Zbiór Orzeczeń

WYROK SĄDU (szósta izba w składzie powiększonym)

z dnia 8 stycznia 2025 r.*

[Tekst sprostowany postanowieniem z dnia 3 czerwca 2025 r.]

Przetwarzanie danych osobowych – Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii – Rozporządzenie (UE) 2018/1725 – Pojęcie „przekazania danych osobowych do państwa trzeciego” – Przekazanie danych przy przeglądaniu strony internetowej – EU Login – Skarga o stwierdzenie nieważności – Akt niepodlegający zaskarżeniu – Niedopuszczalność – Skarga na bezczynność – Zajęcie stanowiska kończące stan bezczynności – Umorzenie postępowania – Skarga o zadośćuczynienie – Wystarczająco istotne naruszenie normy prawnej przyznającej uprawnienia jednostkom – Związek przyczynowy – Krzywda

W sprawie T-354/22

Thomas Bindl, zamieszkały w Monachium (Niemcy), którego reprezentował T. Herbrich, adwokat,

strona skarżąca,

przeciwko

Komisji Europejskiej, którą reprezentowali A. Bouchagiar, B. Hofstötter i H. Kranenborg, w charakterze pełnomocników,

strona pozwana,

SĄD (szósta izba w składzie powiększonym),

w składzie: M.J. Costeira (sprawozdawczyni), prezes, M. Kancheva, U. Öberg, P. Zilgalvis i E. Tichy-Fisslberger, sędziowie,

sekretarz: S. Jund, administratorka,

uwzględniając pisemny etap postępowania,

uwzględniając środek organizacji postępowania z dnia 21 lipca 2023 r. oraz odpowiedzi Komisji i skarżącego złożone w sekretariacie Sądu w dniach 7 i 8 września 2023 r.,

po przeprowadzeniu rozprawy w dniu 17 października 2023 r.,

* Język postępowania: niemiecki.

uwzględniając środek organizacji postępowania z dnia 9 lutego 2024 r. oraz odpowiedzi Komisji i skarżącego złożone w sekretariacie Sądu w dniach 12 i 13 marca 2024 r.,

wydaje następujący

Wyrok

1 W skardze na podstawie art. 263, 265 i 268 TFUE skarżący, Thomas Bindl, wnosi do Sądu: po pierwsze, o stwierdzenie nieważności przekazania jego danych osobowych do państw trzecich niezapewniających odpowiedniego stopnia ochrony; po drugie, o stwierdzenie, że Komisja Europejska niezgodnie z prawem zaniechała zajęcia stanowiska w przedmiocie jego wniosku o udzielenie informacji z dnia 1 kwietnia 2022 r.; i po trzecie, o naprawienie krzywdy, jakiej miał doznać w wyniku, z jednej strony, naruszenia jego prawa dostępu do informacji, a z drugiej – przekazania jego danych osobowych.

Okoliczności powstania sporu i fakty dotyczące okresu po wniesieniu skargi

2 Skarżący jest obywatelem niemieckim, który interesuje się kwestiami z dziedziny informatyki i ochrony danych osobowych.

3 Dyrekcja Generalna ds. Komunikacji Społecznej Komisji jest administratorem danych osobowych w zakresie strony internetowej Konferencji w sprawie przyszłości Europy pod adresem „https://futureu.europa.eu” (zwanej dalej „stroną internetową KoPE”).

4 Skarżący wielokrotnie przeglądał stronę internetową KoPE w latach 2021 i 2022. Przeglądał on tę stronę internetową między innymi w dniu 30 marca 2022 r. i za pośrednictwem swojego konta na Facebooku zarejestrował się do wzięcia udziału w wydarzeniu „GoGreen”, o którym informacja była tam zamieszczona, a w dniu 8 czerwca 2022 r. ponownie przeglądał wspomnianą stronę internetową.

5 E-mailem z dnia 9 listopada 2021 r. (zwanym dalej „żądaniem udzielenia informacji z dnia 9 listopada 2021 r.”) skarżący zwrócił się do inspektora ochrony danych Komisji o udzielenie mu informacji na podstawie rozporządzenia 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.U. 2018, L 295, s. 39).

6 W omawianym e-mailu, po pierwsze, skarżący wskazał, że zauważył, iż przy połączeniu ze stroną internetową KoPE, uruchomiło się połączenie z dostawcami trzecimi, takimi jak amerykańskie przedsiębiorstwo Amazon Web Services; po drugie, zwrócił się o wskazanie, które dotyczące go dane osobowe zostały przetworzone lub przechowywane a które zostały ewentualnie przekazane osobom trzecim; po trzecie, zażądał informacji na temat podstawy prawnej takiego przekazania, a także na temat istnienia ewentualnych gwarancji dotyczących przekazywania danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony.

7 E-mailem z dnia 3 grudnia 2021 r. Dyrekcja Generalna ds. Komunikacji Społecznej Komisji przekazała skarżącemu link elektroniczny i poinformowała go, że link ten pozwala mu na bezpośrednie generowanie wykazu danych osobowych, które były przetwarzane podczas

przeglądania strony internetowej KoPE. Ponadto wskazała ona skarżącemu, po pierwsze, że jego dane osobowe nie zostały przekazane odbiorcom znajdującym się poza Unią Europejską, a po drugie, że są one przechowywane i przetwarzane przez stronę internetową KoPE, która korzystała z sieci dostarczania treści zarządzanej przez Amazon Web Services EMEA SARL (zwaną dalej „AWS EMEA"), z siedzibą w Luksemburgu (Luksemburg). Ponadto wyjaśniła ona, że w ramach umów zawartych między Komisją a AWS EMEA administrator danych nie korzysta z usług wymagających przekazywania danych partnerom AWS EMEA mającym siedzibę w Stanach Zjednoczonych i że przekazywanie danych poza terytorium Unii nie jest co do zasady dozwolone.

8 [Sprostowany postanowieniem z dnia 3 czerwca 2025 r.] E-mailem z dnia 1 kwietnia 2022 r. skarżący zwrócił się do Komisji, na podstawie rozporządzenia 2018/1725, z wnioskiem o udzielenie informacji na temat przetwarzania jego danych (zwanym dalej „wnioskiem o udzielenie informacji z dnia 1 kwietnia 2022 r."). W pierwszej kolejności wskazał, że zauważył, iż w momencie połączenia się ze stroną internetową KoPE uruchomiło się połączenie z dostawcami będącymi osobami trzecimi, takimi jak AWS EMEA, i że przy wykorzystaniu swoich danych dotyczących połączenia Facebooka w celu zarejestrowania się na tej stronie internetowej powstało połączenie z przedsiębiorstwem Meta Platforms. W drugiej kolejności zwrócił się on o wskazanie, jakie dotyczące go dane osobowe zostały przetworzone lub przechowywane i jakie zostały ewentualnie przekazane osobom trzecim. W trzeciej kolejności zażądał informacji na temat podstawy prawnej takiego przekazania, a także na temat istnienia ewentualnych gwarancji dotyczących przekazywania danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony. W czwartej kolejności zażądał on kopii swoich danych, w tym danych przechowywanych lub przetwarzanych przez osoby trzecie, takie jak Facebook.

9 W e-mailach z dni 22 kwietnia i 2 maja 2022 r. skarżący nalegał, aby Komisja odpowiedziała na wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r.

10 Pismem złożonym w sekretariacie Sądu w dniu 9 czerwca 2022 r. skarżący wniósł skargę w niniejszej sprawie.

11 E-mailem z dnia 30 czerwca 2022 r. Komisja poinformowała skarżącego, że uważa, iż wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r. jest prawie identyczny z wnioskiem o udzielenie informacji z dnia 9 listopada 2021 r. i że już odpowiedziała na ten wniosek wiadomością z dnia 3 grudnia 2021 r.

12 Amazon Web Services jest przedsiębiorstwem z siedzibą w Stanach Zjednoczonych, a AWS EMEA jest przedsiębiorstwem z siedzibą w Luksemburgu. Oba te przedsiębiorstwa są spółkami zależnymi przedsiębiorstwa prawa amerykańskiego Amazon.com, Inc.

Żądania stron

13 Skarżący wnosi do Sądu o:

– stwierdzenie nieważności przekazania danych osobowych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony, do którego doszło w dniach 30 marca i 8 czerwca 2022 r.;

– stwierdzenie, że Komisja niezgodnie z prawem zaniechała zajęcia stanowiska w przedmiocie wniosku o udzielenie informacji z dnia 1 kwietnia 2022 r.;

– zasądzenie od Komisji na jego rzecz kwoty 1200 EUR wraz z odsetkami, odpowiadającej, po pierwsze, kwocie 800 EUR tytułem zadośćuczynienia za krzywdę doznaną w wyniku naruszenia prawa dostępu do informacji, a po drugie, kwocie 400 EUR tytułem zadośćuczynienia za krzywdę doznaną w wyniku wspomnianego przekazania jego danych;

– obciążenie Komisji kosztami postępowania.

14 Komisja wnosi do Sądu o:

– odrzucenie żądań stwierdzenia nieważności i żądań stwierdzenia bezczynności jako niedopuszczalnych;

– tytułem żądania ewentualnego – umorzenie postępowania w przedmiocie żądania stwierdzenia bezczynności;

– oddalenie żądań odszkodowawczych jako bezzasadnych;

– obciążenie skarżącego kosztami postępowania.

Co do prawa

Uwagi wstępne na temat ochrony danych osobowych przez instytucje, organy i jednostki organizacyjne Unii

15 Artykuł 16 ust. 1 TFUE i art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą”) stanowią, że każdy ma prawo do ochrony danych osobowych, które go dotyczą.

16 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) ustanawia normy ogólne mające na celu ochronę osób fizycznych w związku z przetwarzaniem danych osobowych oraz zapewnienie swobodnego przepływu takich danych (art. 1 ust. 1 rozporządzenia 2016/679).

17 Rozporządzenie 2018/1725 ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy Unii oraz przepisy o swobodnym przepływie danych osobowych między tymi instytucjami i organami Unii lub do innych odbiorców mających siedzibę w Unii (art. 1 ust. 1 rozporządzenia 2018/1725). To rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych (art. 1 ust. 2 rozporządzenia 2018/1725). Omawiane rozporządzenie stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy Unii (art. 2 ust. 1 rozporządzenia 2018/1725).

18 W motywie 5 rozporządzenia 2018/1725 przypomniano, że zgodnie z orzecznictwem Trybunału w każdym przypadku, w którym przepisy rozporządzenia 2018/1725 opierają się na tych samych założeniach, co przepisy rozporządzenia 2016/679, przepisy obu aktów należy interpretować tak samo, w szczególności ze względu na fakt, że systematyka rozporządzenia 2018/1725 powinna

być uznawana za tożsamą z systematyką rozporządzenia 2016/679. W tym względzie z brzmienia przepisów art. 2 ust. 3 rozporządzenia 2016/679 i art. 99 rozporządzenia 2018/1725 wynika, że to ostatnie rozporządzenie jest dostosowane do zasad i przepisów rozporządzenia 2016/679.

W przedmiocie dopuszczalności

Dopuszczalność skargi żądań stwierdzenia nieważności

19 W ramach żądania pierwszego skarżący wnosi o stwierdzenie nieważności przekazania jego danych osobowych do państw trzecich niezapewniających odpowiedniego stopnia ochrony, do którego doszło w dniach 30 marca i 8 czerwca 2022 r. (zwanego dalej „spornymi przekazaniami danych").

20 W odpowiedzi na skargę Komisja podnosi niedopuszczalność tego żądania stwierdzenia nieważności ze względu na to, że nie jest ono skierowane przeciwko aktowi zaskarżalnemu w rozumieniu art. 263 TFUE, lecz zmierza do skierowania do niej nakazu.

21 Skarżący podnosi dopuszczalność żądania stwierdzenia nieważności, twierdząc przy tym, że sporne przekazania danych są czynnościami wywołującymi wiążące skutki prawne i mającymi wpływ na jego sytuację prawną i naruszającymi jego prawo podstawowe do ochrony danych osobowych zagwarantowane w art. 8 Karty. Każda inna wykładnia byłaby niezgodna z prawem podstawowym do skutecznej ochrony sądowej, podczas gdy art. 64 ust. 1 rozporządzenia 2018/1725 wyraźnie ustanawia to prawo.

22 Jak przypomniano w art. 64 ust. 1 i motywie 79 rozporządzenia 2018/1725, każda osoba ma prawo do skutecznego środka ochrony prawnej przed Trybunałem Sprawiedliwości Unii Europejskiej, zgodnie z traktatami, jeżeli uzna, że jej prawa ustanowione w tym rozporządzeniu zostały naruszone.

23 Wynika z tego, że w ramach rozporządzenia 2018/1725 każda osoba, której dane dotyczą, ma prawo wnieść skargę o stwierdzenie nieważności na warunkach przewidzianych w art. 263 TFUE.

24 Zgodnie z utrwalonym orzecznictwem skarga o stwierdzenie nieważności przewidziana w art. 263 TFUE przysługuje przeciwko każdemu aktowi prawnemu instytucji, niezależnie od jego formy, zmierzającemu do wywołania wiążących skutków prawnych mogących naruszać interesy strony skarżącej poprzez istotną zmianę jej sytuacji prawnej (zob. wyroki: z dnia 19 stycznia 2017 r., Komisja/Total i Elf Aquitaine, C-351/15 P, EU:C:2017:27, pkt 35, 36 i przytoczone tam orzecznictwo; z dnia 16 lipca 2020 r., Inclusion Alliance for Europe/Komisja, C-378/16 P, EU:C:2020:575, pkt 71 i przytoczone tam orzecznictwo).

25 W celu ustalenia, czy akt wywołuje wiążące skutki prawne, należy zgodnie z utrwalonym orzecznictwem Trybunału uwzględnić jego istotę i dokonać oceny jego skutków w świetle obiektywnych kryteriów, takich jak treść wspomnianego aktu, biorąc pod uwagę w razie potrzeby kontekst jego przyjęcia, a także uprawnienia instytucji, organu lub jednostki organizacyjnej Unii, które są jego autorami (zob. wyrok z dnia 15 lipca 2021 r., FBF, C-911/19, EU:C:2021:599, pkt 38 i przytoczone tam orzecznictwo).

26 W niniejszej sprawie skarżący żąda stwierdzenia nieważności spornych przekazań danych, do których jego zdaniem doszło trzykrotnie. W pierwszej kolejności, podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. (zwanego dalej „spornym przekazaniem danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r."), należące do niej dane osobowe, w szczególności adres IP oraz informacje o przeglądarce i terminalu, zostały przekazane amerykańskiemu przedsiębiorstwu Amazon Web Services jako operatorowi sieci dostarczania treści zwanej Amazon CloudFront, która jest wykorzystywana przez wspomnianą stronę internetową.

27 W drugiej kolejności, podczas połączenia przez skarżącego w dniu 30 marca 2022 r. z usługą uwierzytelniania użytkownika Komisji EU Login za pomocą jego konta na Facebooku w celu rejestracji na wydarzenie „GoGreen" zamieszczone na stronie internetowej KoPE (zwane dalej „spornym przekazaniem danych podczas połączenia z EU Login w dniu 30 marca 2022 r.") należące do niego dane osobowe, w szczególności jego adres IP oraz informacje o przeglądarce i terminalu, zostały przekazane amerykańskiemu przedsiębiorstwu Meta Platforms, Inc.

28 W trzeciej kolejności, podczas przeglądania przez skarżącego strony internetowej KoPE w dniu 8 czerwca 2022 r. (zwanego dalej „spornym przekazaniem danych podczas przeglądania strony internetowej KoPE z dnia 8 czerwca 2022 r.") należące do niego dane osobowe zostały przekazane do serwera Amazon CloudFront znajdującego się w Newark (New Jersey, Stany Zjednoczone).

29 Ponadto skarżący wskazuje w skardze, że uzyskał dostęp do strony internetowej KoPE w dniu 9 listopada 2021 r. i że w tym dniu zarejestrował się na stronie internetowej KoPE za pośrednictwem swojego konta na Facebooku. Jednakże nie powołuje się on na żadną konkretną okoliczność pozwalającą na stwierdzenie, że jego żądanie stwierdzenia nieważności spornych przekazań danych dotyczy tych okoliczności. Należy zatem wziąć pod uwagę wyłącznie sporne przekazania danych, o których mowa w pkt 26–28 powyżej.

30 Należy zauważyć, że sporne przekazania danych, których stwierdzenia nieważności domaga się skarżący, wspomniane w pkt 26–28 powyżej, odpowiadają, zdaniem samego skarżącego, operacjom informatycznym związanym z migracją danych, które zostały zainicjowane przez systemy lub służby informatyczne Komisji, w szczególności przez stronę internetową KoPE, na serwery należące do przedsiębiorstw trzecich mających siedzibę poza terytorium Unii.

31 Prawdą jest, że operacja polegająca na przekazywaniu danych osobowych z instytucji lub organu Unii do państwa trzeciego stanowi jako taka przetwarzanie danych osobowych w rozumieniu art. 3 pkt 3 rozporządzenia 2018/1725, dokonywane na terytorium Unii, do którego to przetwarzania rozporządzenie to ma zastosowanie na mocy art. 2 ust. 5 (zob. analogicznie wyrok z dnia 16 lipca 2020 r., Facebook Ireland i Schrems, C-311/18, zwany dalej „wyrokiem Schrems II", EU:C:2020:559, pkt 83).

32 Jednakże nie wszystkie operacje mogące prowadzić do przekazania danych osobowych w rozumieniu art. 3 pkt 3 rozporządzenia 2018/1725 stanowią akty zaskarżalne w rozumieniu art. 263 TFUE, zgodnie z jego wykładnią dokonaną w orzecznictwie przypomnianym w pkt 24 powyżej.

33 W niniejszej sprawie – zakładając, że zostanie wykazane, iż doszło do spornych przekazań danych – należy stwierdzić, że stanowią one czynności materialne, a nie akty prawne. Sporne przekazania danych, takie jak opisane w skardze, są bowiem operacjami informatycznymi migracji danych

z jednego terminala lub serwera na drugi, które wynikają z interakcji między skarżącym a systemami lub usługami informatycznymi Komisji podczas przeglądania przez niego strony internetowej KoPE lub korzystania z usługi EU Login. Natomiast sporne przekazania danych nie są aktami Komisji wywołującymi wiążące skutki prawne, to znaczy nie mają na celu uregulowania sytuacji prawnej i, jak wynika z samego ich charakteru, Komisja w żaden sposób nie miała zamiaru nadać im takich skutków.

34 W związku z tym sporne przekazania danych nie mogą wywoływać wiążących skutków prawnych mogących naruszyć interesy skarżącego, zmieniając w istotny sposób jego sytuację prawną, zgodnie z orzecznictwem przypomnianym w pkt 24 powyżej. Nie można ich zatem uznać za akty zaskarżalne w rozumieniu art. 263 TFUE.

35 Z powyższego wynika, że żądania skarżącego dotyczące stwierdzenia nieważności należy odrzucić jako niedopuszczalne.

Dopuszczalność żądań stwierdzenia bezczynności

36 W żądaniu drugim skarżący wnosi do Sądu o stwierdzenie, że Komisja niezgodnie z prawem zaniechała zajęcia stanowiska w przedmiocie wniosku o udzielenie informacji z dnia 1 kwietnia 2022 r.

37 W odpowiedzi na skargę Komisja podnosi niedopuszczalność tego żądania stwierdzenia bezczynności ze względu na brak wezwania do działania w rozumieniu art. 265 akapit drugi TFUE. Tytułem ewentualnym Komisja podnosi, że postępowanie w sprawie żądania stwierdzenia bezczynności należy umorzyć ze względu na jej odpowiedź udzieloną skarżącemu w wiadomości elektronicznej z dnia 30 czerwca 2022 r.

38 Skarżący twierdzi zasadniczo, że Komisja jest nadal zobowiązana do odpowiedzi na wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r., ponieważ informacje, które przekazała w wiadomości elektronicznej z dnia 30 czerwca 2022 r., są niewystarczające i niedokładne.

39 Zgodnie z utrwalonym orzecznictwem środek zaskarżenia przewidziany w art. 265 TFUE opiera się na założeniu, że podnoszona niezgodna z prawem bezczynność danej instytucji pozwala na wystąpienie do sądu Unii o stwierdzenie, że zaniechanie działania jest sprzeczne z traktatem, jeżeli dana instytucja nie zaradziła temu zaniechaniu (wyrok z dnia 12 lipca 1988 r., Parlament/Rada, 377/87, EU:C:1988:387, pkt 9; zob. także wyrok z dnia 16 grudnia 2015 r., Szwecja/Komisja, T-521/14, niepublikowany, EU:T:2015:976, pkt 33 i przytoczone tam orzecznictwo).

40 W przypadku gdy akt, którego zaniechanie jest przedmiotem sporu, został podjęty po wniesieniu skargi, lecz przed ogłoszeniem wyroku, stwierdzenie przez sąd Unii niezgodności z prawem pierwotnego zaniechania nie może już prowadzić do skutków przewidzianych w art. 266 TFUE. Wynika z tego, że w takim przypadku przedmiot skargi przestał istnieć, w związku z czym należy umorzyć postępowanie (wyrok z dnia 12 lipca 1988 r., Parlament/Rada, 377/87, EU:C:1988:387, pkt 10, 11; zob. także postanowienie z dnia 13 grudnia 2000 r., Sodima/Komisja, C-44/00 P, EU:C:2000:686, pkt 83 i przytoczone tam orzecznictwo).

41 W niniejszej sprawie należy stwierdzić, że Komisja odpowiedziała na wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r. w wiadomości elektronicznej z dnia 30 czerwca 2022 r. (zob. pkt 11 powyżej). Komisja położyła zatem kres bezczynności zarzucanej przez skarżącego

w ramach niniejszej skargi po wniesieniu tej skargi. Żądanie drugie mające na celu stwierdzenie, na podstawie art. 265 TFUE, bezczynności Komisji w braku odpowiedzi na żądanie udzielenia informacji z dnia 1 kwietnia 2022 r. stało się zatem bezprzedmiotowe.

42 Okoliczność, że treść wiadomości elektronicznej Komisji z dnia 30 czerwca 2022 r. nie odpowiada odpowiedzi żądanej przez skarżącego, jest w tym względzie bez znaczenia. Okoliczność, że to zajęcie stanowiska przez instytucję nie satysfakcjonuje strony skarżącej, jest bowiem w tym względzie bez znaczenia, ponieważ art. 265 TFUE dotyczy bezczynności z powodu zaniechania działania lub zajęcia stanowiska, a nie wydania aktu innego niż ten, którego przyjęcie strona skarżąca uznała za pożądane lub konieczne (zob. postanowienie z dnia 6 kwietnia 2017 r., Brancheforeningen for Regulerkraft i Danmark/Komisja, T-203/16, niepublikowane, EU:T:2017:279, pkt 22 i przytoczone tam orzecznictwo).

43 Z powyższego wynika, że należy umorzyć postępowanie w przedmiocie wysuniętego przez skarżącego żądania stwierdzenia bezczynności i że nie ma potrzeby orzekania w przedmiocie podniesionej przez Komisję niedopuszczalności tych żądań.

W przedmiocie żądań odszkodowawczych

44 W żądaniu trzecim skarżący formułuje dwa żądania odszkodowawcze. W pierwszej kolejności domaga się on zapłaty 800 EUR tytułem zadośćuczynienia za krzywdę, jakiej miał doznać z powodu nieprzestrzegania przez Komisję przysługującego mu prawa dostępu do informacji z naruszeniem art. 14 ust. 3 i 4 oraz art. 17 ust. 1 i 2 rozporządzenia 2018/1725, a także zasady przejrzystości przewidzianej w art. 4 ust. 1 lit. a) tego rozporządzenia. W drugiej kolejności domaga się on zapłaty 400 EUR tytułem zadośćuczynienia za krzywdę, jakiej miał doznać w wyniku spornych przekazań danych, co nastąpiło z naruszeniem art. 46 i art. 48 ust. 1 i art. 48 ust. 2 lit. b) rozporządzenia 2018/1725.

45 Komisja wnosi o oddalenie żądań odszkodowawczych.

Uwagi wstępne w przedmiocie przesłanek powstania pozaumownej odpowiedzialności Unii w ramach rozporządzenia 2018/1725

46 Artykuł 65 rozporządzenia 2018/1725 stanowi, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia tego rozporządzenia, ma prawo uzyskać od instytucji lub organu Unii odszkodowanie za poniesioną szkodę, z zastrzeżeniem „warunków określonych w traktatach”.

47 Artykuł 65 rozporządzenia 2018/1725 należy interpretować w ten sposób, że przewiduje on, iż prawo do uzyskania od instytucji lub organu Unii naprawienia szkody poniesionej w wyniku naruszenia tego rozporządzenia jest uzależnione od spełnienia przesłanek określonych w art. 340 akapit drugi TFUE, stosownie do którego Unia powinna naprawić, zgodnie z zasadami ogólnymi wspólnymi dla praw państw członkowskich, szkody wyrządzone przez jej instytucje lub jej pracowników przy wykonywaniu ich obowiązków.

48 Zgodnie z utrwalonym orzecznictwem powstanie odpowiedzialności pozaumownej Unii jest uzależnione od łącznego spełnienia trzech przesłanek, a mianowicie bezprawności zarzucanego instytucjom działania, rzeczywistego charakteru szkody oraz istnienia związku przyczynowego

między tym działaniem a szkodą (zob. podobnie wyroki: z dnia 4 lipca 2000 r., Bergaderm i Goupil/Komisja, C-352/98 P, EU:C:2000:361, pkt 39–42; z dnia 28 października 2021 r., Vialto Consulting/Komisja, C-650/19 P, EU:C:2021:879, pkt 138).

49 Ze względu na to, że przesłanki te muszą być spełnione łącznie, jeśli jedna z nich nie jest spełniona, skargę o odszkodowanie należy oddalić w całości, bez potrzeby badania pozostałych przesłanek (wyrok z dnia 9 września 1999 r., Lucaccioni/Komisja, C-257/98 P, EU:C:1999:402, pkt 14, 63; zob. również wyrok z dnia 25 lutego 2021 r., Dalli/Komisja, C-615/19 P, EU:C:2021:133, pkt 42 i przytoczone tam orzecznictwo).

50 Co się tyczy pierwszej z przesłanek, orzecznictwo wymaga, aby ustalone zostało istnienie wystarczająco istotnego naruszenia normy prawnej, która przyznaje jednostkom określone uprawnienia (zob. wyrok z dnia 4 lipca 2000 r., Bergaderm i Goupil/Komisja, C-352/98 P, EU:C:2000:361, pkt 42 i przytoczone tam orzecznictwo).

51 Ów wymóg wystarczająco istotnego naruszenia prawa Unii ma na celu, bez względu na rodzaj rozpatrywanego bezprawnego aktu, uniknięcie sytuacji, w której ryzyko konieczności ponoszenia ciężaru odszkodowania za szkody podnoszone przez zainteresowane osoby upośledziłoby zdolność danej instytucji do wykonywania w pełnym zakresie swoich kompetencji w interesie ogólnym, zarówno w ramach jej działalności prawodawczej czy wymagającej podejmowania decyzji z zakresu polityki ekonomicznej, jak i w sferze jej kompetencji administracyjnych, a przy tym jednak ma również na celu niedopuszczenie do tego, by ciężar konsekwencji oczywistych i nieusprawiedliwionych naruszeń spoczywał na jednostkach (zob. podobnie wyrok z dnia 14 grudnia 2018 r., East West Consulting/Komisja, T-298/16, EU:T:2018:967, pkt 124 i przytoczone tam orzecznictwo).

52 Rozstrzygające kryterium pozwalające stwierdzić, że naruszenie jest wystarczająco istotne, polega na oczywistym i poważnym wykroczeniu przez odnośną instytucję lub organ Unii poza granice przysługującego im uznania. Jeżeli tej instytucji lub temu organowi przysługuje jedynie znacznie ograniczony zakres uznania lub nie ma on takiego zakresu uznania, jakiekolwiek naruszenie prawa Unii może wystarczyć do wykazania istnienia wystarczająco istotnego naruszenia (zob. wyrok z dnia 10 grudnia 2002 r., Komisja/Camar i Tico, C-312/00 P, EU:C:2002:736, pkt 54 i przytoczone tam orzecznictwo). Jednak w orzecznictwie tym nie ustanowiono żadnego automatycznego związku między brakiem uprawnień dyskrecjonalnych danej instytucji z jednej strony a zakwalifikowaniem naruszenia jako wystarczająco istotnego naruszenia prawa Unii z drugiej strony (wyrok z dnia 3 marca 2010 r., Artegodan/Komisja, T-429/05, EU:T:2010:60, pkt 59). O ile bowiem zakres uprawnień dyskrecjonalnych danej instytucji posiada decydujące znaczenie, o tyle nie stanowi on wyłącznego kryterium. W tym względzie Trybunał konsekwentnie przypominał, że system wypracowany przez niego na podstawie art. 340 akapit drugi TFUE uwzględnia ponadto w szczególności złożoność sytuacji, które podlegają uregulowaniu, oraz trudności w stosowaniu lub wykładni aktów prawnych (zob. wyrok z dnia 23 listopada 2011 r., Sison/Rada, T-341/07, EU:T:2011:687, pkt 36, 37 i przytoczone tam orzecznictwo) lub, bardziej ogólnie, dziedzinę, przesłanki i kontekst, w którym naruszona norma jest wiążąca dla danej instytucji lub danego organu Unii (zob. wyrok z dnia 4 kwietnia 2017 r., Rzecznik Praw Obywatelskich/Staelen, C-337/15 P, EU:C:2017:256, pkt 40 i przytoczone tam orzecznictwo).

53 Wynika z tego, że jedynie stwierdzenie istnienia nieprawidłowości, której nie dopuściłby się w podobnych okolicznościach organ administracyjny w zwykły sposób rozważny i staranny, pozwala na powstanie odpowiedzialności Unii. Sąd Unii powinien zatem, po ustaleniu, czy danej instytucji przysługuje zakres uznania, wziąć pod uwagę złożoność podlegającej uregulowaniu

sytuacji, trudności w stosowaniu lub wykładni przepisów prawa, stopień jasności i precyzji naruszonej normy oraz umyślny lub nieznajdujący uzasadnienia charakter popełnionego naruszenia (wyrok z dnia 3 marca 2010 r., Artegodan/Komisja, T-429/05, EU:T:2010:60, pkt 62).

54 Jeśli chodzi o przesłankę dotyczącą rzeczywistego charakteru szkody, szkoda musi być rzeczywista i pewna, czego udowodnienie należy do strony skarżącej (zob. wyrok z dnia 9 listopada 2006 r., Agraz i in./Komisja, C-243/05 P, EU:C:2006:708, pkt 27 i przytoczone tam orzecznictwo). Natomiast szkoda czysto hipotetyczna i nieokreślona nie daje podstaw do żądania odszkodowania (zob. wyrok z dnia 26 października 2011 r., Dufour/EBC, T-436/09, EU:T:2011:634, pkt 192 i przytoczone tam orzecznictwo).

55 Ta ostatnia przesłanka dotycząca związku przyczynowego wymaga istnienia wystarczająco bezpośredniego związku przyczynowego pomiędzy zachowaniem zarzucanym instytucji a szkodą, a udowodnienie tego związku należy do strony skarżącej w taki sposób, że zarzucane zachowanie powinno być decydującą przyczyną szkody (zob. wyrok z dnia 13 grudnia 2018 r., Unia Europejska/ASPLA i Armando Álvarez, C-174/17 P i C-222/17 P, EU:C:2018:1015, pkt 23 i przytoczone tam orzecznictwo).

56 Ponadto należy przypomnieć, że skarga o odszkodowanie na podstawie art. 340 akapit drugi TFUE, została wprowadzona jako autonomiczny środek prawny, odgrywający szczególną rolę w systemie środków zaskarżenia i podlegający wymogom ustanowionym ze względu na jego szczególny cel, skutkiem czego stwierdzenie niedopuszczalności żądania o stwierdzenie nieważności nie powoduje automatycznie niedopuszczalności żądania odszkodowawczego (zob. wyrok z dnia 5 września 2019 r., Unia Europejska/Guardian Europe i Guardian Europe/Unia Europejska, C-447/17 P i C-479/17 P, EU:C:2019:672, pkt 49 i przytoczone tam orzecznictwo).

57 Wynika z tego, że odrzucenie żądania stwierdzenia nieważności z uwagi na jego niedopuszczalność oraz odrzucenie żądania stwierdzenia bezczynności z uwagi na umorzenie postępowania w jego zakresie, zgodnie z pkt 35 i 43 powyżej, nie oznaczają w konsekwencji odrzucenia żądań odszkodowawczych, o których mowa w pkt 44 powyżej, jako niedopuszczalnych.

58 W świetle tych właśnie uwag należy zbadać zarzuty podniesione przez skarżącego w ramach żądań odszkodowawczych.

W przedmiocie pierwszego żądania odszkodowawczego, zmierzającego do uzyskania zadośćuczynienia za krzywdę wynikającą z naruszenia prawa dostępu do informacji

59 W pierwszym żądaniu odszkodowawczym skarżący wnosi o zasądzenie od Komisji na jego rzecz kwoty 800 EUR tytułem zadośćuczynienia za krzywdę doznaną w następstwie naruszenia jego prawa dostępu do informacji.

60 Przede wszystkim skarżący zarzuca Komisji, że nie odpowiedziała na wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r. w wyznaczonym terminie i że nie podała mu uzasadnienia swojej bezczynności z naruszeniem art. 14 ust. 3 i 4 oraz art. 17 ust. 1 i 2 rozporządzenia 2018/1725, a także zasady przejrzystości przewidzianej w art. 4 ust. 1 lit. a) tego rozporządzenia. Ponadto Komisja naruszyła art. 17 ust. 1 lit. c) i art. 17 ust. 2 rozporządzenia 2018/1725, ponieważ oświadczenie o ochronie prywatności, które znajduje się na stronie internetowej KoPE, nie zawiera informacji dotyczących przekazywania danych osobowych do państw trzecich i ewentualnych odpowiednich zabezpieczeń do celów wspomnianego przekazania, czego wymaga

art. 48 wspomnianego rozporządzenia. Poza tym w wiadomości elektronicznej z dnia 3 grudnia 2021 r. Komisja przedstawiła błędne informacje, ponieważ zaprzeczyła przekazaniu danych osobowych skarżącego do odbiorców w Stanach Zjednoczonych.

61 Następnie skarżący twierdzi, że zawiniona bezczynność Komisji uniemożliwiła mu kontrolowanie przetwarzania jego danych osobowych, co stanowi krzywdę w rozumieniu motywu 46 rozporządzenia 2018/1725. Wreszcie podnosi on, że krzywda, którą szacuje na 800 EUR, jest bezpośrednio spowodowana zawinionym zachowaniem Komisji.

62 Komisja kwestionuje te argumenty i podnosi zasadniczo, że żadna z przesłanek powstania odpowiedzialności pozaumownej nie została spełniona w niniejszej sprawie.

63 Przede wszystkim, jeśli chodzi o przesłankę dotyczącą bezprawności zarzucanego zachowania, należy zbadać, czy skarżący powołał się na naruszenie norm prawnych mających na celu przyznanie uprawnień jednostkom.

64 W tym względzie należy zauważyć, że art. 17 ust. 1 lit. c) rozporządzenia 2018/1725 ustanawia prawo dostępu osoby, której dane dotyczą, do informacji dotyczących odbiorców, którym jej dane osobowe zostały ujawnione, w szczególności odbiorców mających siedzibę w państwach trzecich. Przepis ten konkretyzuje zatem zasadę ustanowioną w art. 4 ust. 1 lit. a) rozporządzenia 2018/1725, zgodnie z którą wszelkie informacje i komunikaty dotyczące przetwarzania danych osobowych powinny być łatwo dostępne.

65 Ponadto art. 14 ust. 3 rozporządzenia 2018/1725 wyznacza administratorowi danych osobowych miesięczny termin na odpowiedź na wnioski o udzielenie informacji. Dodatkowo art. 14 ust. 4 tego rozporządzenia zobowiązuje administratora danych osobowych, w przypadku gdy zdecyduje się on nie uwzględnić wniosku, do poinformowania wnioskodawcy w terminie jednego miesiąca o powodach niepodjęcia działań, możliwości wniesienia skargi do Europejskiego Inspektora Ochrony Danych (EIOD) oraz możliwości skorzystania ze środka ochrony prawnej przed sądem. Przepisy te są zatem przepisami postępowania administracyjnego, które przyczyniają się do realizacji prawa dostępu do informacji o danych osobowych osoby, której dane dotyczą, poprzez jego konkretyzację i modulację. Co więcej, przepisy te przyczyniają się do konkretyzacji przyznanego każdej osobie na mocy art. 41 Karty prawa do rozpatrzenia jej sprawy w rozsądnym terminie przez instytucje i organy Unii.

66 W konsekwencji rozpatrywane łącznie przepisy art. 4 ust. 1 lit. a), art. 14 ust. 3 i 4 oraz art. 17 ust. 1 lit. c) rozporządzenia 2018/1725 stanowią normy prawne mające na celu przyznanie uprawnień jednostkom w rozumieniu orzecznictwa przywołanego w pkt 50 powyżej.

67 Następnie należy zbadać, czy naruszenie tych przepisów przez Komisję zostało wykazane w niniejszej sprawie.

68 Po pierwsze, skarżący utrzymuje, że Komisja naruszyła art. 17 ust. 1 lit. c) i art. 17 ust. 2 rozporządzenia 2018/1725, ponieważ oświadczenie o ochronie prywatności, które znajduje się na stronie internetowej KoPE, nie zawiera informacji o przekazywaniu danych osobowych odbiorcom mającym siedzibę w państwach trzecich, o ewentualnych odpowiednich zabezpieczeniach dotyczących wspomnianego przekazania lub o identyfikacji wykonawców jako odbiorców tych danych.

69 Jak wspomniano w pkt 64 powyżej, art. 17 ust. 1 lit. c) i art. 17 ust. 2 rozporządzenia 2018/1725 przewidują, że osoba, której dane dotyczą, ma w szczególności prawo do uzyskania informacji o odbiorcach mających siedzibę w państwach trzecich, którym dane osobowe zostały ujawnione, a także o odpowiednich zabezpieczeniach w odniesieniu do przekazywania danych tym odbiorcom.

70 Wynika z tego, że przepisy te ustanawiają prawo dostępu osoby, której dane dotyczą, do niektórych informacji, lecz nie przewidują, że informacje te muszą obowiązkowo znajdować się w danym dokumencie, a nawet w oświadczeniu o ochronie prywatności, takim jak oświadczenie znajdujące się na stronie internetowej KoPE. Innymi słowy, z przepisów tych nie wynika, że dane informacje powinny zostać ujawnione w drodze wspomnianego oświadczenia. Niemniej jednak skarżący, podobnie jak każda osoba, której dane dotyczą, zachowuje prawo do uzyskania takich informacji poprzez skorzystanie z prawa dostępu do informacji ustanowionego w art. 17 ust. 1 lit. c) i art. 17 ust. 2 rozporządzenia 2018/1725, która to kwestia wykracza poza zakres zarzucanej przez skarżącego Komisji niezgodności z prawem, która ogranicza się do treści oświadczenia o ochronie prywatności (zob. pkt 68 powyżej).

71 W każdym razie w niniejszej sprawie z brzmienia wspomnianego oświadczenia o ochronie prywatności, załączonego do skargi, wynika, że zawiera ono informacje dotyczące odbiorców lub kategorii odbiorców, którym dane osobowe zostały lub zostaną przekazane. I tak w pkt 7 wspomnianego oświadczenia wskazano w szczególności, że dostęp do danych osobowych „mają upoważnieni pracownicy [Komisji] i jej podwykonawcy, którzy odpowiadają za przeprowadzenie tej operacji przetwarzania danych zgodnie z zasadą ograniczonego dostępu”. Ponadto argument skarżącego, że wspomniane oświadczenie nie zawiera informacji o przekazywaniu danych osobowych odbiorcom mającym siedzibę w państwach trzecich, opiera się na założeniu, że przeglądanie strony internetowej KoPE wiąże się z przekazaniem danych osobowych użytkowników do państwa trzeciego. Jednakże niniejsze żądanie odszkodowawcze ma za podstawę naruszenie prawa dostępu do informacji, a nie naruszenie przepisów dotyczących przekazywania danych osobowych do państw trzecich, które zresztą stanowi podstawę drugiego żądania odszkodowawczego.

72 W związku z tym w niniejszej sprawie nie wykazano, że Komisja naruszyła art. 17 ust. 1 lit. c) i art. 17 ust. 2 rozporządzenia 2018/1725 w odniesieniu do oświadczenia o ochronie prywatności znajdującego się na stronie internetowej KoPE.

73 Po drugie, skarżący zarzuca Komisji, że ta nie odpowiedziała na wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r. w wyznaczonym terminie i że nie podała mu uzasadnienia swojej bezczynności z naruszeniem art. 14 ust. 3 i 4 oraz art. 17 ust. 1 i 2 rozporządzenia 2018/1725, a także zasady przejrzystości. Ponadto Komisja przekazała mu błędne informacje w wiadomości elektronicznej z dnia 3 grudnia 2021 r.

74 Na wstępie należy zauważyć, że skarżący nie przedstawia żadnego konkretnego argumentu na poparcie naruszenia zasady przejrzystości. Argument ten nie ma zatem autonomicznej treści w stosunku do zarzutu dotyczącego nieprzestrzegania terminu na odpowiedź na wniosek o udzielenie informacji i dotyczącego obowiązku podania powodów przekroczenia tego terminu.

75 Poza tym argumenty skarżącego dotyczące naruszenia art. 17 ust. 1 i 2 rozporządzenia 2018/1725, a także okoliczności, że Komisja przekazała mu błędne informacje w wiadomości elektronicznej z dnia 3 grudnia 2021 r., opierają się na założeniu, że przeglądanie strony internetowej KoPE wiąże się z przekazaniem danych osobowych użytkowników do państwa trzeciego. Tymczasem,

jak wskazano w pkt 71 powyżej, niniejsze żądanie odszkodowawcze oparte jest na naruszeniu prawa dostępu do informacji, a nie na naruszeniu przepisów dotyczących przekazywania danych osobowych do państw trzecich, które stanowi podstawę drugiego żądania odszkodowawczego.

76 W związku z tym w niniejszej sprawie nie wykazano, że Komisja naruszyła art. 17 ust. 1 i 2 rozporządzenia 2018/1725.

77 Co się tyczy zarzutu skarżącego dotyczącego naruszenia art. 14 ust. 3 i 4 rozporządzenia 2018/1725, z akt sprawy wynika, że Komisja odpowiedziała na wniosek o udzielenie informacji z dnia 9 listopada 2021 r. w terminie jednego miesiąca przewidzianym w art. 14 ust. 3 rozporządzenia 2018/1725 (zob. pkt 5 i 7 powyżej). Co się tyczy wniosku o udzielenie informacji z dnia 1 kwietnia 2022 r., Komisja poinformowała skarżącego e-mailem z dnia 30 czerwca 2022 r., że uważa, iż wniosek o udzielenie informacji z dnia 1 kwietnia 2022 r. jest prawie identyczny z wnioskiem o udzielenie informacji z dnia 9 listopada 2021 r. i że już odpowiedziała na ten wniosek wiadomością z dnia 3 grudnia 2021 r. (zob. pkt 11 powyżej).

78 Wynika stąd, że w odniesieniu do wniosku o udzielenie informacji z dnia 1 kwietnia 2022 r. Komisja nie dochowała miesięcznego terminu przewidzianego w art. 14 ust. 4 rozporządzenia 2018/1725 (zob. pkt 65 powyżej).

79 Z pkt 68–78 powyżej wynika, że jedyną zarzucaną Komisji w niniejszej sprawie bezprawnością jest niedochowanie terminu przewidzianego w art. 14 ust. 4 rozporządzenia 2018/1725.

80 W tych okolicznościach i niezależnie od kwestii, czy niedochowanie tego terminu przez Komisję stanowi wystarczająco istotne naruszenie normy prawnej, należy na wstępie zbadać, czy niedochowanie tego terminu spowodowało u skarżącego rzeczywistą i pewną krzywdę w rozumieniu orzecznictwa przypomnianego w pkt 54 powyżej.

81 W odniesieniu do rzeczywistego charakteru podnoszonej krzywdy należy przypomnieć, że o ile złożenie wniosku dowodowego niekoniecznie jest uważane za przesłankę uznania takiej krzywdy, o tyle na stronie skarżącej spoczywa przynajmniej obowiązek wykazania, że zachowanie zarzucane danej instytucji mogło wyrządzić jej taką krzywdę (wyrok z dnia 16 lipca 2009 r., SELEX Sistemi Integrati/Komisja, C-481/07 P, niepublikowany, EU:C:2009:461, pkt 38; zob. również wyrok z dnia 2 lipca 2019 r., Fulmen/Rada, T-405/15, EU:T:2019:469, pkt 188 i przytoczone tam orzecznictwo).

82 W niniejszej sprawie skarżący domaga się zadośćuczynienia za krzywdę w wysokości 800 EUR, twierdząc, że zachowanie zarzucane Komisji uniemożliwiło mu kontrolowanie przetwarzania jego danych osobowych.

83 Należy jednak stwierdzić, że taka krzywda nie została wykazana w niniejszej sprawie. Jedyną stwierdzoną w niniejszej sprawie bezprawnością jest bowiem nieprzestrzeganie przez Komisję terminu jednego miesiąca przewidzianego w art. 14 ust. 4 rozporządzenia 2018/1725 (zob. pkt 79 powyżej). Termin ten nie został jednak przekroczony o więcej niż dwa miesiące (zob. pkt 77 powyżej). Ponadto wnioski o udzielenie informacji z dni 9 listopada 2021 r. i 1 kwietnia 2022 r. były zasadniczo takie same (zob. pkt 5 i 8 powyżej), w związku z czym skarżący otrzymał już odpowiedź na co najmniej część swojego wniosku o udzielenie informacji w dniu 3 grudnia 2021 r., kiedy to Komisja odpowiedziała na wniosek o udzielenie informacji z dnia 9 listopada 2021 r. (zob. pkt 7 powyżej).

84 Ponadto argument skarżącego dotyczący przekazania błędnych informacji (zob. pkt 75 powyżej) dotyczy zasadności informacji, a nie przestrzegania przepisu proceduralnego, którego naruszenie zostało ustalone w pkt 78 powyżej, a zatem nie ma znaczenia dla wykazania podnoszonej krzywdy.

85 Wynika z tego, że nie wykazano, iż niedochowanie przez Komisję terminu przewidzianego w art. 14 ust. 4 rozporządzenia 2018/1725 mogło spowodować podnoszoną przez skarżącego krzywdę.

86 W konsekwencji, skoro jedna z kumulatywnych przesłanek powstania odpowiedzialności pozaumownej Unii przewidzianych w art. 340 akapit drugi TFUE nie została spełniona, pierwsze żądanie odszkodowawcze skarżącego należy oddalić.

W przedmiocie drugiego żądania odszkodowawczego, zmierzającego do uzyskania zadośćuczynienia za krzywdę wynikającą ze spornych przekazań danych

87 W drugim żądaniu odszkodowawczym skarżący żąda zapłaty 400 EUR tytułem zadośćuczynienia za krzywdę, jakiej miał doznać z powodu spornych przekazań danych, o których mowa w pkt 26–28 powyżej, a mianowicie spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r., spornego przekazania danych podczas połączenia z EU Login w dniu 30 marca 2022 r. oraz spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r.

88 Skarżący twierdzi w istocie, że sporne przekazania danych odbyły się na rzecz odbiorców mających siedzibę w Stanach Zjednoczonych, które to państwo nie ma odpowiedniego stopnia ochrony. Komisja nie wskazała żadnej z odpowiednich gwarancji, które mogłyby uzasadniać takie przekazywanie, przewidzianych w rozdziale V rozporządzenia 2018/1725, a zatem naruszyła art. 46, art. 48 ust. 1 i art. 48 ust. 2 lit. b) tego rozporządzenia oraz art. 7, 8 i 47 Karty. Sporne przekazania danych spowodowały ryzyko dostępu do danych skarżącego przez służby wywiadu i bezpieczeństwa tego państwa, a w konsekwencji wyrządziło mu krzywdę w rozumieniu motywu 46 rozporządzenia 2018/1725, ponieważ został on pozbawiony praw i wolności oraz nie mógł sprawować kontroli nad swoimi danymi.

89 Komisja kwestionuje te argumenty, podnosząc zasadniczo, że żadna z przesłanek powstania odpowiedzialności pozaumownej nie została spełniona w niniejszej sprawie.

– Uwagi wstępne w przedmiocie przepisów dotyczących przekazywania danych osobowych do państw trzecich

90 W pierwszej kolejności należy zauważyć, że zgodnie z brzmieniem art. 2 ust. 5 rozporządzenia 2018/1725, ma ono zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

91 W drugiej kolejności pojęcie „danych osobowych” należy interpretować w ten sposób, że oznacza ono wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zgodnie z art. 3 pkt 1 rozporządzenia 2018/1725.

92 W trzeciej kolejności należy zauważyć, że przekazanie danych stanowi operację „przetwarzania” danych w rozumieniu art. 3 pkt 3 rozporządzenia 2018/1725.

93 W czwartej kolejności należy zauważyć, że „przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych” jest uregulowane w rozdziale V rozporządzenia 2018/1725, który jednak go nie definiuje.

94 Jednakże z motywu 63 rozporządzenia 2018/1725 wynika, że przekazywanie danych, o którym mowa w rozdziale V tego rozporządzenia, dotyczy danych osobowych przekazywanych z instytucji i organów Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym.

95 Ponadto z wykładni systemowej rozporządzenia 2018/1725 wynika, że przekazywanie danych osobowych do państw trzecich w rozumieniu art. 46 wymaga: po pierwsze, aby administrator danych należał do instytucji lub organu Unii, a zatem by podlegał temu rozporządzeniu (art. 1 rozporządzenia 2018/1725); po drugie, by administrator udostępniał dane osobowe poprzez przekazanie lub w inny sposób odbiorcy, w szczególności innej osobie fizycznej lub prawnej (art. 3 pkt 3 i 13 rozporządzenia 2018/1725), a po trzecie, by odbiorca ten miał siedzibę w państwie trzecim (art. 46 rozporządzenia 2018/1725), czyli w państwie, które nie jest członkiem ani Unii, ani Europejskiego Obszaru Gospodarczego (EOG).

96 W piątej kolejności należy stwierdzić, że przepisy rozdziału V rozporządzenia 2018/1725 mają na celu zachowanie poziomu ochrony osób fizycznych, w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, jaki jest gwarantowany w Unii, zgodnie z celem określonym w motywie 63.

97 W szóstej kolejności art. 46 rozporządzenia 2018/1725 ustanawia ogólną zasadę, zgodnie z którą przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko wtedy, gdy – z zastrzeżeniem innych przepisów tego rozporządzenia – administrator i podmiot przetwarzający spełnią warunki określone w jego rozdziale V.

98 W siódmej kolejności, co się tyczy warunków określonych w rozdziale V rozporządzenia 2018/1725, należy zauważyć, że art. 47 ust. 1 tego rozporządzenia przewiduje, iż przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, jeżeli Komisja zadecyduje w drodze decyzji stwierdzającej odpowiedni stopień ochrony przyjętej w szczególności na podstawie art. 45 ust. 3 rozporządzenia 2016/679, że dane państwo lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, a przekazywanie danych osobowych odbywa się wyłącznie po to, aby umożliwić wykonywanie zadań wchodzących w zakres kompetencji administratora.

99 W tym względzie należy przypomnieć, że obie decyzje Komisji stwierdzające odpowiedni stopień ochrony dotyczące Stanów Zjednoczonych zostały uznane za nieważne. Po pierwsze na mocy wyroku z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650), Trybunał stwierdził nieważność decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r. zgodnie z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz.U. 2000, L 215, s. 7). Po drugie, na mocy wyroku Schrems II Trybunał stwierdził nieważność decyzji wykonawczej Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r., zgodnie z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz.U. 2016, L 207, s. 1).

100 Wynika z tego, że w dniu dokonania spornych przekazań danych w odniesieniu do Stanów Zjednoczonych nie istniała żadna decyzja stwierdzająca odpowiedni stopień ochrony w rozumieniu art. 47 rozporządzenia 2018/1725.

101 W braku decyzji Komisji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Stanów Zjednoczonych zastosowanie ma art. 48 ust. 1 rozporządzenia 2018/1725, zgodnie z którym przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko wtedy, gdy administrator lub podmiot przetwarzający przewidzieli odpowiednie zabezpieczenia i pod warunkiem, że osobom, których dane dotyczą, przysługują egzekwowalne prawa i skuteczne środki ochrony prawnej.

102 Odpowiednie zabezpieczenia, o których mowa w art. 48 ust. 1 rozporządzenia 2018/1725, wymienione w art. 48 ust. 2 i 3 tego rozporządzenia, mogą być zapewniane w szczególności za pomocą standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z art. 48 ust. 2 lit. b) tego rozporządzenia.

103 Jednakże standardowe klauzule ochrony danych przewidziane w art. 48 ust. 2 lit. b) rozporządzenia 2018/1725 mogą wymagać przyjęcia dodatkowych środków w celu zapewnienia przestrzegania odpowiedniego stopnia ochrony w świetle prawa Unii (zob. analogicznie wyrok Schrems II, pkt 133, 134).

104 Ponadto odpowiednie zabezpieczenia, o których mowa w art. 48 ust. 1 rozporządzenia 2018/1725, można zapewnić w szczególności za pomocą klauzul umownych, o których mowa w art. 48 ust. 3 lit. a) tego rozporządzenia, zawartych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim, pod warunkiem uzyskania zezwolenia EIOD.

105 Ponadto należy przypomnieć, że art. 7, 8 i 47 Karty ustanawiają, odpowiednio, prawo do poszanowania życia prywatnego, prawo do ochrony danych osobowych oraz prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu.

106 W niniejszej sprawie należy na wstępie zauważyć, że drugie żądanie odszkodowawcze skarżącego ma za podstawę naruszenie przez Komisję przepisów art. 46, art. 48 ust. 1 i art. 48 ust. 2 lit. b) rozporządzenia 2018/1725, a także art. 7, 8 i 47 Karty. Tymczasem z pkt 91–105 powyżej wynika, że wspomniane przepisy rozporządzenia 2018/1725 konkretyzują prawa podstawowe, takie jak ustanowione w art. 7 i 8 Karty, i mają w całości na celu zapewnienie ciągłości wysokiego poziomu ochrony danych osobowych w przypadku przekazywania tych danych do państw trzecich lub organizacji międzynarodowych.

107 Wynika z tego, że przepisy, na których naruszenie powołuje się skarżący na poparcie drugiego żądania odszkodowawczego, mają na celu ochronę indywidualnego interesu zainteresowanych osób, a zatem stanowią normy prawne mające na celu przyznanie uprawnień jednostkom w rozumieniu orzecznictwa przypomnianego w pkt 50 powyżej.

108 Należy obecnie zbadać, czy przesłanki powstania odpowiedzialności pozaumownej Komisji są spełnione w odniesieniu do każdego z trzech spornych przekazań, o których mowa w pkt 87 powyżej.

109 Zważywszy, że do spornych przekazań danych, o których mowa w pkt 26 i 28 powyżej, doszło ze względu na korzystanie przez stronę internetową KoPE z sieci dostarczania treści (w języku angielskim „content delivery network" lub „CDN") pod nazwą Amazon CloudFront (zwanej dalej „usługą Amazon CloudFront"), należy najpierw zbadać warunki funkcjonowania owej usługi w ramach tej strony internetowej.

– *W przedmiocie funkcjonowania usługi Amazon CloudFront w ramach strony internetowej KoPE*

110 W niniejszej sprawie bezsporne jest, że strona internetowa KoPE korzysta z sieci dostarczania treści Amazon CloudFront i że sieć ta jest uruchamiana przy każdym przeglądaniu wspomnianej strony internetowej przez użytkownika.

111 Z akt sprawy, a w szczególności z odpowiedzi stron na środek organizacji postępowania z dnia 21 lipca 2023 r. oraz ich wystąpień i odpowiedzi na rozprawie w dniu 17 października 2023 r. wynika, że w pierwszej kolejności usługa Amazon CloudFront jest usługą internetową, która przyspiesza dystrybucję treści internetowych użytkownikom, w niniejszym przypadku treści strony internetowej KoPE. Usługa Amazon CloudFront rozpowszechnia treść za pośrednictwem globalnej sieci serwerów lub centrów danych zwanych „punktami brzegowymi" lub „serwerami brzegowymi".

112 W drugiej kolejności usługa Amazon CloudFront opiera się na mechanizmie przekierowywania, który przekierowuje żądanie użytkownika strony internetowej KoPE do serwera brzegowego, który zapewnia najniższą latencję, zgodnie z zasadą bliskości względem terminalu użytkownika, w celu przekazania treści użytkownikowi w najlepszych możliwych warunkach. Jeżeli, w szczególności ze względu na trudności techniczne, serwer brzegowy o najniższej latencji nie jest dostępny, połączenie zostaje utworzone z serwerem o drugiej najniższej latencji i tak dalej.

113 W trzeciej kolejności usługa Amazon CloudFront jest wykorzystywana w odniesieniu do strony internetowej KoPE na podstawie umowy nr 2020-1742, podpisanej między Komisją a AWS EMEA, która jest spółką zależną spółki prawa amerykańskiego Amazon.com z siedzibą w Luksemburgu (zob. pkt 12 powyżej).

114 W czwartej kolejności w ramach tej umowy Komisja wybrała, jeśli chodzi o stronę internetową KoPE, obszar geograficzny zwany „Ameryką Północną (Stany Zjednoczone, Meksyk, Kanada), Europa i Izrael". Oznacza to, że dostarczanie treści tej strony internetowej nie odbywa się za pośrednictwem globalnej sieci punktów brzegowych Amazon CloudFront, lecz wyłącznie za pośrednictwem tych, które znajdują się na wyżej wymienionych obszarach geograficznych, a mianowicie w Stanach Zjednoczonych, Meksyku, Kanadzie, Europie i Izraelu.

115 W piątej kolejności, ze względu na zasadę bliskości, o której mowa w pkt 112 powyżej, żądania użytkowników z Unii o przeglądanie strony internetowej KoPE są zazwyczaj kierowane do serwerów brzegowych sieci Amazon CloudFront znajdujących się na tym terytorium, podczas gdy przypadki, w których żądania te są skierowane na serwery poza Unią, są rzadkie.

116 W szóstej kolejności, co się tyczy infrastruktury sieci punktów brzegowych Amazon CloudFront, z akt sprawy wynika, że jest ona dostarczana przez szereg przedsiębiorstw, z których niektóre należą do grupy Amazon, a inne są przedsiębiorstwami trzecimi, których wykaz można znaleźć na stronie internetowej Amazon Web Services w zależności od danego obszaru geograficznego. W odniesieniu do obszaru geograficznego o nazwie „Ameryka Północna (Stany Zjednoczone, Meksyk, Kanada), Europa i Izrael" przedsiębiorstwa te mają siedzibę zarówno w państwach

członkowskich Unii, jak i poza Unią, w szczególności w Stanach Zjednoczonych, Izraelu, Meksyku, Szwajcarii lub Zjednoczonym Królestwie. Każde przedsiębiorstwo obsługuje serwery w państwie, w którym ma siedzibę, a w konsekwencji lokalizacja geograficzna serwerów, które są zaangażowane w świadczenie usługi Amazon CloudFront, zależy również od lokalizacji zainteresowanych przedsiębiorstw.

117 W siódmej kolejności postanowienia umowy między Komisją a AWS EMEA przewidują w szczególności, co następuje:

– AWS EMEA musi być w stanie zagwarantować, że dane pozostaną w stanie spoczynku i w tranzycie na terytorium EOG (klauzula 11.2 umowy);

– AWS EMEA nie może zmienić lokalizacji przetwarzania danych bez uprzedniej zgody Komisji [klauzula 12.2.3(a) umowy];

– jakiekolwiek przekazanie danych osobowych na podstawie umowy do państw trzecich lub organizacji międzynarodowych musi być w pełni zgodne z wymogami określonymi w rozdziale V rozporządzenia 2018/1725 [klauzula 12.2.3(b) umowy];

– AWS EMEA nie może przekazywać żadnych danych osobowych do państwa spoza EOG, chyba że Komisja udzieliła uprzedniej pisemnej zgody na takie przekazanie i przekazanie odbywa się zgodnie z warunkami wspomnianego rozdziału V (klauzula 1.8.9 umowy);

– AWS EMEA przekazuje Komisji wszelkie wnioski o udzielenie dostępu do danych osobowych i musi skorzystać ze wszystkich dostępnych środków odwoławczych w odniesieniu do tych wniosków (klauzula 1.8.3, 1.8.4 i 1.8.5 umowy);

– AWS EMEA musi upewnić się, że środki te są również stosowane w przypadku korzystania z usług podwykonawców (klauzula 1.8.8 umowy).

118 W ósmej kolejności Komisja zasięgnęła opinii EIOD w przedmiocie wspomnianych wyżej postanowień umownych, ale nie uzyskano formalnego zezwolenia EIOD na podstawie art. 48 ust. 3 lit. a) rozporządzenia 2018/1725.

– Sporne przekazanie danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r.

119 [Sprostowany postanowieniem z dnia 3 czerwca 2025 r.] Skarżący twierdzi zasadniczo, że podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. stwierdził on, iż niektóre należące do niego dane osobowe, w szczególności jego adres IP oraz informacje o przeglądarce i terminalu, zostały przekazane do Stanów Zjednoczonych. Po pierwsze, wspomniana strona internetowa korzysta bowiem z sieci dostarczania treści zwanej „Amazon CloudFront”, której operatorem jest Amazon Web Services, amerykańska spółka zależna amerykańskiej spółki Amazon.com. Po drugie, podczas tego przeglądania dane osobowe skarżącego zostały wysłane do usługi Amazon CloudFront, a dokładniej do serwera Amazon.com z siedzibą w Seattle (Waszyngton, Stany Zjednoczone), którego adres IP to 18.66.192.74. Po trzecie, Amazon dostarczył klucza bezpieczeństwa używanego przez stronę internetową KoPE (zwanego dalej „certyfikatem SSL”), w związku z czym należy domniemywać, że miał on możliwość odkodowania wszystkich danych osobowych skarżącego przekazanych na jego serwery, w tym opinii skarżącego na temat przyszłości Europy. Po czwarte, przedsiębiorstwo, które świadczy usługę Amazon CloudFront,

podlega prawu amerykańskiemu, a zatem jest zobowiązane do przekazywania informacji służbom bezpieczeństwa i wywiadu w Stanach Zjednoczonych, i to nawet w przypadku, gdy serwery są zlokalizowane poza tym państwem. Ponadto Komisja nie przyjęła „dodatkowych środków" w rozumieniu wyroku Schrems II w celu zapewnienia odpowiedniego stopnia ochrony danych przekazywanych do Stanów Zjednoczonych.

120 Komisja nie zgadza się z tymi argumentami.

121 Co się tyczy przeglądania strony internetowej KoPE w dniu 30 marca 2022 r., z akt sprawy wynika, że skarżący przeglądał tę stronę internetową w tym dniu (zob. pkt 3 powyżej) i że podczas tego przeglądania doszło do przekazania jego adresu IP oraz informacji o przeglądarce i terminalu.

122 W tym względzie należy stwierdzić, że adres IP należy uznać za dane osobowe w rozumieniu art. 3 pkt 1 rozporządzenia 2018/1725, ponieważ spełnia on dwa warunki w nim przewidziane. Po pierwsze, informacja ta odnosi się do osoby fizycznej, a po drugie, odnosi się do osoby zidentyfikowanej lub możliwej do zidentyfikowania, w tym wypadku skarżącego (wyrok z dnia 26 kwietnia 2023 r., SRB/EIOD, T-557/20, odwołanie w toku, EU:T:2023:219, pkt 59; zob. także podobnie i analogicznie wyroki: z dnia 24 listopada 2011 r., Scarlet Extended, C-70/10, EU:C:2011:771, pkt 51; z dnia 19 października 2016 r., Breyer, C-582/14, EU:C:2016:779, pkt 49). Nawet bowiem adresy IP zwane „dynamicznymi", które z natury zmieniają się, odpowiadają dokładnej tożsamości w danym momencie, który w niniejszej sprawie zbiega się z chwilą, w której nastąpiło przeglądanie strony internetowej KoPE.

123 Wykazano również, że przekazanie danych, o którym mowa w pkt 121 powyżej, zostało zainicjowane przez stronę internetową KoPE za pośrednictwem usługi Amazon CloudFront na serwer o adresie IP 18.66.192.74.

124 Wykazano również, że w chwili zaistnienia okoliczności faktycznych adres IP 18.66.192.74 był przypisany serwerowi zlokalizowanemu w Monachium (Niemcy) i że serwer ten należał do przedsiębiorstwa A 100 ROW GmbH z siedzibą w Niemczech i znajdował się w wykazie przedsiębiorstw, o którym mowa w pkt 116 powyżej.

125 Wynika z tego, że prawdą jest, iż podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. doszło do przekazania danych osobowych skarżącego w rozumieniu art. 3 pkt 1 rozporządzenia 2018/1725, w szczególności jego adresu IP.

126 Jednakże w niniejszej sprawie nie wykazano, że podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. doszło do przekazania danych osobowych skarżącego do państwa trzeciego, a w szczególności do Stanów Zjednoczonych.

127 Natomiast z pkt 121–124 powyżej wynika, że podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. przekazanie danych osobowych skarżącego zostało zainicjowane przez stronę internetową KoPE za pośrednictwem usługi Amazon CloudFront na serwer znajdujący się w Monachium. Serwer ten należał do przedsiębiorstwa mającego siedzibę w Niemczech, które wchodziło w skład świadczeniodawców infrastruktury usługi Amazon CloudFront, która jest świadczona na rzecz Komisji na podstawie umowy z AWS EMEA, przedsiębiorstwem z siedzibą w Luksemburgu.

128 Wynika z tego, że podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. dane osobowe skarżącego zostały przekazane odbiorcy mającemu siedzibę w Unii.

129 Ponadto nawet przy założeniu, że dane osobowe skarżącego nie opuściły terytorium Unii, dane te zostały jednak przekazane do serwera należącego do sieci punktów brzegowych usługi Amazon CloudFront, która obejmuje, w odniesieniu do dostarczania treści strony internetowej KoPE, sieć punktów brzegowych, która nie ogranicza się do terytorium EOG, lecz wykracza poza to terytorium (zob. pkt 116 powyżej).

130 Jednakże konkretne okoliczności opisane w pkt 127 powyżej nie świadczą o tym, że doszło do przekazania danych osobowych odbiorcom mającym siedzibę poza terytorium EOG, w szczególności w Stanach Zjednoczonych.

131 Sporne przekazanie danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. nie odpowiada zatem przekazaniu danych osobowych do państwa trzeciego w rozumieniu art. 46 rozporządzenia 2018/1725, ponieważ koncepcja przekazywania danych do państwa trzeciego wymaga, aby dane osobowe były udostępniane odbiorcy mającemu siedzibę poza EOG (zob. pkt 93 powyżej).

132 Wniosku tego nie podważa argument skarżącego oparty na okoliczności, że AWS EMEA jest zobowiązana, jako spółka zależna przedsiębiorstwa amerykańskiego, do przekazania danych osobowych organom amerykańskim, nawet jeśli dane te są przechowywane na terytorium Unii.

133 O ile prawdą jest, że uzyskanie dostępu do danych osobowych przetwarzanych w EOG przez organy państwa trzeciego na podstawie przepisów tego państwa stanowi przekazanie danych osobowych do państwa trzeciego w rozumieniu art. 46 rozporządzenia 2018/1725, o tyle w niniejszej sprawie nie wykazano, że nastąpiło takie uzyskanie dostępu. Skarżący nie wykazał bowiem ani nie twierdził, że doszło do przekazania organom amerykańskim jakichkolwiek należących do niego danych osobowych, ani też nie wykazał, ani nie podniósł, że owe organy zwróciły się o uzyskanie danych, które zostały przekazane do serwera Amazon CloudFront znajdującego się w Monachium.

134 W związku z tym argument skarżącego nie dotyczy bezpośredniego naruszenia przepisów rozdziału V rozporządzenia 2018/1725, lecz wyłącznie ryzyka takiego naruszenia, w sytuacji gdy AWS EMEA ze względu na swój status spółki zależnej spółki amerykańskiej nie byłaby w stanie sprzeciwić się żądaniu władz amerykańskich dotyczącemu dostępu do danych przechowywanych na serwerach zlokalizowanych na terytorium EOG.

135 Tymczasem samo ryzyko dostępu państwa trzeciego do danych osobowych nie jest równoznaczne z przekazaniem danych w rozumieniu art. 46 rozporządzenia 2018/1725, zgodnie z jego wykładnią dokonaną w pkt 93 powyżej, ponieważ nie wykazano, że doszło do przekazania lub udostępnienia danych osobowych skarżącego odbiorcy mającemu siedzibę w państwie trzecim. Innymi słowy, ryzyka naruszenia wspomnianego art. 46 nie można utożsamiać z bezpośrednim naruszeniem tego przepisu.

136 Należy też przypomnieć, że w ramach niniejszego żądania odszkodowawczego badanie Sądu dotyczy weryfikacji przesłanek powstania odpowiedzialności pozaumownej Komisji, a w szczególności przesłanki dotyczącej bezprawności zachowania Komisji, która wymaga wykazania wystarczająco istotnego naruszenia przepisów rozporządzenia 2018/1725 i Karty, na które powołuje się skarżący.

137 W tym względzie samo ryzyko naruszenia przepisów rozdziału V rozporządzenia 2018/1725 nie może w żadnym razie wystarczyć do wykazania zawinionego zachowania Komisji odpowiadającego wystarczająco istotnemu naruszeniu tych przepisów.

138 Tego wniosku nie podważa argument skarżącego dotyczący wyroku Schrems II. Należy bowiem zauważyć, że w wyroku tym Trybunał wypowiedział się w przedmiocie niektórych warunków, na jakich może odbywać się przekazywanie danych osobowych do Stanów Zjednoczonych, a nie warunków, w jakich takie dane mogą być przetwarzane na terytorium EOG przez spółki zależne prawa amerykańskiego, takie jak AWS EMEA.

139 Z całości powyższych rozważań wynika, że w odniesieniu do spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. skarżący nie wykazał, że Komisja dopuściła się wystarczająco istotnego naruszenia, w rozumieniu orzecznictwa przypomnianego w pkt 50 powyżej, przepisów art. 46 i art. 48 ust. 1 i art. 48 ust. 2 lit. b) rozporządzenia 2018/1725, a także art. 7, 8 i 47 Karty.

140 W konsekwencji, ponieważ jedna z kumulatywnych przesłanek powstania odpowiedzialności pozaumownej Unii przewidzianych w art. 340 akapit drugi TFUE nie jest spełniona, należy oddalić drugie żądanie odszkodowawcze w odniesieniu do spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r., bez konieczności badania pozostałych argumentów skarżącego.

– *Sporne przekazanie danych podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r.*

141 Skarżący utrzymuje, że podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r. nastąpiło przekazanie jego danych osobowych, w szczególności jego adresu IP, na serwery Amazon CloudFront znajdujące się w Stanach Zjednoczonych. Zdaniem skarżącego przekazania te nie wynikają z jego działalności jako użytkownika strony internetowej, lecz są wynikiem funkcjonowania usługi Amazon CloudFront, w ramach której ryzyko przekazania danych do Stanów Zjednoczonych jest nieodłącznie związane z globalną infrastrukturą, na której opiera się ta usługa. Sytuacja skarżącego nie różni się od sytuacji obywatela Unii, który przegląda stronę internetową KoPE na przykład podczas podróży służbowej do Stanów Zjednoczonych. Komisja nie wykazała się wszelką starannością wymaganą do uniknięcia przekazywania danych do Stanów Zjednoczonych, ponieważ wybrała sieć dostarczania treści opartą na strukturze na poziomie światowym zamiast czysto europejskiego rozwiązania hostingowego.

142 Zdaniem skarżącego wspomniane przekazanie danych osobowych wyrządziło mu krzywdę w rozumieniu motywu 46 rozporządzenia 2018/1725, ponieważ utracił on kontrolę nad swoimi danymi, które zostały przekazane do Stanów Zjednoczonych i poddane niezgodnemu z prawem monitoringowi ze strony organów amerykańskich, oraz został pozbawiony swoich praw i wolności.

143 Komisja nie zgadza się z tymi argumentami.

144 Na wstępie i biorąc pod uwagę argumentację skarżącego, należy przypomnieć, że w ramach niniejszego żądania odszkodowawczego badanie Sądu nie dotyczy bezpośrednio zgodności z prawem decyzji Komisji o korzystaniu z usługi Amazon CloudFront do dostarczania treści

strony internetowej KoPE, lecz weryfikacji przesłanek powstania odpowiedzialności pozaumownej Komisji w odniesieniu do spornego przekazania danych podczas przeglądania strony internetowej w dniu 8 czerwca 2022 r.

145 W niniejszym przypadku Sąd uważa za właściwe zbadanie w pierwszej kolejności przesłanki dotyczącej istnienia związku przyczynowego między zarzucanym bezprawnym zachowaniem Komisji a podnoszoną krzywdą.

146 Z orzecznictwa przypomnianego w pkt 55 powyżej wynika, że przesłanka dotycząca związku przyczynowego wymaga istnienia wystarczająco bezpośredniego związku przyczynowego pomiędzy zachowaniem zarzucanym instytucji a szkodą, a udowodnienie tego związku należy do skarżącego w taki sposób, że zarzucane zachowanie powinno być decydującą przyczyną szkody.

147 Poza tym z orzecznictwa wynika, że związek przyczynowy wymagany dla powstania odpowiedzialności pozaumownej Unii na podstawie art. 340 akapit drugi TFUE istnieje wówczas, gdy szkoda jest bezpośrednim skutkiem rozpatrywanego działania sprzecznego z prawem (wyrok z dnia 28 czerwca 2007 r., Internationaler Hilfsfonds/Komisja, C-331/05 P, EU:C:2007:390, pkt 23).

148 Co się tyczy bezpośredniego charakteru związku przyczynowego, Sąd orzekł już, że szkoda powinna wynikać bezpośrednio z podnoszonej bezprawności, a nie z wyboru sposobu zareagowania przez skarżącego na rzekomo bezprawny akt. Uznano zatem, że sam fakt, iż bezprawne zachowanie stanowiło warunek konieczny (conditio sine qua non) wystąpienia szkody w tym znaczeniu, że szkoda nie wystąpiłaby bez zachowania bezprawnego, nie jest wystarczający do stwierdzenia istnienia wystarczająco bezpośredniego związku przyczynowego w rozumieniu orzecznictwa Unii (zob. podobnie i analogicznie wyroki: z dnia 30 listopada 2011 r., Transnational Company „Kazchrome" i ENRC Marketing/Rada i Komisja, T-107/08, EU:T:2011:704, pkt 80 i przytoczone tam orzecznictwo; z dnia 23 maja 2019 r., Remag Metallhandel i Jaschinsky/Komisja, T-631/16, niepublikowany, EU:T:2019:352, pkt 52 i przytoczone tam orzecznictwo).

149 Z orzecznictwa wynika zatem, że taki związek przyczynowy nie zostaje wykazany, gdy podnoszona szkoda jest bezpośrednim skutkiem własnej decyzji lub swobodnego wyboru skarżącego i w konsekwencji nie może zostać przypisana zainteresowanej instytucji lub danemu organowi (zob. podobnie i analogicznie wyroki: z dnia 28 czerwca 2007 r., Internationaler Hilfsfonds/Komisja, C-331/05 P, EU:C:2007:390, pkt 22–29; z dnia 17 lutego 2017 r., Novar/EUIPO, T-726/14, EU:T:2017:99, pkt 31, 32; z dnia 28 lutego 2018 r., Vakakis kai Synergates/Komisja, T-292/15, EU:T:2018:103, pkt 173 i przytoczone tam orzecznictwo).

150 W niniejszej sprawie należy zatem zbadać, czy zarzucane Komisji zachowanie, a mianowicie korzystanie z usługi Amazon CloudFront jako sieci dostarczania treści strony internetowej KoPE, jest bezpośrednią przyczyną podnoszonej krzywdy, polegającej na utracie kontroli nad danymi osobowymi skarżącego, które zostały przekazane do Stanów Zjednoczonych podczas przeglądania wspomnianej strony internetowej w dniu 8 czerwca 2022 r.

151 W tym względzie, po pierwsze, z akt sprawy oraz z odpowiedzi stron na pytania zadane na rozprawie wynika, że w dniu 8 czerwca 2022 r. skarżący znajdował się w Monachium i że wielokrotnie przeglądał stronę internetową KoPE. Podczas tego przeglądania adres IP skarżącego stworzył kolejne połączenia z różnymi serwerami usługi Amazon CloudFront, geograficznie bardzo oddalonymi od siebie. I tak połączył się o godzinie 7.13 z serwerem znajdującym się

w Monachium, o godzinie 11.13 z serwerem znajdującym się w Londynie (Zjednoczone Królestwo), o godzinie 12.56 z serwerem znajdującym się w Hillsboro (Oregon, Stany Zjednoczone), o godz. 13.05 z serwerem znajdującym się w Newark i o godz. 19.12 z serwerem znajdującym się we Frankfurcie nad Menem (Niemcy).

152 Po drugie, z akt sprawy wynika, że adres IP skarżącego został przekazany na różne serwery usługi Amazon CloudFront wymienione w pkt 151 powyżej, w tym serwery zlokalizowane w Stanach Zjednoczonych.

153 Po trzecie, należy przypomnieć, że adres IP skarżącego stanowi dane osobowe.

154 Po czwarte, należy zauważyć, że w dniu 8 czerwca 2022 r. strona internetowa KoPE zanotowała 4548 wyświetleń i 18 różnych adresów IP. Wśród nich jeden adres IP, a mianowicie adres skarżącego, stworzył połączenie z serwerami znajdującymi się poza Unią, a mianowicie w Stanach Zjednoczonych i w Zjednoczonym Królestwie. W tym względzie należy zauważyć, że nie wykazano ani nawet nie twierdzono, że w dniu 8 czerwca 2022 r. usługa Amazon CloudFront dla strony internetowej KoPE miała problemy techniczne lub innego rodzaju problemy, co uniemożliwiło normalne funkcjonowanie jej mechanizmu przekierowania według zasady bliskości, która kieruje żądania użytkowników strony internetowej KoPE do serwera brzegowego zapewniającego najmniejszą latencję w zależności od geograficznego położenia użytkownika (zob. pkt 112 powyżej).

155 Po piąte, jeśli chodzi o okoliczności związane z połączeniami utworzonymi przez adres IP skarżącego z serwerami znajdującymi się w Stanach Zjednoczonych, to z akt sprawy oraz z odpowiedzi udzielonych przez strony podczas rozprawy wynika, że skarżący utrzymuje, iż połączenia te były wynikiem funkcjonowania Amazon CloudFront, a nie jakiejkolwiek przeprowadzonej przez siebie manipulacji. Z kolei Komisja zauważa, że połączenia te były nietypowe i można je wytłumaczyć jedynie manipulacją techniczną ze strony skarżącego.

156 W tym względzie należy stwierdzić, że okoliczności opisane w pkt 151 powyżej świadczą o tym, iż różne lokalizacje serwerów, z którymi połączył się adres IP skarżącego, nie mogą wynikać z fizycznego przemieszczania się skarżącego w tym samym dniu, które byłoby niemożliwe ze względu na rozpatrywane odległości i odstępy czasu. Ponadto nie wykazano ani nawet nie podniesiono żadnego nieprawidłowego funkcjonowania usługi Amazon CloudFront, co pozwala stwierdzić, że w dniu 8 czerwca 2022 r. usługa ta funkcjonowała zgodnie z zasadą bliskości z terminalem użytkownika, ponieważ jej mechanizm przekierowania kierował żądania użytkowników strony internetowej KoPE do serwera brzegowego, który zapewniał najniższy czas latencji (zob. pkt 154 powyżej).

157 W tych okolicznościach połączenia adresu IP skarżącego z serwerami zlokalizowanymi w Stanach Zjednoczonych, podczas gdy on sam znajdował się w Niemczech, nie mogą wynikać z normalnego funkcjonowania usługi Amazon CloudFront, lecz raczej z korekty technicznej dokonanej przez skarżącego w celu zmiany jego widocznej lokalizacji poprzez przedstawienie się w dziedzinie cyfrowej, tak jakby znajdował się on w tym samym dniu w pobliżu Monachium, Londynu, Hillsboro, Newark i Frankfurtu nad Menem.

158 Wynika z tego, że działanie usługi Amazon CloudFront, wraz z jej mechanizmem przekierowania, która funkcjonuje w oparciu o zasadę bliskości i obejmuje obszar geograficzny szerszy niż terytorium EOG, wraz z między innymi Stanami Zjednoczonymi (zob. pkt 112, 114 powyżej), umożliwiło podczas przeglądania strony internetowej KoPE stworzenie połączenia przez adres IP skarżącego z serwerami Amazon CloudFront znajdującymi się w Stanach Zjednoczonych.

159 Jednakże, mimo że korzystanie przez Komisję z usługi Amazon CloudFront jest konieczną przesłanką przekazania danych osobowych do Stanów Zjednoczonych, o których mowa w pkt 152 powyżej, to w okolicznościach niniejszej sprawy nie jest ono wystarczające do wykazania dostatecznie bezpośredniego związku przyczynowego między krzywdą, którą miał ponieść skarżący, a bezprawnym w ocenie skarżącego zachowaniem Komisji, polegającym na korzystaniu z takiej usługi z naruszeniem przepisów rozdziału V rozporządzenia 2018/1725.

160 To właśnie zachowanie skarżącego, a nie zawinione działanie, jakiego w jego ocenie miała dopuścić się Komisja poprzez korzystanie z usługi Amazon CloudFront, należy bowiem uznać za bezpośrednią i natychmiastową przyczynę podnoszonej przez niego krzywdy.

161 Tak więc to skarżący stworzył warunki niezbędne do uruchomienia połączeń z serwerami znajdującymi się w Stanach Zjednoczonych poprzez działanie usługi Amazon CloudFront. To zachowanie skarżącego spowodowało, że mechanizm przekierowania usługi Amazon CloudFront przekierował jego żądania przeglądania strony internetowej KoPE na serwery zlokalizowane w Stanach Zjednoczonych, ponieważ serwery te miały najniższą latencję w stosunku do tego, co w sferze cyfrowej wydawało się być lokalizacją skarżącego, chociaż nie była to jego rzeczywista lokalizacja.

162 Ponadto skarżący nie powinien najpierw zachowywać się tak, aby wywołać określony rezultat (w postaci mianowicie przekazania swych danych osobowych do państwa trzeciego), a następnie żądać naprawienia krzywdy, twierdząc, że ta miała zostać spowodowana tym rezultatem, do której powstania bezpośrednio się przyczynił. Zatem wbrew temu, co twierdzi skarżący, w ramach skargi o odszkodowanie, takiej jak w niniejszej sprawie, jego sytuacji nie można oceniać w sposób podobny do sytuacji użytkownika, który rzeczywiście przemieścił się do Stanów Zjednoczonych i który w konsekwencji uzyskał dostęp do strony internetowej KoPE z tego państwa.

163 Z całości powyższych rozważań wynika, że odnośnie do spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r., nie wykazano wystarczająco bezpośredniego związku przyczynowego między zarzucanym bezprawnym zachowaniem Komisji a podnoszoną krzywdą.

164 W konsekwencji, ponieważ jedna z kumulatywnych przesłanek powstania odpowiedzialności pozaumownej Unii nie jest spełniona, należy oddalić żądanie odszkodowawcze w odniesieniu do spornego przekazania danych podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r., bez konieczności badania pozostałych przesłanek powstania tej odpowiedzialności.

– *Sporne przekazanie danych podczas połączenia z EU Login w dniu 30 marca 2022 r.*

165 Skarżący twierdzi, że w dniu 30 marca 2022 r., w chwili rejestracji do wzięcia udziału w wydarzeniu „GoGreen”, o którym informację zamieszczono na stronie internetowej KoPE, jego adres IP oraz informacje o przeglądarce i terminalu zostały przekazane spółce Meta Platforms z siedzibą w Stanach Zjednoczonych, która jest właścicielem serwisu społecznościowego

Facebook. Przy dokonywaniu tego wpisu skarżący został bowiem przekierowany do unijnej usługi uwierzytelniania EU Login, która proponuje między innymi połączenie za pośrednictwem kilku serwisów społecznościowych. Skarżący zdecydował się na połączenie za pośrednictwem swojego konta na Facebooku, a gdy kliknął na hiperłącze przekierowujące go do Facebooka, link ten doprowadził do przekazania jego adresu IP Facebookowi. Skarżący zaakceptował jedynie „podstawowe cookies" Facebooka. Inne dane osobowe skarżącego, a mianowicie jego adres e-mail, imię i nazwisko oraz zdjęcie profilowe, zostały zebrane przez Facebook za pomocą plików cookie, w szczególności pliku cookie zwanego „sb", i przekazane na serwery Meta Platforms. Zdaniem skarżącego z orzecznictwa wynika, że podmioty zarządzające stronami internetowymi, które korzystają z Facebooka na swoich stronach internetowych, jak Komisja, ponoszą wspólnie z Facebookiem odpowiedzialność za przestrzeganie prawa Unii dotyczącego ochrony danych. Komisja jest zatem współodpowiedzialna za umieszczanie plików cookie przechowywanych przez Facebook. Skarżący twierdzi, że utracił kontrolę nad swoimi danymi osobowymi przekazanymi Facebookowi i został pozbawiony swoich praw i wolności, co stanowi krzywdę w rozumieniu motywu 46 rozporządzenia 2018/1725.

166 Komisja nie zgadza się z tymi argumentami. Podnosi ona zasadniczo, że nie dokonała ani nie rozpoczęła transferu danych do Meta Platforms. Uważa ona, że rejestracja za pośrednictwem EU Login nie jest obowiązkowa, aby uczestniczyć w wydarzeniu „GoGreen", a nawet przy korzystaniu z EU Login skarżący miał różne opcje uwierzytelnienia, w tym opcje, które nie wymagają korzystania z konta w serwisach społecznościowych. Był to zatem wybór skarżącego, aby połączyć się z usługą EU Login za pośrednictwem konta na Facebooku a więc to on, a nie Komisja, uruchomił dostęp do strony internetowej Facebooka. Ponadto z technicznego punktu widzenia opcja uwierzytelnienia przez Facebook odbywa się za pomocą hiperłącza wyświetlanego na stronie internetowej EU Login, które nie zawiera danych osobowych użytkownika. Wbrew temu, co twierdzi skarżący, dane zebrane przez pliki cookies wykorzystywane przez Facebook nie są przekazywane Komisji podczas połączenia z EU Login i nie wchodzą w zakres jej odpowiedzialności. Te pliki cookie wynikają z wymiany informacji między Facebookiem a skarżącym na podstawie jego zgody, ponieważ Komisja nie uczestniczyła w tej wymianie. Ponadto Komisja utrzymuje, że orzecznictwo przywołane przez skarżącego nie ma zastosowania w niniejszej sprawie i że w każdym razie argument skarżącego dotyczący domniemanej wspólnej odpowiedzialności Komisji i Meta Platforms jest nowym zarzutem podniesionym po raz pierwszy na etapie repliki, który w konsekwencji jest niedopuszczalny.

167 W niniejszej sprawie należy najpierw zbadać okoliczności faktyczne, w które wpisuje się sporne przekazanie danych podczas połączenia z EU Login w dniu 30 marca 2022 r., biorąc pod uwagę informacje wynikające z akt sprawy, a także odpowiedzi stron na pytania zadane przez Sąd na rozprawie i w ramach środka organizacji postępowania z dnia 9 lutego 2024 r.

168 W tym względzie należy stwierdzić, że wydarzenie „GoGreen", zorganizowane przez organizację z siedzibą w Niderlandach, zostało ogłoszone na stronie internetowej KoPE. Zapisów na to wydarzenie można było dokonywać w szczególności na stronie internetowej KoPE za pośrednictwem usługi EU Login.

169 Skarżący postanowił zarejestrować się na stronie internetowej KoPE, korzystając z EU Login.

170 EU Login jest usługą uwierzytelniania użytkownika Komisji, która chroni kilkaset stron internetowych i aplikacji związanych z Unią. W niniejszej sprawie połączenie z EU Login w celu zarejestrowania się na wydarzenie „GoGreen” miało na celu zapewnienie, by rejestracja ta została dokonana za pomocą zweryfikowanego adresu poczty elektronicznej, ograniczając ryzyko związane z rejestracją fałszywych użytkowników lub z przywłaszczeniem tożsamości.

171 EU Login wyświetla na swojej stronie internetowej kilka opcji połączenia. Pierwszą opcją jest bezpośrednie połączenie się z EU Login albo poprzez wypełnienie danych o połączeniach dla istniejącego konta EU Login, albo poprzez utworzenie konta dla tej usługi. Drugą opcją jest stosowanie elektronicznego dowodu tożsamości „eID”, dostępnego dla obywateli niektórych państw członkowskich. Trzecia opcja, dostępna dla ograniczonej liczby usług, polega na korzystaniu z konta, które użytkownik posiada już na Facebooku, Twitterze lub Google'u, klikając na odpowiednie hiperłącze wyświetlane na stronie internetowej EU Login.

172 Możliwość połączenia się z EU Login za pośrednictwem konta na Facebooku wynika z faktu, że Komisja uznała, iż użytkownikom należy pozostawić decyzję o połączeniu się z EU Login za pośrednictwem wcześniej istniejących kont na platformach, aby zapewnić im łatwiejszy i szybki dostęp, a także możliwość uwierzytelnienia bez potrzeby tworzenia kont EU Login, a tym samym uniknięcia mnożenia liczby kont i podmiotów, którym użytkownicy muszą udostępniać swoje dane osobowe. Ponadto Komisja uznała, że Facebook był wiarygodny do celów weryfikacji adresów e-mail użytkowników, biorąc pod uwagę wprowadzone przez niego środki. Niemniej jednak hiperłącze pozwalające na połączenie się za pomocą istniejącego wcześniej konta na Facebooku jest dostępne na EU Login wyłącznie dla stron internetowych lub aplikacji wymagających jedynie podstawowego poziomu bezpieczeństwa.

173 Skarżący wybrał opcję połączenia się z EU Login za pośrednictwem swojego konta na Facebooku, korzystając z hiperłącza „Sign in with Facebook”, które wyświetla się na stronie internetowej EU Login (zwanego dalej „hiperłączem »zaloguj się przez Facebooka«”).

174 Hiperłącze „zaloguj się przez Facebooka” zawiera link do strony internetowej spoza Komisji. Po uruchomieniu tego hiperłącza, po kliknięciu na nie, udostępnia ono adres URL strony internetowej Facebooka, czyli indywidualny adres tej strony internetowej.

175 Dostęp do adresu URL strony internetowej Facebooka prowadzi do komunikacji między przeglądarką użytkownika a wspomnianą stroną internetową, w ramach której przeglądarka przekazuje adres IP użytkownika danej stronie internetowej. Przekazanie to jest podobne do przekazania, do którego dochodzi, gdy użytkownik wpisuje bezpośrednio adres URL dowolnej strony internetowej w przeglądarce, ponieważ każdy internauta pragnący uzyskać dostęp do strony internetowej musi koniecznie podać adres IP.

176 Za pośrednictwem hiperłącza „zaloguj się przez Facebooka” EU Login przesyła Facebookowi pewne informacje, które są niezbędne do procesu uwierzytelniania i przyjmują formę następującego przykładu:

https://www.facebook.com/v3.0/dialog/oauth?response_type=code&
client_id=1200572836629487&
redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthCallback&scope=email&
state=useFacebook%7CECAS_LR-5249395-
yQYIt4muQF7PyfSbvEk42Lt0Zm6AmYrUlJfVU5FfsrkYNTaFX552FQShXP9oggHF9jlEUohJx6I4ACrQJ0zPJ4-rS0vSrmBGYCzOpBivVtNak-
93Am7vhlDrqH4FT9cBOzViGrSdq4b2TrFkbOxzHB4zyingpuKF16KQfMnmu5izfXzUIIDHx1HqNS9QGEFVWzoeq0

177 W szczególności informacje zawarte w hiperłączu „zaloguj się przez Facebooka” są następujące:

– po pierwsze, część „client_id=1200572836629487” zawiera „niepowtarzalny kod identyfikacyjny”, który określa EU Login jako aplikację. Ten numer identyfikacyjny jest taki sam dla wszystkich użytkowników, którzy chcą uzyskać uwierzytelnienie w EU Login za pomocą Facebooka;

– po drugie, część „redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthCallback” zawiera ogólny adres URL EU Loginu, na który to adres Facebook musi odsyłać użytkownika po wyrażeniu przez niego zgody na przekazanie jego danych osobowych przez Facebook do EU Login;

– po trzecie, część „scope=email” zawiera dane, które Facebook musi przekazać EU Login w celu zapewnienia udanego uwierzytelnienia użytkownika, w szczególności adres e-mail użytkownika oraz imię i nazwisko wskazane na stronie Facebooka przy tworzeniu konta na Facebooku;

– po czwarte, część „state=useFacebook” wskazuje, że następujący po tym długi łańcuch znaków stanowi przypadkową wartość bezpieczeństwa, która jest wykorzystywana do zapobiegania atakom na bezpieczeństwo i ma ograniczony okres ważności. Ta przypadkowa wartość bezpieczeństwa jest generowana losowo przez EU Login i pełni funkcję tajnego zdania, które Facebook musi powtórzyć przy przekazywaniu danych do EU Login, aby umożliwić EU Login ustalenie, że podany adres e-mail, imię i nazwisko dotyczą użytkownika, który uruchomił metodę uwierzytelniania. Po upływie terminu lub po uwierzytelnieniu nie jest już możliwe stosowanie wartości bezpieczeństwa; oraz

– po piąte, część „response_type=code” wskazuje, że transmisji danych przez Facebook do EU Login towarzyszy jeszcze jeden kod. Ten niepowtarzalny kod obejmuje przypadkową wartość bezpieczeństwa, o której mowa powyżej. Niepowtarzalny kod jest równoznaczny z niepowtarzalnym numerem rejestracyjnym lub numerem seryjnym, który uwierzytelnia dane przesyłane przez Facebook do EU Login.

178 Użytkownik, po uzyskaniu dostępu do adresu URL Facebooka, znajduje się na tej stronie internetowej, na której najpierw wyświetla się okno, w którym prosi się go o zezwolenie na użycie plików cookies z Facebooka. Następnie, jeżeli użytkownik zezwoli na pliki cookies, otwiera się inne okno, umożliwiające wpisanie nazwy użytkownika i hasła konta użytkownika na Facebooku. Wreszcie po połączeniu ze swoim kontem na Facebooku użytkownik może zezwolić Facebookowi na korzystanie z plików cookies na innych aplikacjach i stronach internetowych, odpowiadając na pytanie „allow Facebook to use cookies and similar technologies placed on

other apps and websites?”. Jeżeli użytkownik wyrazi zgodę na takie korzystanie, zostanie następnie poproszony o wyrażenie zgody na to, by Facebook przekazał EU Login imię, nazwisko, zdjęcie profilowe i adres e-mail związany z jego kontem na Facebooku. Ponadto w trakcie całego tego procesu użytkownik może przerwać uwierzytelnianie za pomocą swojego konta na Facebooku, wybierając opcję „Cancel”. W takim przypadku zostaje on przekierowany do strony internetowej EU Login, gdzie ponownie wyświetla się strona z opcjami połączenia.

179 W niniejszej sprawie, gdy skarżący kliknął na hiperłącze „zaloguj się przez Facebooka”, jego przeglądarka internetowa znalazła się pod adresem URL strony internetowej Facebooka i w konsekwencji podała swój adres IP tej stronie internetowej. Następnie, gdy skarżący znajdował się na stronie internetowej Facebooka, wybrał opcje umożliwiające Facebookowi korzystanie wyłącznie z podstawowych plików cookies, później połączył się ze swoim kontem na Facebooku i wreszcie zezwolił Facebookowi na podanie EU Login swojego imienia, nazwiska, zdjęcia profilowego i adresu e-mail, które podał na swoim koncie na Facebooku.

180 W następstwie tych zezwoleń udzielonych przez skarżącego Facebook odesłał go do strony internetowej EU Login, zgodnie ze wskazówkami zawartymi w hiperłączu „zaloguj się przez Facebooka” (zob. pkt 177 tiret pierwsze i drugie powyżej).

181 Jednocześnie Facebook przekazał EU Login przypadkową wartość bezpieczeństwa i niepowtarzalny kod, o których mowa w pkt 177 tiret czwarte i piąte powyżej. To przekazanie informacji przez Facebook pozwoliło EU Login dowiedzieć się, że dane osobowe, które udostępnia mu Facebook, dotyczą użytkownika, który rozpoczął proces uwierzytelnienia, czyli w niniejszym przypadku skarżącego. Dodatkowo umożliwiło ono EU Login dostęp przez ograniczony czas do danych osobowych, o których mowa w pkt 177 tiret trzecie powyżej, a mianowicie w szczególności do imienia, nazwiska i adresu e-mail skarżącego, które ten podał na swoim koncie na Facebooku. Przekazanie tych danych przez Facebook do EU Login nastąpiło za pomocą zaszyfrowanego połączenia między nimi. To właśnie na podstawie danych udostępnionych przez Facebook EU Login uwierzytelniło adres e-mail skarżącego.

182 Ponadto należy zauważyć, że serwis społecznościowy Facebook należy do Meta Platforms, spółki z siedzibą w Stanach Zjednoczonych.

183 Trzeba dodać, że wyświetlanie tego hiperłącza na stronie internetowej EU Login regulują ogólne warunki serwisu Facebook, zamieszczone pod adresem internetowym „https://developers.facebook.com/terms”.

184 To w świetle tych właśnie rozważań należy zbadać, czy zostały spełnione przesłanki powstania odpowiedzialności pozaumownej Komisji.

185 Skarżący podnosi w istocie, że podczas połączenia z EU Login w dniu 30 marca 2022 r. nastąpiło przekazanie należących do niego danych osobowych, w szczególności jego adresu IP, na serwery serwisu społecznościowego Facebook, którego właścicielem jest spółka z siedzibą w Stanach Zjednoczonych. Przekazanie to nastąpiło z naruszeniem art. 46 rozporządzenia 2018/1725 i wyrządziło skarżącemu krzywdę polegającą na utracie kontroli nad jego danymi oraz pozbawieniu go praw i wolności.

186 Na wstępie należy przypomnieć, że jak wynika z pkt 95 powyżej, przekazywanie danych osobowych do państwa trzeciego w rozumieniu art. 46 rozporządzenia 2018/1725 wymaga, aby instytucja, jednostka organizacyjna lub organ Unii udostępniały dane osobowe poprzez transmisję lub w inny sposób do odbiorcy mającego siedzibę w państwie trzecim, czyli państwie niebędącym członkiem ani Unii, ani EOG.

187 W niniejszej sprawie wykazano, po pierwsze, że wśród opcji połączeń z EU Login skarżący zdecydował się na połączenie ze swoim kontem na Facebooku. Po drugie, hiperłącze „zaloguj się przez Facebooka" zawiera link do adresu URL strony internetowej Facebooka. Po trzecie, kiedy skarżący aktywował to hiperłącze, klikając na nie, jego przeglądarka uzyskała dostęp do adresu URL strony internetowej Facebooka, a następnie przekazała jego adres IP Facebookowi (zob. pkt 173–175 powyżej).

188 Wynika z tego, że Komisja za pomocą hiperłącza „zaloguj się przez Facebooka", wyświetlanego na stronie internetowej EU Login, stworzyła warunki umożliwiające przekazanie Facebookowi adresu IP skarżącego. Tymczasem ten adres IP stanowi dane osobowe skarżącego (zob. pkt 122 powyżej), które za pośrednictwem hiperłącza zostały przekazane Meta Platforms, przedsiębiorstwu z siedzibą w Stanach Zjednoczonych. Przekazanie to odpowiada zatem przekazaniu danych osobowych do państwa trzeciego w rozumieniu art. 46 rozporządzenia 2018/1725.

189 Ponadto w niniejszej sprawie wykazano, że w chwili tego przekazania danych, czyli w dniu 30 marca 2022 r., w odniesieniu do Stanów Zjednoczonych nie istniała żadna decyzja stwierdzająca odpowiedni stopień ochrony w rozumieniu art. 47 rozporządzenia 2018/1725 (zob. pkt 100 powyżej).

190 W braku decyzji Komisji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Stanów Zjednoczonych przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko wtedy, gdy administrator lub podmiot przetwarzający przewidzieli odpowiednie zabezpieczenia, i pod warunkiem że osobom, których dane dotyczą, przysługują egzekwowalne prawa i skuteczne środki ochrony prawnej, zgodnie z art. 48 ust. 1 rozporządzenia 2018/1725 (zob. pkt 101 powyżej).

191 W niniejszej sprawie Komisja nie wykazała ani nawet nie podniosła istnienia odpowiedniego zabezpieczenia, w szczególności standardowej klauzuli ochrony danych lub klauzuli umownej przyjętych na warunkach przewidzianych w art. 48 ust. 2 i 3 rozporządzenia 2018/1725 (zob. pkt 102–104 powyżej). Wykazano natomiast, że wyświetlanie hiperłącza „zaloguj się przez Facebooka" na stronie internetowej EU Login jest całkowicie regulowane ogólnymi warunkami serwisu Facebook (zob. pkt 183 powyżej).

192 W konsekwencji Komisja stworzyła warunki, w jakich doszło do przekazania danych osobowych skarżącego do państwa trzeciego, nie przestrzegając przy tym warunków określonych w art. 46 rozporządzenia 2018/1725.

193 Należy zatem stwierdzić, bez konieczności badania pozostałych argumentów skarżącego, że Komisja dopuściła się wystarczająco istotnego naruszenia – w rozumieniu orzecznictwa przypomnianego w pkt 50 powyżej – art. 46 rozporządzenia 2018/1725 w odniesieniu do spornego przekazania danych podczas połączenia z EU Login w dniu 30 marca 2022 r.

194 Należy zatem zbadać, czy w niniejszej sprawie zostały spełnione pozostałe przesłanki powstania odpowiedzialności pozaumownej Komisji, dotyczące szkody i związku przyczynowego.

195 Skarżący twierdzi, że niezgodne z prawem przekazanie jego adresu IP przedsiębiorstwu z siedzibą w Stanach Zjednoczonych wyrządziło mu krzywdę polegającą na utracie kontroli nad jego danymi oraz pozbawieniu go praw i wolności.

196 W tym względzie należy stwierdzić, że art. 65 rozporządzenia 2018/1725 przyznaje prawo do naprawienia nie tylko szkody majątkowej, ale również niemajątkowej doznanej w wyniku naruszenia tego rozporządzenia, bez konieczności wykazywania jakiegokolwiek progu wagi szkody [zob. podobnie i analogicznie wyrok z dnia 4 maja 2023 r., Österreichische Post (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), C-300/21, EU:C:2023:370, pkt 45, 51].

197 W niniejszej sprawie krzywdę, której naprawienia dochodzi skarżący, należy uznać za rzeczywistą i pewną w rozumieniu orzecznictwa przypomnianego w pkt 54 powyżej, ponieważ przekazanie, o którym mowa w pkt 188 powyżej, dokonane z naruszeniem art. 46 rozporządzenia 2018/1725, postawiło skarżącego w sytuacji niepewności co do przetwarzania jego danych osobowych, w szczególności adresu IP.

198 Ponadto istnieje wystarczająco bezpośredni związek przyczynowy w rozumieniu orzecznictwa przypomnianego w pkt 55 powyżej między naruszeniem przez Komisję art. 46 rozporządzenia 2018/1725 a krzywdą doznaną przez skarżącego.

199 W okolicznościach niniejszej sprawy kwotę zadośćuczynienia za krzywdę wyrządzoną przez Komisję należy oszacować ex æquo et bono na kwotę 400 EUR.

200 W związku z tym należy zasądzić od Komisji na rzecz skarżącego kwotę 400 EUR tytułem zadośćuczynienia za krzywdę doznaną w wyniku spornego przekazania danych podczas połączenia z EU Login w dniu 30 marca 2022 r.

W przedmiocie kosztów

201 Zgodnie z art. 134 § 3 regulaminu postępowania przed Sądem w razie częściowego tylko uwzględnienia żądań każdej ze stron Sąd może rozstrzygnąć, że każda ze stron pokrywa własne koszty. Jednakże, jeżeli jest to uzasadnione okolicznościami sprawy, Sąd może orzec, że jedna ze stron pokrywa, oprócz własnych kosztów, część kosztów poniesionych przez stronę przeciwną.

202 W niniejszym wypadku wysunięte przez skarżącego żądania pierwsze i drugie, a także część żądania trzeciego nie zostały uwzględnione. Jednakże żądanie trzecie zostało częściowo uwzględnione i zasądza się od Komisji odszkodowanie, którego domagał się skarżący tytułem zadośćuczynienia za krzywdę, jakiej doznał z powodu spornego przekazania danych podczas połączenia z EU Login w dniu 30 marca 2022 r. W tych okolicznościach należy orzec, że Komisja pokrywa własne koszty oraz połowę kosztów poniesionych przez skarżącego. Skarżący pokrywa połowę własnych kosztów.

Z powyższych względów

SĄD (szósta izba w składzie powiększonym)

orzeka, co następuje:

1) **Skarga zostaje odrzucona jako niedopuszczalna w zakresie dotyczącym żądań stwierdzenia nieważności.**

2) **Umarza się postępowanie w przedmiocie żądań mających na celu uzyskanie stwierdzenia, że Komisja Europejska niezgodnie z prawem powstrzymała się od zajęcia stanowiska w kwestii złożonego przez Thomasa Bindla w dniu 1 kwietnia 2022 r. wniosku o udzielenie informacji.**

3) **Komisja zostaje zobowiązana do zapłaty kwoty 400 EUR na rzecz T. Bindla tytułem zadośćuczynienia za doznaną krzywdę.**

4) **W pozostałym zakresie żądania odszkodowawcze zostają oddalone.**

5) **Komisja zostaje obciążona własnymi kosztami, a także połową kosztów poniesionych przez T. Bindla.**

6) **Thomas Bindl pokrywa połowę własnych kosztów postępowania.**

Costeira Kancheva Öberg

Zilgalvis Tichy-Fisslberger

Wyrok ogłoszono na posiedzeniu jawnym w Luksemburgu w dniu 8 stycznia 2025 r.

Podpisy

Spis treści

Okoliczności powstania sporu i fakty dotyczące okresu po wniesieniu skargi . . . 2

Żądania stron . . . 3

Co do prawa . . . 4

Uwagi wstępne na temat ochrony danych osobowych przez instytucje, organy i jednostki organizacyjne Unii . . . 4

W przedmiocie dopuszczalności . . . 5

Dopuszczalność skargi żądań stwierdzenia nieważności . . . 5

Dopuszczalność żądań stwierdzenia bezczynności . . . 7

W przedmiocie żądań odszkodowawczych . . . 8

Uwagi wstępne w przedmiocie przesłanek powstania pozaumownej odpowiedzialności Unii w ramach rozporządzenia 2018/1725 . . . 8

W przedmiocie pierwszego żądania odszkodowawczego, zmierzającego do uzyskania zadośćuczynienia za krzywdę wynikającą z naruszenia prawa dostępu do informacji . . . 10

W przedmiocie drugiego żądania odszkodowawczego, zmierzającego do uzyskania zadośćuczynienia za krzywdę wynikającą ze spornych przekazań danych . . . 14

– Uwagi wstępne w przedmiocie przepisów dotyczących przekazywania danych osobowych do państw trzecich . . . 14

– W przedmiocie funkcjonowania usługi Amazon CloudFront w ramach strony internetowej KoPE . . . 17

– Sporne przekazanie danych podczas przeglądania strony internetowej KoPE w dniu 30 marca 2022 r. . . . 18

– Sporne przekazanie danych podczas przeglądania strony internetowej KoPE w dniu 8 czerwca 2022 r. . . . 21

– Sporne przekazanie danych podczas połączenia z EU Login w dniu 30 marca 2022 r. . . 24

W przedmiocie kosztów . . . 30