

Sprawa C-60/22

Streszczenie wniosku o wydanie orzeczenia w trybie prejudycjalnym zgodnie z art. 98 § 1 regulaminu postępowania przed Trybunałem Sprawiedliwości

Data wpływu:

1 lutego 2022 r.

Oznaczenie sądu odsyłającego:

Verwaltungsgericht Wiesbaden (Niemcy)

Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym:

27 stycznia 2022 r.

Skarżący:

UZ

Druga strona postępowania:

Bundesrepublik Deutschland

Przedmiot postępowania głównego

Prawo ochrony danych – Rozporządzenie 2016/679 (ogólne rozporządzenie o ochronie danych) – Artykuł 5 ust. 2 – Rozliczalność – Artykuł 17 ust. 1 lit. d) i art. 18 ust. 1 lit. b) – Zgodność przetwarzania z prawem – Prawo do usunięcia danych lub do ograniczenia przetwarzania – Wykorzystanie przetwarzanych danych

Przedmiot i podstawa prawna odesłania prejudycjalnego

Wykładnia prawa Unii, art. 267 TFUE

Pytania prejudycjalne

- 1) Czy nieprzestrzeganie, zaniechanie przestrzegania lub niepełne przestrzeganie przez administratora obowiązku rozliczalności określonego w art. 5 rozporządzenia 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 (ogólnego rozporządzenia o ochronie danych, zwanego dalej „RODO”), na przykład z powodu brakującego lub niekompletnego rejestru czynności przetwarzania danych, o którym mowa w art. 30 RODO, lub braku uzgodnień w sprawie wspólnego sposobu postępowania zgodnie z art. 26 RODO, skutkuje tym, że przetwarzanie danych jest niezgodne z prawem w rozumieniu art. 17 ust. 1 lit. d) RODO i art. 18 ust. 1 lit. b) RODO, wobec czego osoba, której dane dotyczą, może żądać usunięcia danych lub ograniczenia przetwarzania?

- 2) W razie udzielenia odpowiedzi twierdzącej na pytanie pierwsze: Czy istnienie prawa do usunięcia danych lub do ograniczenia przetwarzania skutkuje tym, że przetwarzane dane nie mogą zostać wzięte pod uwagę w postępowaniu sądowym? Czy w każdym razie dotyczy to sytuacji, gdy osoba, której dane dotyczą, sprzeciwia się wykorzystaniu danych w postępowaniu sądowym?
- 3) W razie udzielania odpowiedzi przeczącej na pytanie pierwsze: Czy naruszenie przez administratora art. 5, 30 lub 26 RODO skutkuje tym, że w odniesieniu do wykorzystywania przetwarzania danych w postępowaniu sądowym sąd krajowy może uwzględnić te dane tylko wtedy, gdy osoba, której dane dotyczą, wyrażnie się na to wykorzystywanie zgodzi?

Przywołane przepisy prawa Unii

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.U. 2016, L 119, s. 1), motyw 82, art. 5, 9, 17, 18, 26, 30, 94

Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (Dz.U. 2013, L 180, s. 60), motyw 52

Karta praw podstawowych Unii Europejskiej, art. 7 i 8

Przywołane przepisy krajowe

Bundesdatenschutzgesetz (federalna ustawa o ochronie danych osobowych, zwana dalej „BDSG”, BGBl. I s. 2097), § 43 ust. 3

Zwięzłe przedstawienie stanu faktycznego i przebiegu postępowania

- 1 Skarżący odwołuje się od odmownej decyzji Bundesamtes für Migration und Flüchtlinge (federalnego urzędu ds. migracji i uchodźców) i wnosi o nadanie statusu uchodźcy na podstawie § 3 Asylgesetz (ustawy o azylu, zwanej dalej „AsylG”). Decyzja drugiej strony postępowania opiera się na tzw. elektronicznych aktach urzędu federalnego MARIS, które są również przekazywane do sądu za pośrednictwem Elektronische Gerichts- und Verwaltungspostfach (elektronicznej skrzynki pocztowej sądów i administracji, zwanej dalej „EGVP”) w ramach wspólnego postępowania zgodnie z art. 26 RODO. Jeśli chodzi o pytania dotyczące przekazania kompletnych akt, odsyła się do pytań już przedłożonych Trybunałowi Sprawiedliwości (sprawa C-564/21).
- 2 Istnieją wątpliwości, czy u drugiej strony postępowania w ogóle istnieje lub też czy istnieje w kompletnej postaci rejestr czynności przetwarzania w rozumieniu art. 30 RODO w odniesieniu do tzw. elektronicznych akt MARIS. Nie ma również uzgodnień ani regulacji prawnej w rozumieniu art. 26 RODO dotyczących postępowania w sprawie elektronicznego przekazywania akt i określenia odpowiedzialności w tym postępowaniu. Sąd odsyłający zażądał tych dokumentów w toku postępowania. Druga strona postępowania odmówiła jednak ich przedłożenia, uzasadniając to między innymi tym, że w odniesieniu do EGVP nie zawarto żadnych uzgodnień na podstawie art. 26 RODO.

Zwięzłe przedstawienie uzasadnienia odesłania prejudycjalnego

- 3 Powstaje pytanie, jak sąd powinien postąpić z danymi osobowymi skarżącego, przynajmniej w przypadku (formalnej) niezgodności z prawem przetwarzania tych danych przez drugą stronę postępowania, gdyż zgodnie z dyrektywą 2013/32 RODO ma zastosowanie do procedur azylowych na podstawie prawa krajowego. Ani AsylG, ani prawo o postępowaniu przed sądami administracyjnymi nie zawierają żadnych regulacji w tym zakresie.
- 4 Zgodnie z motywem 52 dyrektywy 2013/32 przetwarzanie danych osobowych w ramach procedur azylowych w państwach członkowskich na mocy tej dyrektywy jest regulowane przepisami dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Dyrektywa 95/46 została uchylona ze skutkiem od dnia 25 maja 2018 r. na podstawie art. 94 ust. 1 RODO. Jednakże zgodnie z art. 94 ust. 2 RODO odesłania do uchylonej dyrektywy 95/46 należy traktować jako odesłania do tego rozporządzenia. W związku z tym RODO ma pełne zastosowanie do procedur udzielania ochrony międzynarodowej.
- 5 Już dyrektywa 95/46 przewidywała dokumentowanie zautomatyzowanego przetwarzania danych, tzw. zawiadomienie, o którym mowa w art. 18 tej dyrektywy. Treść zawiadomienia, określona w art. 19 dyrektywy 95/46, odpowiadała zasadniczo dzisiejszemu art. 30 RODO, przy czym nowa norma

odnosi się do wszystkich form przetwarzania danych, tj. również do zbiorów danych.

- 6 W czasie obowiązywania dyrektywy 95/46 druga strona postępowania dysponowała jedynie bardzo rudymmentarnym katalogiem przetwarzania dotyczącym elektronicznych akt MARIS, stanowiącym zawiadomienie w rozumieniu dyrektywy 95/46 (§ 4e BDSG w poprzedniej wersji). Ówczesny rejestr czynności przetwarzania danych (zawiadomienie) nie zawierał żadnych szczególnych regulacji dotyczących przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO (art. 8 dyrektywy 95/46). Zdaje się, że takie szczególne regulacje dotyczące postępowania z danymi, o których mowa w art. 9 i 10 RODO, nie powstały także i do dziś. Dane dotyczące zdrowia i wyznania, podobnie jak dane dotyczące wyroków skazujących, są bowiem z reguły włączane do elektronicznych akt MARIS jako tzw. „zwykłe dokumenty”. Nie jest widoczna żadna szczególna ochrona bezpieczeństwa danych poza tym, że prawdopodobnie istnieje protokół dostępu. Jednakże akta osoby ubiegającej się o azyl mogą być przeglądane w każdej jednostce lokalnej drugiej strony postępowania na terenie Niemiec, tak samo jak w samej centrali.
- 7 Zwłaszcza w odniesieniu do prowadzenia akt i przedkładania ich sądowi sąd odsyłający ma poważne wątpliwości co do tego, czy druga strona postępowania spełnia wymogi art. 5 ust. 1 RODO w związku z przykładowo art. 26 czy art. 30 RODO. Wbrew żądaniu sądu rejestr czynności przetwarzania nie został przedłożony. W związku z tym planowane jest przesłuchanie kierownika odpowiedzialnej jednostki w charakterze drugiej strony postępowania, po wydaniu przez Trybunał orzeczenia w odniesieniu do obowiązku rozliczalności, o którym mowa w art. 5 ust. 2 RODO.
- 8 Przed przesłuchaniem należy jednak wyjaśnić, czy zaniechanie przestrzegania obowiązków wynikających z RODO i związana z tym niezgodność przetwarzania danych z prawem prowadzi do zastosowania sankcji, takiej jak usunięcie danych na podstawie art. 17 ust. 1 lit. d) RODO lub ograniczenie przetwarzania na podstawie art. 18 ust. 1 lit. b) RODO. A co najmniej, czy ma to miejsce wtedy, gdy zażąda tego osoba, której dane dotyczą, w tym przypadku skarżący. W przeciwnym razie sąd byłby bowiem zmuszony do uczestniczenia w niezgodnym z prawem przetwarzaniu danych w ramach postępowania sądowego. Organy władzy mogłyby stale naruszać RODO bez żadnej sankcji.
- 9 W takim przypadku tylko organ nadzorczy w rozumieniu z art. 58 RODO mógłby podjąć działania. Nałożenie kary pieniężnej na Bundesamt für Migration und Flüchtlinge (federalny urząd ds. migracji i uchodźców) nie wchodziłoby jednak w grę na gruncie prawa krajowego. Zgodnie z § 43 ust. 3 BDSG, który opiera się na art. 83 ust. 7 RODO, na organy i inne podmioty publiczne nie nakłada się administracyjnych kar pieniężnych. Nie byłoby żadnej zachęty dla organów władzy, by postępować zgodnie z prawem. Skutkowałoby to tym, że wymogi dyrektywy 2013/32, podobnie jak samo RODO, nie byłyby spełnione.

- 10 Trybunał orzekł już, że „zawiadomienie” (obecnie: rejestr czynności przetwarzania) musi być kompletne w momencie przetwarzania, ale nie wcześniej (sprawy C-92/09 i C-93/09, wyrok z dnia 9 listopada 2011 r., ECLI:EU:C:2010:662, pkt. 95 i nast.). W tym przypadku dane osobowe skarżącego były przetwarzane przez drugą stronę postępowania już od momentu złożenia przez niego wniosku o udzielenie azylu (w dniu 7 maja 2019 r.). W związku z tym, przynajmniej zgodnie z orzecznictwem Trybunału, w tym momencie powinien istnieć kompletny rejestr czynności przetwarzania dotyczących akt MARIS (a tym samym akt azylowych skarżącego). Tak jednak nie jest.
- 11 Trybunał nie rozstrzygnął do tej pory – ani na podstawie dyrektywy 95/46, ani na podstawie RODO – co ma zastosowanie w tej sytuacji. Jeżeli przyjąć, że dla zachowania zgodności z RODO administrator lub podmiot przetwarzający powinni prowadzić rejestr czynności przetwarzania, za które są odpowiedzialni (motyw 82 RODO), powstaje pytanie, jakie konsekwencje wynikają z zaniechania tego obowiązku przez odpowiedzialną jednostkę. W takim przypadku bowiem obowiązek rozliczalności zgodnie z art. 5 RODO nie może zostać spełniony.
- 12 Wprawdzie art. 83 ust. 5 lit. a) RODO stanowi, że naruszenie obowiązku rozliczalności, o którym mowa w art. 5 RODO może być sankcjonowane administracyjną karą pieniężną w wysokości do 20 000 000 EUR. Jednakże, jak już wyjaśniono, nie ma to – na podstawie § 43 ust. 3 BSDG – zastosowania do organów federalnych. Artykuł 17 ust. 1 lit. d) RODO stanowi jednak, że dane przetwarzane niezgodnie z prawem muszą zostać usunięte – przynajmniej na żądanie osoby, której dane dotyczą.
- 13 Brakujący lub niekompletny rejestr czynności przetwarzania danych w przekonaniu sądu odsyłającego prowadzi – przynajmniej w świetle art. 5 RODO – do „formalnej” niezgodności z prawem przetwarzania danych. Pojawia się zatem pytanie, czy w takim przypadku sankcją za zaniechanie obowiązku wynikającego z art. 5 RODO w związku z art. 30 RODO nie powinno być usunięcie lub przynajmniej zablokowanie danych. W przeciwnym razie, wobec braku ewentualnej sankcji, RODO nie mogłoby być skutecznie egzekwowane.
- 14 W końcu, o ile wiadomo, na przykład Republika Francuska w czasie obowiązywania art. 18 i nast. dyrektywy 95/46 wprowadziła do prawa krajowego regulację, że w postępowaniach sądowych obowiązuje ścisły zakaz prawny wykorzystywania danych osobowych, które nie zostały przez odpowiedzialną jednostkę zgłoszone w formie zawiadomienia do organu nadzorczego (CNIL) przez podmiot odpowiedzialny, ponieważ wykorzystanie danych było – z powodu braku dokumentacji – niezgodne z prawem. Zatem w tym przypadku zastosowano już co najmniej sankcję w postaci zakazu przetwarzania i wykorzystywania danych przez sąd. Pod rządami RODO również w Portugalii i w innych państwach członkowskich brak rejestru czynności przetwarzania danych prowadzi, jak się wydaje, do zakazu ich stosowania. To mechanizm, który nie został wprowadzony w Republice Federalnej Niemiec ani w ramach transpozycji dyrektywy 95/46, ani

w czasie obowiązywania RODO. Stworzono tu raczej podstawy do „tolerowania” brakującego zawiadomienia.

- 15 Przekazywanie akt i pism procesowych przez drugą stronę postępowania drogą elektroniczną również stanowi przetwarzanie danych w rozumieniu art. 4 pkt 2 RODO, które musi być zgodne z zasadami przetwarzania danych, o których mowa w art. 5 RODO. Dlatego również w tym przypadku powstają wątpliwości co do formalnej zgodności z prawem przetwarzania danych poprzez przekazywanie tzw. elektronicznych akt urzędu federalnego oraz pism procesowych przez drugą stronę postępowania za pomocą odpowiednich środków przekazu. Również w tym przypadku nie ma rejestru czynności przetwarzania danych ani regulacji o wspólnej odpowiedzialności. Istnieje wprowadzone *Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach* (rozporządzenie o technicznych warunkach ramowych elektronicznego obrotu prawnego oraz o specjalnej elektronicznej skrzynce pocztowej organów władzy) z dnia 24 listopada 2017 r. (BGBl. I s. 3803, zmienione przez art. 6 ustawy z dnia 5 października 2021 r., BGBl. I s. 4607). Reguluje ono przekazywanie dokumentów elektronicznych do sądów krajów związkowych i federacji. Najwyższe organy władzy federacji lub rządy krajów związkowych mogą przy tym, w swoim zakresie kompetencji, sprawdzić u podmiotów prawa publicznego tożsamość organów władzy lub osób prawnych prawa publicznego w celu dopuszczenia ich do *Besonderes elektronisches Behördenpostfach* (specjalnej elektronicznej skrzynki pocztowej organów władzy, tzw. BeBPos). Najwyższe organy władzy federacji lub kilka rządów krajowych mogą również wspólnie wyznaczyć podmiot prawa publicznego dla swoich zakresów kompetencji. Nie zostało uregulowane, co to właściwie jest za podmiot. Ostatecznie prawdopodobnie oznacza to tak zwaną *Bund-Länder-Arbeitsgruppe der Justizministerien* (*Bund-Länder-Kommission für Informationstechnik in der Justiz* [BLK] *Arbeitsgruppe IT-Standards in der Justiz* – grupę roboczą federacji i krajów związkowych przy ministerstwie sprawiedliwości – komisję federacji i krajów związkowych w zakresie technik informatycznych w wymiarze sprawiedliwości [BLK] grupę roboczą w zakresie standardów IT w wymiarze sprawiedliwości). Nie wiadomo i nie udokumentowano, który organ lub organy są odpowiedzialne za rejestr czynności EGVP lub BeBPos, ani nawet niezbędnej struktury serwerów.
- 16 Nie ma również odpowiednich przepisów prawnych lub innych pisemnych regulacji dotyczących stosunków między sądami i organami władzy, które byłyby wymagane na podstawie art. 26 RODO w celu uregulowania odpowiedzialności. Nawet w krajach związkowych, które zgodnie z własnym rozporządzeniem prawnym wybrały model wspólnego postępowania, brakuje odpowiedniego wdrożenia zgodnego z ochroną danych. W Hesji rozporządzenie stanowi nawet, że elektroniczna skrzynka pocztowa jest prowadzona wyłącznie na serwerach „centrum danych” wymiaru sprawiedliwości, tj. w *Hessische Zentrale für Datenverarbeitung* (heskiej centrali przetwarzania danych, zwanej dalej „HZD”). HZD nie jest jednak częścią wymiaru sprawiedliwości i jest co najwyżej jako pośrednik podmiotem przetwarzającym dane zgodnie z art. 28 RODO.

- 17 Wiadomo jedynie, że faktycznie to Landesamt für Datensicherheit in Nordrhein-Westfalen (krajowy urząd ds. bezpieczeństwa danych w Nadrenii Północnej-Westfalii) jako „pośrednik” jest prawdopodobnie odpowiedzialny za administrowanie i obsługę centralnego, ponadkrajowego serwera rejestru S.A.F.E. Identyfikator SAFE ma być niezmienny i przyznawany tylko raz (zob. SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift_SAFE_ID_Stand_Dez_2014.pdf). Ponadto skrzynki pocztowe w EGVP są oznaczone niepowtarzalnym numerem identyfikacyjnym (tzw. Govello-ID). O ile sądowi odsyłającemu wiadomo, identyfikatory te powinny być zapisane w rejestrze czynności prowadzonym przez Nadrenię Północną-Westfalię (IT-NRW). Nie jest uregulowane, kto jest faktycznie odpowiedzialny za przyznawanie identyfikatora Govello w ramach związku federacji i krajów związkowych.
- 18 Nie wiadomo, na jakiej podstawie prawnej w zakresie przetwarzania danych jest prowadzona EGVP. W odniesieniu do zapytania o uzgodnienia, o którym mowa w art. 26 RODO, druga strona postępowania odmówiła złożenia wyjaśnień i przedłożenia tych uzgodnień. Dlatego też, ze względu na brak określenia zakresu odpowiedzialności zgodnie z art. 26 RODO, wątpliwe jest również, czy za pośrednictwem tzw. specjalnej elektronicznej skrzynki pocztowej organów władzy może mieć miejsce zgodne z prawem przekazanie danych. Dotyczy to również bezpieczeństwa danych, ponieważ żaden z dokumentów nie jest szyfrowany podczas transmisji.
- 19 Zdaniem sądu odsyłającego kwestia, czy na podstawie obowiązującego prawa pozytywnego w przypadku specjalnej elektronicznej skrzynki pocztowej adwokata należy stosować szyfrowanie typu „od końca do końca”, nie ma decydującego znaczenia. Przynajmniej w Hesji nie szyfruje się wiadomości, które mają być przekazywane między pośrednikiem, HZD i odpowiednim sądem – a więc również sądem administracyjnym w Wiesbaden.
- 20 Nie jest to jednak w tym przypadku istotne, ponieważ procedura odpowiada procedurze przesyłania e-maili. Trybunał rozstrzygnął w odniesieniu do internetowej usługi Gmail, że nie stanowi ona usługi łączności, ponieważ taka usługa, nieobejmująca dostępu do Internetu, która nie polega całkowicie lub głównie na przekazywaniu sygnałów w sieciach łączności elektronicznej, nie stanowi „usługi łączności elektronicznej” (wyrok z dnia 13 czerwca 2019 r., C-193/18, ECLI:EU:C:2019:498). Dlatego też EGVP nie jest usługą objętą zakresem stosowania dyrektywy 2002/58/WE (art. 2 ust. 4 RODO). W związku z tym RODO ma zastosowanie, co oznacza, że EGVP i związane z nim procedury muszą zostać zapisane w rejestrze czynności przetwarzania, a odpowiednie zakresy odpowiedzialności muszą zostać uzgodnione, gdyż jest to procedura z wieloma administratorami danych, o której mowa w art. 26 RODO. W przedmiotowej sprawie żaden z tych dwóch wymogów nie został spełniony. W związku z tym istnieją wątpliwości co do zgodności z prawem przekazywania danych.

- 21 EGVP jest procedurą organów administracji sądowej, które są częścią drugiej władzy, władzy wykonawczej, oraz procedurą drugiej strony postępowania, która również jest częścią władzy wykonawczej. Sąd jest zatem przekonany, że druga strona postępowania musi zapewnić zgodność z RODO elektronicznej procedury przekazywania danych zawartych w pismach procesowych i aktach.
- 22 Dla sądu odsyłającego powstaje zatem w ramach sprawowania wymiaru sprawiedliwości pytanie, jak postępować z danymi dostarczonymi za pośrednictwem systemu EGVP przez tzw. skrzynkę pocztową organu władzy, jeżeli procedura EGVP i związane z nią przetwarzanie danych, jako takie, nie są zgodne z RODO.
- 23 Sąd odsyłający musi przestrzegać RODO i stosować się do niego w ramach sprawowania wymiaru sprawiedliwości.
- 24 Nie ma to wpływu na zgodność z prawem przetwarzania danych przez administrację sądową, ponieważ znajduje się to poza sferą „sprawowania wymiaru sprawiedliwości”, w zakresie kompetencji drugiej władzy, władzy wykonawczej. Jednakże sąd odsyłający musi przestrzegać i stosować się do prawa europejskiego. Jeżeli uczestnicy postępowania naruszają to prawo, to wydaje się, że sądowe wykorzystanie danych nie będzie dopuszczalne, ponieważ w przeciwnym razie sąd uczestniczyłby w niezgodnym z prawem przetwarzaniu danych. W niniejszej sprawie sytuację pogarsza fakt, że druga strona postępowania, w świetle dotychczasowej korespondencji, prawdopodobnie (umyślnie) narusza prawo europejskie.
- 25 Nie zachodzi też przypadek, który uzasadniałby wykorzystanie danych przez sąd na podstawie art. 17 ust. 3 lit. e) RODO do ustalenia, dochodzenia lub obrony roszczeń prawnych drugiej strony postępowania. Wprawdzie dane zebrane przez drugą stronę postępowania służą do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi – art. 17 ust. 3 lit. b) RODO. W ten sposób jednak na stałe zostałoby zalegalizowane działanie naruszające prawo o ochronie danych.
- 26 W związku z tym przedstawione pytania mają szczególne znaczenie, jeśli chodzi o wdrożenie RODO w postępowaniu sądowym. Osiągnięcie celu z art. 1 ust. 2 RODO, jakim jest wspieranie podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, mogłoby zostać udaremnione.
- 27 W tym względzie, przynajmniej w razie udzielenia odpowiedzi przeczącej na pytanie pierwsze, powinna być konieczna dyspozycja osoby, której dane dotyczą, lub nawet wyraźna zgoda osoby, której dane dotyczą – w tym przypadku

skarżącego – na wykorzystanie jej danych w postępowaniu sądowym pomimo formalnej niezgodności przetwarzania z prawem.

- 28 Jednakże skutkowałoby to również tym, że w przypadku odmowy dane przetwarzane przez drugą stronę postępowania, które przekazuje ona w formie tzw. elektronicznych akt organu władzy MARIS, nie mogłyby być przetwarzane (wykorzystywane) przez sąd. Prowadziłoby to z kolei do tego, że nie byłoby już podstawy do wydania decyzji, dopóki nie zostałyby spełnione obowiązki związane z dokumentacją. Pierwotna decyzja drugiej strony postępowania zawsze w takim przypadku musiałaby zostać uchylona. Decyzja w sprawie wniosku o nadanie statusu uchodźcy byłaby możliwa dopiero po wypełnieniu obowiązków dokumentacyjnych.

DOKUMENT ROBOCZY