1 ustawy stanowi, iż niedopuszczalne jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu

---

[10] Wyrok WSA w Warszawie z 30 września 2021 r., sygn. akt II SA/Wa 1741/21, LEX nr 3340473; wyrok WSA w Warszawie z 3 listopada 2021 r., sygn. II SA/Wa 1779/21, LEX nr 3468991; wyrok WSA w Warszawie z 3 listopada 2022 r., sygn. akt II SA/Wa 660/22, Legalis nr 2791882.

[11] P. Liszwic, T. Ochocki, Ł. Pociecha, Komentarz do art. 24. Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Legalis. Nb. 9.

jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, danych dotyczących seksualności i orientacji seksualnej osoby fizycznej, zwanych dalej „danymi wrażliwymi. Wyjątek przewiduje art. 14 ust. 2 pkt 1 ODO, zgodnie z którym dopuszcza się przetwarzanie danych wrażliwych, jeżeli: 1) przepisy prawa zezwalają na ich przetwarzanie. Przepis art. 21 nb ustawy o Policji nie określa jednak, jakie konkretnie dane osobowe i na jakich zasadach przetwarzane są w KSIP.

W odniesieniu do braku przepisów określających maksymalny okres przetwarzania danych w KSIP wskazać należy na pkt 69 wyroku. Trybunał Sprawiedliwości UE wskazał w nim, że odniesienie się przez ustawodawcę krajowego do chwili śmierci podmiotu danych jako „terminu" usunięcia danych można uznać za termin „odpowiedni" jedynie w szczególnych okolicznościach, które należycie go uzasadniają. W sposób oczywisty nie jest tak w przypadku, gdy stosuje się go w sposób ogólny i niezróżnicowany do każdej osoby prawomocnie skazanej. Przepisy prawa dotyczące działania KSIP nie określają maksymalnego okresu przetwarzania danych osobowych w tym zbiorze, ani też nie przewidują przesłanek, po zaistnieniu których administrator powinien dokonać ich przeglądu i podjąć decyzję w przedmiocie ich usunięcia. Nie spełniają zatem standardów określonych w omawianym orzeczeniu.

Wnioski:

Przedstawiona wyżej analiza stanowiska TSUE wyrażonego w wyroku z dnia 30 stycznia 2024 r. w sprawie o **sygn. C- 118/22 Direktor na Glavna direktsia „Natsionalna politsia" pri Ministerstvo na vatreshnite raboti-Sofia** prowadzi do wniosku, że konieczne jest rozważenie wprowadzenia zmian w ustawie z 6 kwietnia 1990 r. o Policji w zakresie uregulowań dotyczących Krajowego Systemu Informacyjnego Policji.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych