

Michał Krzysztof Michalski

ORCID: 0009-0009-3324-5411

mkf.michalski@gmail.com

Akademia Leona Koźmińskiego

Kontekstowy charakter kwalifikacji spseudonimizowanych danych jako danych osobowych w prawie Unii Europejskiej – częściowo krytyczna glosa do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 4 września 2025 r., C-413/23 P

Słowa kluczowe: dane osobowe; pseudonimizacja; RODO; ochrona danych osobowych; identyfikowalność

Glosa dotyczy wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 4 września 2025 r. w sprawie C-413/23 P. Głosowany wyrok porusza ważną kwestię, jaką jest kwalifikacja danych poddanych pseudonimizacji jako danych osobowych. W wyroku uznano, że ocena, czy spseudonimizowane dane są danymi osobowymi dla danego podmiotu, jest relatywna. Innymi słowy, z punktu widzenia podmiotu, który nie dysponuje narzędziami pozwalającymi na przypisanie danych konkretnej osobie, spseudonimizowane dane otrzymane od administratora nie muszą mieć charakteru danych osobowych. Glosa próbuje analizę przyjętą przez Trybunał w kontekście klasyfikacji uwag jako danych osobowych oraz momentu powstania obowiązku informacyjnego ciążącego na administratorze na mocy art. 15 rozporządzenia 2018/1725. Jednocześnie autor glosy kwestionuje wyodrębnienie dwóch rodzajów danych spseudonimizowanych: identyfikowalnych oraz nieidentyfikowalnych, które wynikają z błędnej interpretacji przepisów. Dodatkowo autor polemizuje z przyjętym przez Trybunał rozumieniem identyfikowalności w niniejszej sprawie oraz z trendem przesuwania granicy relatywności rozumienia danych osobowych w kontekście pseudonimizacji i rozpatrywania jej osobno dla każdego podmiotu w łańcuchu przetwarzania. Jak wyjaśnia autor, takie działanie prowadzi do niejasności i uderza w system ochrony danych osobowych.

Wprowadzenie

Przed wszystkim należy zauważyć, że zarówno pojęcie pseudonimizacji, jak i rozumienie innych pojęć omówionych w niniejszej glosie ma wspólne brzmienie na gruncie rozporządzenia 2018/1725 w sprawie ochrony osób

fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych¹ oraz rozporządzenia 2016/679

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwa-

z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych².

Pseudonimizacja stanowi ważny instrument systemu ochrony danych osobowych w prawie unijnym. Jest to przetworzenie danych osobowych w taki sposób, żeby nie można ich już było przypisać konkretnej osobie bez użycia dodatkowych informacji, które są przechowywane oddzielnie i podlegają odpowiednim środkom technicznym oraz organizacyjnym³. Jest to zatem zabieg polegający na zastąpieniu części danych osobowych „pseudonimem”, czyli odpowiednio przetworzonym ekwiwalentem danych⁴. Pseudonimizacja różni się od anonimizacji w tym względzie, że w przypadku tej drugiej doszło do takiego przekształcenia, iż konkretna osoba przestaje być możliwa do zidentyfikowania⁵. Do momentu publikacji omawianego wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie C-413/23 P⁶ w doktrynie istniał konsensus co do tego, że spseudonimizowane dane

pozostają danymi osobowymi, ponieważ pseudonimizację można cofnąć⁷.

Celem glosy jest przeprowadzenie analizy i oceny wyroku w sprawie SRB w szczególności w kontekście rozważań dotyczących spseudonimizowanych danych osobowych oraz zbadanie powiązanych konsekwencji wynikających z rozpatrywania statusu spseudonimizowanych danych jako danych osobowych osobno dla każdego podmiotu w łańcuchu przetwarzania. Analiza przeprowadzona jest przy pomocy metody dogmatyczno-prawnej polegającej na interpretacji przepisów prawa unijnego w świetle wykładni doktrynalnej oraz orzecznictwa Trybunału. Główną hipotezą przedstawioną w opracowaniu jest to, że kontekstowa klasyfikacja danych spseudonimizowanych jako danych osobowych prowadzi do sprzeczności w dwustronnej strukturze obowiązków pomiędzy administratorem i odbiorcą danych osobowych.

I. Opis stanu faktycznego

Sprawa SRB wynikała na tle restrukturyzacji i likwidacji hiszpańskiego banku Banco Popular Español SA prowadzonej przez Jednolitą Radę do spraw Restrukturyzacji i Uporządkowanej Likwidacji (SRB). W ramach tego postępowania SRB zleciła spółce Deloitte sporządzenie wyceny mającej ustalić, czy akcjonariusze i wierzyciele zostaliby potraktowani korzystniej w przypadku zastosowania standardowego postępowania upad-

rzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. L 295/39, 21.11.2018).

² 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. L 119/1, 4.05.2016), dalej: RODO.

³ Art. 3 ust. 6 rozporządzenia 2018/1725. Zob. także: K. Witkowska-Nowakowska, *Komentarz do art. 4 pkt 5*, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2018, s. 203–208.

⁴ M. Kołodziej, *Pseudonimizacja w RODO – kiedy i jak stosować?*, „ABI Expert” 2018, nr 7, s. 44.

⁵ A. Mednis, *Pojęcie danych osobowych*, [w:] *System Prawa Medycznego*, t. 3: *Organizacja systemu ochrony zdrowia*, D. Bach-Golecka, R. Stankiewicz (red.), Warszawa 2020, s. 935.

⁶ Wyrok TSUE z dnia 4 września 2025 r. w sprawie C-413/23 P, *EIOD przeciwko SRB*, ECLI:EU:C:2025:645, dalej: sprawa SRB.

⁷ Tak m.in. P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 4*, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, P. Litwiński (red.), Warszawa 2025; J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, s. 135–137; A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 282–284; opinia 05/2014 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 w sprawie technik anonimizacji przyjęta dnia 10 kwietnia 2014 r., s. 11.

łościowego. Po sporządzeniu wyceny przyjęto decyzję wstępną w przedmiocie wypłaty ewentualnej rekompensaty oraz wszczęto postępowanie umożliwiające zainteresowanym skorzystanie z prawa do bycia wysłuchanym.

Postępowanie to przebiegało dwuetapowo. W ramach pierwszego etapu opublikowano oświadczenie o ochronie prywatności oraz weryfikowano uprawnienia uczestników do udziału w procedurze. Następnie w ramach drugiego etapu uprawnieni mogli przedstawić uwagi dotyczące decyzji wstępnej SRB. Uwagi te były składane za pośrednictwem spersonalizowanych linków i oznaczane losowo generowanymi kodami alfanumerycznymi, a następnie trafiły do analizy Deloitte. W wyniku zastosowanej pseudonimizacji jedynie SRB była w stanie powiązać uwagi z konkretnymi osobami.

Na tle postępowania prowadzonego przez SRB akcjonariusze oraz wierzyciele wnieśli skargę do Europejskiego Inspektora Ochrony Danych (EIOD), zarzucając naruszenie obowiązku informacyjnego z art. 15 ust. 1 lit. d rozporządzenia 2018/1725 poprzez zatajenie faktu przekazania ich danych osobowych spółce Deloitte. EIOD w swojej decyzji uznał m.in. to, że udostępnione dane były danymi spseudonimizowanymi, przez co miały charakter danych osobowych, a Deloitte był ich odbiorcą w rozumieniu art. 3 pkt 13 rozporządzenia 2018/1725. SRB zaskarżyła tę decyzję do Sądu Unii Europejskiej, podnosząc naruszenie art. 3 pkt 1 rozporządzenia 2018/1725 oraz argumentując, że informacje przekazane Deloitte nie stanowiły dla tego podmiotu danych osobowych. Sąd UE podzielił to stanowisko⁸, wskazując, że EIOD dokonał kwalifikacji danych na podstawie domniemań: bez analizy treści, celu i skutków oraz zbadania, czy Deloitte mógł zidentyfikować osoby, których uwagi dotyczyły. Od tego wyroku EIOD wniósł odwołanie do TSUE, zarzucając m.in. błędną wykładnię definicji danych osobowych oraz pseudonimizacji.

2. Rozstrzygnięcie TSUE

W glosowanym wyroku TSUE odniósł się do trzech zasadniczych zagadnień. Po pierwsze, nawiązując do utrwalonego orzecznictwa⁹, uznał, że uwagi przekazane Deloitte stanowiły dane osobowe, ponieważ odzwierciedlały opinie i stanowiska ich autorów¹⁰. Trybunał odrzucił stanowisko Sądu UE, który powołując się na sprawę C-434/16¹¹, wymagał, by EIOD badał treść, cel i skutki tych uwag¹² w celu ustalenia, czy stanowią one dane osobowe. Trybunał zauważył, że w przytoczonej sprawie niejako automatycznie uznano, iż przedmiotowe dane są osobowe, ponieważ wyrażały prywatną opinię lub ocenę (pkt 59 wyroku).

Po drugie, TSUE odniósł się do znaczenia pseudonimizacji dla kwalifikacji danych jako osobowych. Trybunał podkreślił, że pseudonimizacja nie oznacza automatycznie, iż dane zachowują charakter danych osobowych wobec wszystkich podmiotów i w każdych okolicznościach (pkt 69–89 wyroku). Odwołując się do art. 3 pkt 1 oraz motywu 16 rozporządzenia 2018/1725, wskazał, że dane mogą zostać uznane za osobowe wyłącznie wówczas, gdy odnoszą się do osoby zidentyfikowanej lub możliwej do zidentyfikowania. Opierając się o opinię Rzecznika Generalnego Deana Spielmann¹³, uznał, że pseudonimizacja nie stanowi elementu definicyjnego danych osobowych, lecz jest środkiem technicznym i organizacyjnym służącym ograniczeniu ryzyka związanego z przetwarzaniem

⁸ Wyrok Sądu UE z dnia 26 kwietnia 2023 r. w sprawie T-557/20, *SRB przeciwko EIOD*, ECLI:EU:T:2023:219.

⁹ Tak m.in. wyrok TSUE z dnia 4 maja 2023 r. w sprawie C-487/21, *Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369, pkt 23; wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-479/22 P, *OC przeciwko Komisji*, ECLI:EU:C:2024:215, pkt 45 (dalej: sprawa OC).

¹⁰ Sprawa *SRB*, pkt 56–60.

¹¹ Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, *Nowak*, ECLI:EU:C:2017:994.

¹² Wyrok Sądu UE z dnia 26 kwietnia 2023 r. w sprawie T-557/20, pkt 73–74.

¹³ Opinia Rzecznika Generalnego Deana Spielmann z dnia 6 lutego 2025 r. w sprawie C-413/23 P, *EIOD przeciwko SRB*, ECLI:EU:C:2025:59, pkt 46–48.

(pkt 72 wyroku). Dodatkowo TSUE, w ślad za Rzecznikiem Generalnym¹⁴, podkreślił w kontekście motywu 16 rozporządzenia 2018/1725 zdanie trzecie oraz czwarte, że wyjaśnienia tam zawarte byłyby pozbawione skuteczności, gdyby uznać, że dane spseudonimizowane są w każdym wypadku danymi osobowymi (pkt 80 wyroku). Co więcej, bazując na wcześniejszym orzecznictwie¹⁵, TSUE uznał, że jeżeli identyfikacja osoby jest prawnie zabroniona, praktycznie niewykonalna lub wymagałaby niewspółmiernego nakładu środków, czasu i pracy, dane spseudonimizowane mogą z perspektywy danego podmiotu utracić charakter danych osobowych (pkt 82 wyroku). Jednocześnie odwołując się do innego orzeczenia¹⁶, zaznaczył, że dane pozornie bezosobowe mogą ponownie uzyskać charakter danych osobowych, jeżeli zostaną udostępnione podmiotowi dysponującemu realnymi możliwościami identyfikacji osoby, której dotyczą (pkt 84 wyroku). W tym kontekście TSUE, odwołując się do argumentacji Rzecznika Generalnego¹⁷, uznał, że obowiązki informacyjne przewidziane w art. 15 rozporządzenia 2018/1725 nie mogą obciążać podmiotu, który obiektywnie nie jest w stanie zidentyfikować osoby, której dane dotyczą (pkt 89 wyroku).

Po trzecie, TSUE doprecyzował zakres oraz moment powstania obowiązku informacyjnego administratora. Jak wskazano, informacje wymienione w art. 15 rozporządzenia 2018/1725 (m.in. dotyczące odbiorców danych osobowych), powinny zostać przekazane osobie, której dane dotyczą, w momencie ich zbierania (pkt 106 i 108 wyroku). Ma to umożliwić podjęcie świadomej decyzji o przekazaniu danych oraz skuteczną ochronę praw wobec ich dalszych odbiorców (pkt 109 wyroku). W tym zakresie TSUE podkreślił, że ocena możliwości identyfikacji powinna być dokonywana z perspektywy administratora

i na moment zbierania danych. Bez znaczenia pozostaje fakt, że późniejszy odbiorca danych nie był już w stanie dokonać identyfikacji osób po zastosowanej pseudonimizacji (pkt 111–112 wyroku).

3. Ocena rozstrzygnięcia TSUE

Stanowisko i argumentację TSUE w zakresie uznania opinii i uwag za dane osobowe należy ocenić pozytywnie. Trafna jest również wykładnia dotycząca momentu powstania obowiązku informacyjnego w chwili zbierania danych osobowych. Zastrzeżenia budzi natomiast część uzasadnienia odnosząca się do pseudonimizacji oraz kontekstowego charakteru kwalifikacji danych spseudonimizowanych jako danych osobowych. Trybunał konsekwentnie, poczynawszy od sprawy z dnia 19 października 2016 r. C-582/14¹⁸, przyjmuje zrelatywizowaną koncepcję obiektywną pojęcia danych osobowych¹⁹. Zgodnie z tą koncepcją identyfikowalność osoby oceniana jest przez pryzmat środków, którymi dany podmiot może się racjonalnie posłużyć oraz takie osoby trzecie, do których podmiot racjonalnie może się odwołać w celu identyfikacji²⁰. W sprawie *SRB* Trybunał po raz pierwszy w sposób tak wyraźny przesunął jednak punkt ciężkości na perspektywę konkretnego uczestnika przetwarzania. W rezultacie uznał, że dane spseudonimizowane, które dla administratora pozostają danymi osobowymi, nie muszą mieć takiego charakteru dla innego podmiotu, który otrzymuje te dane. W niniejszej sprawie zdaniem TSUE skoro Deloitte nie dysponuje środkami umożliwiającymi identyfi-

¹⁴ *Ibidem*, pkt 51.

¹⁵ Sprawa *OC*, pkt 51.

¹⁶ Wyrok TSUE z dnia 9 listopada 2023 r. w sprawie C-319/22, *Gesamtverband Autoteile-Handel*, ECLI:EU:C:2023:837, pkt 46, 49.

¹⁷ Opinia Rzecznika Generalnego Deana Spielmann z dnia 6 lutego 2025 r., pkt 58.

¹⁸ Wyrok TSUE z dnia 19 października 2016 r. w sprawie C-582/14, *Breyer*, ECLI:EU:C:2016:779, dalej: sprawa *Breyer*.

¹⁹ P. Litwiński, *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrik Breyer*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 54.

²⁰ D. Lubasz, A. Szkurlat, *Zrelatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, „Monitor Prawniczy” 2021, nr 23, s. 1575–1584.

kację osób, to nie musi traktować tych danych jako osobowych.

Przyjęcie takiego stanowiska prowadzi do daleko idących konsekwencji systemowych. W istocie wydaje się, że TSUE wprowadza rozróżnienie pomiędzy danymi spseudonimizowanymi „identyfikowalnymi” oraz „nieidentyfikowalnymi”, przy czym jedynie te pierwsze kwalifikują się jako dane osobowe. Trudno bowiem w tej sprawie traktować dane spseudonimizowane „nieidentyfikowalne” jako dane w pełni zanonimizowane w sytuacji, gdy administrator jest w stanie odwrócić ten proces. Rozróżnienie to TSUE wywodzi głównie ze zdania pierwszego i drugiego motywu 16 rozporządzenia 2018/1725, wskazując, że razem z następującymi po nich zdaniami trzecim i czwartym precyzują ocenę możliwości zidentyfikowania osoby i byłoby pozbawione sensu, gdyby spseudonimizowane dane należało uznać w każdym wypadku za dane osobowe (pkt 78–80 wyroku). Taka wykładnia wydaje się jednak nadmiernie rozszerzająca. Motyw 16 rozporządzenia 2018/1725, podobnie jak motyw 26 RODO, nie koncentruje się na pseudonimizacji, tylko wyraża swoisty negatyw definicji danych osobowych. Odnosi się on do informacji anonimowych jako takich, które – jak wskazuje w zdaniu piątym – „nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną” lub które „zostały zanonimizowane w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować”²¹. Wprowadzanie kategorii danych spseudonimizowanych identyfikowalnych oraz nieidentyfikowalnych wydaje się niepoparte przepisami prawa, a dane, które nie pozwalają na identyfikację osoby w ogóle, powinny być kwalifikowane jako dane anonimowe, a nie jako szczególny podtyp danych spseudonimizowanych.

Jak wskazano wyżej, TSUE przyjął, że kwalifikacja danej informacji spseudonimizowanej jako danych osobowych zależy od możliwości

identyfikacji osoby, której dane dotyczą, ocenianej z perspektywy konkretnego podmiotu. W konsekwencji to, co dla administratora stanowi dane osobowe, nie musi mieć takiego charakteru dla odbiorcy spseudonimizowanych danych osobowych, w szczególności jeśli ten nie dysponuje środkami identyfikacyjnymi. Przyjęcie takiego podejścia rodzi jednak istotne problemy praktyczne i systemowe, prowadząc do niejasności co do zakresu zastosowania ochrony przewidzianej w prawie ochrony danych osobowych.

W omawianej sprawie TSUE uznał, że SRB pozostawał przez cały czas administratorem (pkt 76 wyroku). Funkcja administratora ma zasadniczy charakter w systemie ochrony danych osobowych i jest powiązana szeregiem obowiązków, także tych związanych z przesłaniem danych osobowych do podmiotu trzeciego. Przykładowo powstaje obowiązek informacyjny²², zgodnie z którym na etapie zbierania danych osobowych powinien on wskazać „informacje o odbiorcach danych osobowych lub o kategoriach odbiorców”. Administrator musi również zamieścić w rejestrze czynności przetwarzania danych osobowych²³ informacje o kategoriach odbiorców, którym dane osobowe zostały ujawnione. W sytuacji, gdy dane będą transferowane poza obszar Europejskiego Obszaru Gospodarczego, rodzi to obowiązek przekazania ich z zastrzeżeniem odpowiednich zabezpieczeń²⁴. Nie wspominając o sytuacji, w której odbiorcą danych osobowych byłby podmiot przetwarzający, z którym administrator musi zawrzeć umowę regulującą przetwarzanie danych osobowych²⁵. Występuje tu więc dwustronna relacja między administratorem i odbiorcą danych osobowych, która opiera się na założeniu, że przetwarzane są dane osobowe, co samo z siebie jest źródłem wzajemnych obowiązków.

²² Zob. szerzej: J. Łuczak, *Komentarz do art. 13 i 14, [w:] RODO...*, s. 477–492.

²³ Zob. szerzej: *ibidem*, s. 661–681.

²⁴ Zob. szerzej: P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025, s. 555–565.

²⁵ Zob. szerzej: M. Sakowska-Baryła, *Komentarz do art. 28, [w:] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

²¹ J. Cobbe, *A Relative Mess: Identifying Data Subjects in Multi-Party Processing*, <https://ssrn.com/abstract=5731364> (dostęp: 17.01.2026).

Konstrukcja ta ulega jednak zasadniczemu zachwianiu, gdy administrator przekazuje dane osobowe podmiotowi, który nie będzie ze swojej perspektywy przetwarzał danych osobowych. Administratorowi pozbawia się więc „partnera”, z którym mógłby pozostawać w relacji regulowanej przepisami prawa ochrony danych. Z punktu widzenia RODO oraz rozporządzenia 2018/1725 niejasne staje się wówczas, jaki jest status prawny podmiotu otrzymującego takie dane, jakie obowiązki na nim ciążyą oraz jaką rolę pełni on w łańcuchu przetwarzania. Jak się wydaje, zgodnie z wyrokiem w sprawie *SRB* wyłącza to działania Deloitte spod parasola regulacyjnego, pozostawiając zarządzanie tym przetwarzaniem w sferze prawa prywatnego. Tę sprzeczność doskonale widać w rozważaniach TSUE dotyczących momentu powstania obowiązku informacyjnego. Trybunał słusznie wskazał, że obowiązek ten materializuje się na etapie gromadzenia danych osobowych tak, by osoba, której dane dotyczą, mogła podjąć świadomą decyzję o ich podaniu i by w razie potrzeby mieć możliwość obrony swoich praw względem ich odbiorców (pkt 108–109 wyroku). Słusznie zostało wskazane, że ocena ta musi być podejmowana z perspektywy administratora (pkt 110–115 wyroku). Trybunał stwierdza więc, że *SRB* było zobowiązane do poinformowania osób, których dane dotyczą, o przekazaniu danych osobowych do Deloitte (pkt 110–112 wyroku). W tym kontekście niezrozumiałe stają się jednak dalsze rozważania TSUE, zmierzające do stwierdzenia, że Deloitte może jednak nie otrzymać danych osobowych (pkt 112 wyroku). Skoro zgodnie z logiką TSUE obowiązek informacyjny należy oceniać z punktu widzenia administratora i na moment zbierania danych, a *SRB* ze swojej perspektywy przesyła dane osobowe, to konsekwentnie Deloitte powinien być odbiorcą danych osobowych. Z kolei osoby, których dane dotyczą, powinny móc być w stanie egzekwować swoje prawa względem odbiorców danych osobowych, o których zostali poinformowani przez administratora. Próba późniejszego „oderwania” Deloitte od roli odbiorcy danych osobowych prowadzi do wewnętrznej niespójności rozumowania TSUE i osłabia spójność całego systemu danych osobowych.

W kontekście oceny identyfikowalności TSUE odwołał się do utrwalonego orzecznictwa²⁶, wskazując, że zgodnie z kryterium „uzasadnionego prawdopodobieństwa zastosowania środka identyfikacji” należy wykluczyć sytuacje, w których identyfikacja jest zakazana prawem lub niewykonalna w praktyce, w szczególności z uwagi na nadmierny nakład czasu, kosztów lub pracy ludzkiej (pkt 82 wyroku). Kryterium to ma swoje korzenie w opinii Rzecznika Generalnego Manuela Ámposy-Sancheza-Bordony²⁷ i stanowi niejako twórcze (dodające do niego kryterium zgodności z prawem) rozwinięcie motywu 26 RODO, który nakazuje rozważać „wszelkie rozsądnie prawdopodobne sposoby [identyfikacji]”. Na tym tle rozumowanie przyjęte przez TSUE w sprawie *SRB* budzi wątpliwości. Trybunał uznał, że Deloitte nie przetwarzał danych osobowych, ponieważ nie był w stanie samodzielnie zidentyfikować osób, których dane dotyczyły. Jednocześnie przez cały okres przetwarzania spółka *SRB*, jako administrator pozostający z Deloitte w relacji umownej, dysponowała kluczem identyfikacyjnym pozwalającym na powiązanie danych spseudonimizowanych z konkretnymi osobami. Konfrontując te fakty z rozumowaniem przyjętym przez TSUE, nie wydaje się nieprawdopodobne, niezgodne z prawem ani związane z nadmiernymi nakładami pracy czy kosztów, by administrator wydał podmiotowi, do którego wysłał dane osobowe, polecenie pomocy w audycie czy też asystowania w realizacji jednego z praw osób, których dane dotyczą. Działania takie jak te wskazane wyżej racjonalnie powinny zaś wiązać się z możliwością identyfikacji poszczególnych osób. Niezależnie od tego, czy *SRB* faktycznie skorzystała z takich uprawnień, istniały obiektywnie prawdopodobne środki umożliwiające identyfikację osób stojących za danymi spseudonimizowanymi przetwarzanymi przez Deloitte. Ocena TSUE, zgodnie z którą ryzyko identyfika-

²⁶ Tak m.in. sprawa *Breyer*, pkt 46; sprawa *OC*, pkt 51.

²⁷ Opinia Rzecznika Generalnego Manuela Ámposy-Sancheza-Bordony z dnia 12 maja 2016 r. w sprawie C-582/14, *Breyer*, ECLI:EU:C:2016:339, pkt 68.

cji było w niniejszej sprawie nieprawdopodobne, nie wydaje się w pełni przekonująca.

Podsumowanie

Na zakończenie warto odnieść się do projektowanych zmian w prawie ochrony danych osobowych, które przewidują m.in. redefinicję pojęć danych osobowych i pseudonimizacji. Propozycje te w dużej mierze odzwierciedlają wnioski TSUE w sprawie *SRB*, przewidują bowiem, że informacja dotycząca osoby fizycznej nie musi być uznawana za dane osobowe dla każdego podmiotu, jeżeli dany podmiot nie może jej zidentyfikować przy użyciu środków wystarczających prawdopodobnych w praktyce. Szczegółowa ocena tych zmian wykracza poza ramy niniejszej glosy, zwłaszcza że propozycje te nie zostały jeszcze przyjęte i nie tworzą obowiązującego prawa. W tym kontekście wykładnia przepisów powinna opierać się przede wszystkim na aktualnie obowiązujących regulacjach, z uwzględnieniem spójności systemowej i pewności prawa oraz ochrony osób, których dane dotyczą.

Nie można wykluczyć, że wyrok w sprawie *SRB* będzie w przyszłości przywoływany przez

różne podmioty jako uzasadnienie dla stosowania teoretycznego braku możliwości identyfikacji danych przez poszczególne podmioty i niepodlegania pod rygorystyczny reżim ochrony danych osobowych²⁸. Zdaniem autora glosy ocena identyfikowalności nie powinna być dokonywana w oderwaniu od całego łańcucha przetwarzania, lecz powinna obejmować łącznie wszystkie podmioty, które w sposób rozsądnie prawdopodobny dysponują środkami umożliwiającymi identyfikację osób, których dane dotyczą. Samodzielna zdolność pojedynczego podmiotu do identyfikacji nie powinna być nadrzędnym kryterium decydującym o charakterze danych osobowych. Przyjęcie odmiennego podejścia prowadzi do erozji systemu ochrony danych osobowych oraz do obciążenia osób, których dane dotyczą, ryzykiem wynikającym z uznaniowego stosowania kryterium „uzasadnionego prawdopodobieństwa zastosowania środka identyfikacji”.

²⁸ D. Korff, *Digital Omnibus: Proposed Changes to the Definition of Personal Data in the EU GDPR Analysed in the Light of the SRB and Earlier CJEU Judgments*, <https://ssrn.com/abstract=5891404> (dostęp: 17.01.2026), s. 19–20.

Abstract

The Contextual Nature of the Classification of Pseudonymized Data as Personal Data in European Union Law – a Partially Critical Commentary on the Judgment of the Court of Justice of the European Union of 4 September 2025, C-413/23 P

Keywords: *personal data; pseudonymization; GDPR; personal data protection; identifiability*

This commentary concerns the judgment of the Court of Justice of the European Union of 4 September 2025 in case C-413/23 P. The commented judgment addresses an important issue, which is the classification pseudonymized data as personal data. The Court held that the assessment of whether pseudonymized data constitute personal data for a given entity is relative. In other words, from the perspective of an entity that does not possess the means enabling the attribution of the data to a specific individual, pseudonymized data received from the controller do not necessarily have the character of personal data. The commentary approves the analysis adopted by the Court with regard to the classification of comments as personal data and the determination of the moment at which the information obligation appears on the controller side pursuant

to Article 15 of Regulation 2018/1725. At the same time, the author challenges the distinction between two categories of pseudonymized data: identifiable and non-identifiable, which in the author's view, results from an incorrect interpretation of the relevant legal articles. In addition, the author disputes the Court's understanding of identifiability in the present case, as well as the trend towards shifting the boundaries of the relative concept of personal data in the light of pseudonymization and assessing it separately for each entity within the processing chain. As the author explains, such an approach leads to legal uncertainty and undermines the system of personal data protection.

Bibliografia

Literatura

Barta P., Kawecki M., Litwiński P., *Komentarz do art. 4, [w:] Ustawa o ochronie danych osobowych. Komentarz, [w:] Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, P. Litwiński (red.), Warszawa 2025.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025.

Kołodziej M., *Pseudonimizacja w RODO – kiedy i jak stosować?*, „ABI Expert” 2018, nr 7.

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018.

Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrik Breyer*, „Europejski Przegląd Sądowy” 2017, nr 5.

Lubasz D., Szkurlat A., *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, „Monitor Prawniczy” 2021, nr 23.

Łuczak J., *Komentarz do art. 13 i 14, [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2018.

Sakowska-Baryła M., *Komentarz do art. 28, [w:] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Mednis A., *Pojęcie danych osobowych, [w:] System Prawa Medycznego, t. 3: Organizacja systemu ochrony zdrowia*, D. Bach-Golecka, R. Stankiewicz (red.), Warszawa 2020.

Taczowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

Witkowska-Nowakowska K., *Komentarz do art. 4 pkt 5, [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, E. Bielak-Jomaa, D. Lubasz (red.), Warszawa 2018.

Akty prawne

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. L 119/1, 4.05.2016).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz. Urz. L 295/39, 21.11.2018).

Orzecznictwo

Wyrok TSUE z dnia 19 października 2016 r. w sprawie C-582/14, *Breyer*, ECLI:EU:C:2016:779.

Wyrok TSUE z dnia 20 grudnia 2017 r. w sprawie C-434/16, *Nowak*, ECLI:EU:C:2017:994.

Wyrok Sądu UE z dnia 26 kwietnia 2023 r. w sprawie T-557/20, *SRB przeciwko EIOD*, ECLI:EU:T:2023:219.
Wyrok TSUE z dnia 4 maja 2023 r. w sprawie C-487/21, *Österreichische Datenschutzbehörde*, ECLI:EU:C:2023:369.
Wyrok TSUE z dnia 9 listopada 2023 r. w sprawie C-319/22, *Gesamtverband Autoteile-Handel*, ECLI:EU:C:2023:837.

Wyrok TSUE z dnia 7 marca 2024 r. w sprawie C-479/22 P, *OC przeciwko Komisji*, ECLI:EU:C:2024:215.
Wyrok TSUE z dnia 4 września 2025 r. w sprawie C-413/23 P, *EIOD przeciwko SRB*, ECLI:EU:C:2025:645.

Źródła internetowe

Cobbe J., *A Relative Mess: Identifying Data Subjects in Multi-Party Processing*, <https://ssrn.com/abstract=5731364> (dostęp: 17.01.2026).

Korff D., *Digital Omnibus: Proposed Changes to the Definition of Personal Data in the EU GDPR Analysed in the Light of the SRB and Earlier CJEU Judgments*, <https://ssrn.com/abstract=5891404> (dostęp: 17.01.2026).

Inne

Opinia 05/2014 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 w sprawie technik anonimizacji przyjęta dnia 10 kwietnia 2014 r.

Opinia Rzecznika Generalnego Manuela Ámpos-Sancheza-Bordony z dnia 12 maja 2016 r. w sprawie C-582/14, *Breyer*, ECLI:EU:C:2016:339.

Opinia Rzecznika Generalnego Deana Spielmanna z dnia 6 lutego 2025 r. w sprawie C-413/23 P, *EIOD przeciwko SRB*, ECLI:EU:C:2025:59.

Projekt rozporządzenia Parlamentu Europejskiego i Rady z dnia 19 listopada 2025 r. Digital Omnibus, COM(2025) 837.