Provisional text

JUDGMENT OF THE GENERAL COURT (Sixth Chamber, Extended Composition)

8 January 2025 (*)

(Processing of personal data – Protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies – Regulation (EU) 2018/1725 – Concept of 'transfer of personal data to a third country' – Transfer of data when visiting a website – EU Login – Action for annulment – Act not open to challenge – Inadmissibility – Action for failure to act – Position taken ending the inaction – No need to adjudicate – Action for damages – Sufficiently serious breach of a rule of law conferring rights on individuals – Causal link – Non-material damage)

In Case T-354/22,

Thomas Bindl, residing in Munich (Germany), represented by T. Herbrich, lawyer,

applicant,

v

European Commission, represented by A. Bouchagiar, B. Hofstötter and H. Kranenborg, acting as Agents,

defendant,

THE GENERAL COURT (Sixth Chamber, Extended Composition),

composed of M.J. Costeira (Rapporteur), President, M. Kancheva, U. Öberg, P. Zilgalvis and E. Tichy-Fisslberger, Judges,

Registrar: S. Jund, Administrator,

having regard to the written part of the procedure,

having regard to the measure of organisation of procedure of 21 July 2023 and the replies of the Commission and the applicant lodged at the Registry of the General Court on 7 and 8 September 2023, respectively,

further to the hearing on 17 October 2023,

having regard to the measure of organisation of procedure of 9 February 2024 and the replies of the Commission and the applicant lodged at the Court Registry on 12 and 13 March 2024, respectively,

gives the following

Judgment

1 By his action under Articles 263, 265 and 268 TFEU, the applicant, Mr Thomas Bindl, asks the Court to (i) annul transfers of his personal data to third countries that do not have an adequate level of protection; (ii) declare that the European Commission unlawfully failed to define its position on his request for information of 1 April 2022; and (iii) order compensation for the non-material damage which he claims to have sustained as a result of, first, an infringement of his right of access to information and, secondly, transfers of his personal data.

Background to the dispute and events subsequent to the bringing of the action

2 The applicant is a German citizen who takes an interest in matters pertaining to information technology (IT) and the protection of personal data.

3 The Commission's Directorate-General for Communication is the data controller for the purposes of the website of the Conference on the Future of Europe at 'https://futureu.europa.eu' ('the CFE website').

4 The applicant visited the CFE website on several occasions in 2021 and 2022. In particular he visited that website on

30 March 2022 and, using his Facebook account, registered for the ‘GoGreen’ event featured on it; on 8 June 2022, he visited the website again.

5 By email of 9 November 2021 (‘the information request of 9 November 2021’), the applicant requested that the Commission’s data protection officer provide him with information under Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ 2018 L 295, p. 39).

6 In that email, first, the applicant stated that he had noticed that when he logged in to the CFE website, a connection with third-party providers, such as the United States (US) undertaking Amazon Web Services, had been activated; secondly, he asked which personal data concerning him had been processed or stored and which, if any, had been transferred to third parties; thirdly, he asked for information about the legal basis for any such transfer and whether there were any guarantees in respect of transfers to third countries that do not have an adequate level of protection.

7 By email of 3 December 2021, the Commission’s Directorate-General for Communication sent the applicant an electronic link and informed him that that link would enable him to generate directly a list of the personal data which had been processed when he visited the CFE website. It also informed the applicant that his personal data had not been transferred to recipients outside the European Union and, moreover, that his personal data were stored and processed by the CFE website, which used a content delivery network managed by Amazon Web Services EMEA SARL (‘AWS EMEA’), established in Luxembourg (Luxembourg). Furthermore, it stated that, under the contractual arrangements concluded between the Commission and AWS EMEA, the data controller did not avail of services that would require data to be transferred to partners of AWS EMEA in the United States and that transfers of data outside the territory of the European Union were, in principle, not authorised.

8 By email of 1 April 2022, the applicant requested information from the Commission, pursuant to Regulation 2018/1725, about the processing of his data (‘the information request of 1 April 2022’). First, he stated that he had noticed that when he logged in to the CFE website, a connection with third-party providers such as AWS EMEA was established and that a connection to the company Microsoft had been established when he used his Facebook login details to register on the website. Secondly, he asked which personal data concerning him had been processed or stored and which, if any, had been transferred to third parties. Thirdly, he asked for information about the legal basis for any such transfer and whether there were any guarantees in respect of transfers to third countries that do not have an adequate level of protection. Fourthly, he requested a copy of his data, including data stored or processed by third parties such as Facebook.

9 By emails of 22 April and 2 May 2022, the applicant reiterated his request for a response from the Commission to the information request of 1 April 2022.

10 By application lodged at the Court Registry on 9 June 2022, the applicant brought the present action.

11 By email of 30 June 2022, the Commission informed the applicant that it considered the information request of 1 April 2022 to be virtually identical to the information request of 9 November 2021, and that it had already replied to the latter by its email of 3 December 2021.

12 Amazon Web Services is an undertaking established in the United States; AWS EMEA is an undertaking established in Luxembourg. Both undertakings are subsidiaries of Amazon.com, Inc., an undertaking governed by US law.

Forms of order sought

13 The applicant claims that the Court should:

– annul the transfers of his personal data to third countries that do not have an adequate level of protection, which took place on 30 March and 8 June 2022;

– declare that the Commission unlawfully failed to define its position on the information request of 1 April 2022;

– order the Commission to pay him EUR 1 200, together with interest, comprising (i) EUR 800 in compensation for non-material damage sustained as a result of an infringement of his right of access to information, and (ii) EUR 400 in compensation for non-material damage sustained as a result of those transfers of his data;

– order the Commission to pay the costs.

14 The Commission contends that the Court should:

– dismiss the claim for annulment and the claim for a declaration of failure to act as inadmissible;

– in the alternative, declare that there is no longer any need to adjudicate on the claim for a declaration of failure to act;

– dismiss the claim for damages as unfounded;

– order the applicant to pay the costs.

Law

Preliminary observations on the protection of personal data by the EU institutions, bodies, offices and agencies

15 Article 16(1) TFEU and Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') provide that everyone has the right to the protection of personal data concerning him or her.

16 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1) lays down general rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data (Article 1(1) of Regulation 2016/679).

17 Regulation 2018/1725 lays down rules relating to the protection of natural persons with regard to the processing of personal data by the EU institutions and bodies and rules relating to the free movement of personal data between them or to other recipients established in the European Union (Article 1(1) of Regulation 2018/1725). That regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data (Article 1(2) of Regulation 2018/1725). It applies to the processing of personal data by all EU institutions and bodies (Article 2(1) of Regulation 2018/1725).

18 Recital 5 of Regulation 2018/1725 recalls that, under the case-law of the Court of Justice, whenever the provisions of Regulation 2018/1725 follow the same principles as the provisions of Regulation 2016/679, those two sets of provisions must be interpreted homogeneously, in particular because the scheme of Regulation 2018/1725 should be understood as equivalent to that of Regulation 2016/679. In that regard, it is also apparent from Article 2(3) of Regulation 2016/679, read in conjunction with Article 99 of Regulation 2018/1725, that the latter regulation is to be adapted to the principles and rules of Regulation 2016/679.

Admissibility

Admissibility of the claim for annulment

19 By his first head of claim, the applicant seeks annulment of transfers of his personal data to third countries that do not have an adequate level of protection, transfers which, according to the applicant, took place on 30 March and 8 June 2022 ('the transfers at issue').

20 In its defence, the Commission submits that that application for annulment is inadmissible because it is not directed against a challengeable act, for the purpose of Article 263 TFEU, but seeks the grant of an injunction against the Commission.

21 The applicant maintains that the application for annulment is admissible, arguing that the transfers at issue are acts which have binding legal effects and which affect his legal position by undermining his fundamental right to the protection of personal data, guaranteed by Article 8 of the Charter. Any other interpretation would be incompatible with the fundamental right to effective judicial protection, a right that is expressly recognised by Article 64(1) of Regulation 2018/1725.

22 As recalled by Article 64(1) and recital 79 of Regulation 2018/1725, everyone has the right to an effective judicial remedy before the Court of Justice of the European Union, in accordance with the Treaties, if he or she considers that his or her rights under that regulation are infringed.

23 It follows that, under Regulation 2018/1725, every data subject has the right, inter alia, to bring an action for annulment under the conditions laid down in Article 263 TFEU.

24 According to settled case-law, an action for annulment as provided for in Article 263 TFEU must be available in respect of any act of the institutions, whatever its form, which is intended to have binding legal effects capable of affecting the interests of the applicant by bringing about a distinct change in his or her legal position (see judgments of 19 January 2017, *Commission* v *Total and Elf Aquitaine*, C-351/15 P, EU:C:2017:27, paragraphs 35 and 36 and the case-law cited, and of 16 July 2020, *Inclusion Alliance for Europe* v *Commission*, C-378/16 P, EU:C:2020:575, paragraph 71 and the case-law cited).

25 In order to determine whether an act produces binding legal effects, it is necessary, in accordance with the settled case-law of the Court of Justice, to examine the substance of that act and to assess its effects on the basis of objective criteria, such as the content of that act, taking into account, as appropriate, the context in which it was adopted and the powers of the EU institution, body, office or agency which adopted it (see judgment of 15 July 2021, *FBF*, C-911/19, EU:C:2021:599, paragraph 38 and the case-law cited).

26 In the present case, the applicant seeks annulment of the transfers at issue, which, according to him, took place on three occasions. In the first place, when he visited the CFE website on 30 March 2022 ('the disputed transfer at the time of the visit to the CFE website on 30 March 2022'), his personal data, including his IP address and information about his browser and terminal, were, he claims, transferred to the US undertaking Amazon Web Services in its capacity as operator of the content delivery network known as Amazon CloudFront, which was used by that website.

27 In the second place, when the applicant signed in to the Commission's user authentication service, EU Login, on 30 March 2022, using his Facebook account, in order to register for the 'GoGreen' event on the CFE website ('the disputed transfer on signing in to EU Login on 30 March 2022'), his personal data, including his IP address and information about his browser and terminal, were, he claims, transferred to the US undertaking Meta Platforms, Inc.

28 In the third place, when the applicant visited the CFE website on 8 June 2022 ('the disputed transfer at the time of the visits to the CFE website on 8 June 2022'), his personal data were, he claims, transferred to an Amazon CloudFront server in Newark (New Jersey, United States).

29 The applicant also mentions in his application that he accessed the CFE website on 9 November 2021 and that he registered on the CFE website on that date using his Facebook account. However, he does not rely on anything specific that would suggest that those circumstances are covered by his application for annulment of the transfers at issue. Only the transfers at issue referred to in paragraphs 26 to 28 above should therefore be taken into account.

30 It should be noted that the transfers at issue which the applicant seeks to have annulled, referred to in paragraphs 26 to 28 above, amount, according to the applicant himself, to data migration IT operations that were launched from the Commission's IT systems or services, in particular the CFE website, to servers belonging to third-party undertakings established outside the territory of the European Union.

31 It is true that the operation of having personal data transferred from an EU institution or body to a third country constitutes, in itself, processing of personal data within the meaning of point 3 of Article 3 of Regulation 2018/1725, carried out in the European Union, and falls within the scope of that regulation under Article 2(5) thereof (see, by analogy, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, 'judgment in *Schrems II*', EU:C:2020:559, paragraph 83).

32 However, not all operations that may result in a transfer of personal data, within the meaning of point 3 of Article 3 of Regulation 2018/1725, constitute challengeable acts for the purpose of Article 263 TFEU, as interpreted by the case-law recalled in paragraph 24 above.

33 In the present case, assuming that the transfers at issue are established, it must be noted that they are physical, not legal, acts. The transfers at issue, as described in the application, are IT operations migrating data from one terminal or server to another that result from interactions between the applicant and the Commission's IT systems or services on his visits to the CFE website or the EU Login service. However, the transfers at issue are not acts of the Commission that have binding legal effects, that is to say, they are not intended to regulate a legal situation and, as is apparent from their very nature, the Commission did not have any intention of conferring such effects on them.

34 Accordingly, the transfers at issue are not likely to have binding legal effects capable of affecting the interests of the applicant by bringing about a distinct change in his legal position, in accordance with the case-law recalled in paragraph 24 above. They cannot therefore be considered challengeable acts for the purpose of Article 263 TFEU.

35 It follows that the applicant's claim for annulment must be rejected as inadmissible.

Admissibility of the claim for a declaration of failure to act

36 By his second head of claim, the applicant asks the Court to declare that the Commission unlawfully failed to define its position on the information request of 1 April 2022.

37 In its defence, the Commission submits that that application for a declaration of failure to act is inadmissible because the Commission was not called upon to act, as provided for in the second paragraph of Article 265 TFEU. In the alternative, the Commission contends that there is no longer any need to adjudicate on the application for a declaration of failure to act, in view of its reply to the applicant by email of 30 June 2022.

38 The applicant maintains, in essence, that the Commission remains under an obligation to reply to the information request of 1 April 2022, given that the information which it provided in its email of 30 June 2022 is insufficient and inaccurate.

39 It has consistently been held that the remedy provided for in Article 265 TFEU is founded on the premiss that the unlawful inaction on the part of the institution concerned enables the matter to be brought before the Courts of the European Union in order for a declaration to be obtained that the failure to act is contrary to the Treaty, in so far as it has not been repaired by the institution concerned (judgment of 12 July 1988, *Parliament* v *Council*, 377/87, EU:C:1988:387, paragraph 9; see also judgment of 16 December 2015, *Sweden* v *Commission*, T-521/14, not published, EU:T:2015:976, paragraph 33 and the case-law cited).

40 In circumstances where the act whose absence constitutes the subject matter of the proceedings was adopted after the action was brought but before judgment, a declaration by the Court to the effect that the initial failure to act is unlawful can no longer bring about the consequences prescribed by Article 266 TFEU. It follows that in such a case the subject matter of the action has ceased to exist, and therefore there is no longer any need for the Court to give a decision (judgment of 12 July 1988, *Parliament* v *Council*, 377/87, EU:C:1988:387, paragraphs 10 and 11; see also order of 13 December 2000, *Sodima* v *Commission*, C-44/00 P, EU:C:2000:686, paragraph 83 and the case-law cited).

41 In the present case, it must be noted that the Commission replied to the information request of 1 April 2022 by its email of 30 June 2022 (see paragraph 11 above). The Commission therefore ended the failure to act alleged by the applicant in the context of the present action, after that action had been brought. The second head of claim, seeking a declaration under Article 265 TFEU that, in the absence of a reply to the information request of 1 April 2022, the Commission failed to act has therefore become devoid of purpose.

42 It is irrelevant in that regard that the content of the Commission's email of 30 June 2022 does not correspond to the reply which the applicant wished to receive. The fact that the position adopted by the institution has not satisfied the applicant is of no relevance in this respect because Article 265 TFEU refers to failure to act in the sense of failure to take a decision or to define a position, not the adoption of a measure different from that desired or considered necessary by the applicant (see order of 6 April 2017, *Brancheforeningen for Regulerkraft i Danmark* v *Commission*, T-203/16, not published, EU:T:2017:279, paragraph 22 and the case-law cited).

43 It follows that there is no longer any need to adjudicate on the applicant's claim for a declaration of failure to act, nor any need to rule on the Commission's contention that that claim is inadmissible.

Claim for damages

44 By his third head of claim, the applicant puts forward two applications for damages. In the first place, he seeks payment of EUR 800 in compensation for the non-material damage which he claims to have sustained because of the Commission's failure to respect his right of access to information, contrary to Article 14(3) and (4) and Article 17(1) and (2) of Regulation 2018/1725 and to the principle of transparency laid down in Article 4(1)(a) of that regulation. In the second place, he seeks payment of EUR 400 in compensation for the non-material damage which he claims to have sustained as a result of the transfers at issue, which were contrary to Article 46 and Article 48(1) and (2)(b) of Regulation 2018/1725.

45 The Commission contends that the claim for damages should be dismissed.

Preliminary observations on the conditions for establishing the European Union's non-contractual liability in the context of Regulation 2018/1725

46 Article 65 of Regulation 2018/1725 provides that any person who has suffered material or non-material damage as a result of an infringement of that regulation is to have the right to receive compensation from the EU institution or body for the damage suffered, subject to the 'conditions provided for in the Treaties'.

47 Article 65 of Regulation 2018/1725 must be interpreted as providing that the right to receive compensation from an EU institution or body for the damage suffered as a result of an infringement of that regulation is subject to the conditions in the second paragraph of Article 340 TFEU, under which the European Union is, in accordance with the general principles common to the laws of the Member States, to make good any damage caused by its institutions or by its servants in the performance of their duties.

48 According to settled case-law, the European Union may incur non-contractual liability if three cumulative conditions are satisfied: the unlawfulness of the conduct alleged against the institutions, the fact of damage and the existence of a causal link between that conduct and the damage complained of (see, to that effect, judgments of 4 July 2000, *Bergaderm and Goupil* v *Commission*, C-352/98 P, EU:C:2000:361, paragraphs 39 to 42, and of 28 October 2021, *Vialto Consulting* v *Commission*, C-650/19 P, EU:C:2021:879, paragraph 138).

49 The cumulative nature of those conditions means that if any one of them is not satisfied, the action for damages must be dismissed in its entirety, and there is no need to examine the other conditions (judgment of 9 September 1999, *Lucaccioni* v *Commission*, C-257/98 P, EU:C:1999:402, paragraphs 14 and 63; see also judgment of 25 February 2021, *Dalli* v *Commission*, C-615/19 P, EU:C:2021:133, paragraph 42 and the case-law cited).

50 As regards the first of those conditions, according to the case-law there must be a sufficiently serious breach of a rule of law that is intended to confer rights on individuals (see judgment of 4 July 2000, *Bergaderm and Goupil* v *Commission*, C-352/98 P, EU:C:2000:361, paragraph 42 and the case-law cited).

51 That requirement of a sufficiently serious breach of EU law is intended, whatever the nature of the unlawful act at issue, to avoid the risk of having to bear the losses claimed by the persons concerned obstructing the ability of the institution concerned to exercise to the full its powers in the general interest, whether that be in its legislative activity or in that involving choices of economic policy or in the sphere of its administrative competence, without however thereby leaving individuals to bear the consequences of flagrant and inexcusable conduct (see, to that effect, judgment of 14 December 2018, *East West Consulting* v *Commission*, T-298/16, EU:T:2018:967, paragraph 124 and the case-law cited).

52 The decisive test for finding that a breach is sufficiently serious is whether the EU institution or body concerned manifestly and gravely disregarded the limits on its discretion. Where that institution or body has only considerably reduced, or even no, discretion, the mere infringement of EU law may be sufficient to establish the existence of a sufficiently serious breach (see judgment of 10 December 2002, *Commission* v *Camar and Tico*, C-312/00 P, EU:C:2002:736, paragraph 54 and the case-law cited). However, that case-law does not establish an automatic link between lack of discretion of the institution concerned, on the one hand, and classification of a sufficiently serious breach of EU law on the other (judgment of 3 March 2010, *Artegodan* v *Commission*, T-429/05, EU:T:2010:60, paragraph 59). The extent of the discretion enjoyed by the institution concerned, although determinative, is not the only yardstick. On this point, the Court of Justice has many times recalled that the system of rules it has developed with regard to the second paragraph of Article 340 TFEU also takes into account, in particular, the complexity of the situations to be regulated and the difficulties in applying or interpreting the legislation (see judgment of 23 November 2011, *Sison* v *Council*, T-341/07, EU:T:2011:687, paragraphs 36 and 37 and the case-law cited) or, more generally, the field, the circumstances and the context in which the rule that was infringed was imposed on the EU institution or body concerned (see judgment of 4 April 2017, *Ombudsman* v *Staelen*, C-337/15 P, EU:C:2017:256, paragraph 40 and the case-law cited).

53 It follows that only the finding that an irregularity would not have been committed in similar circumstances by an administrative authority exercising ordinary care and diligence enables the liability of the European Union to be established. It is therefore for the EU judicature, after determining whether the institution concerned had a margin of discretion, to take account of the complexity of the situation to be regulated, the difficulties in the application or interpretation of the legislation, the clarity and precision of the rule infringed, and whether the error of law made was inexcusable or intentional (judgment of 3 March 2010, *Artegodan* v *Commission*, T-429/05, EU:T:2010:60, paragraph 62).

54 As regards the condition relating to the fact of damage, that damage must be actual and certain, which it is for the applicant to prove (see judgment of 9 November 2006, *Agraz and Others* v *Commission*, C-243/05 P, EU:C:2006:708, paragraph 27 and the case-law cited). By contrast, purely hypothetical and indeterminate damage does not give rise to compensation (see judgment of 26 October 2011, *Dufour* v *ECB*, T-436/09, EU:T:2011:634, paragraph 192 and the case-law cited).

55 As regards the condition relating to a causal link, this concerns a sufficiently direct causal nexus between the conduct of the institution complained of and the damage, the burden of proof of which rests on the applicant, so that the conduct complained of must be the determining cause of the damage (see judgment of 13 December 2018, *European Union* v *ASPLA and Armando Álvarez*, C-174/17 P and C-222/17 P, EU:C:2018:1015, paragraph 23 and the case-law cited).

56 Furthermore, it should be recalled that the action for damages under the second paragraph of Article 340 TFEU was introduced as an autonomous form of action, with a particular purpose to fulfil within the system of actions and subject to conditions on its use dictated by its specific purpose, and hence a declaration of inadmissibility of the application for annulment does not automatically render the action for damages inadmissible (see judgment of 5 September 2019, *European Union* v *Guardian Europe* and *Guardian Europe* v *European Union*, C-447/17 P and C-479/17 P, EU:C:2019:672, paragraph 49 and the case-law cited).

57 It follows that the dismissal of the application for annulment on account of its inadmissibility and the dismissal of the application for a declaration of failure to act because there is no longer any need to adjudicate on it, in accordance with paragraphs 35 and 43 above, do not mean that, as a result, the claims for damages referred to in paragraph 44 above must be dismissed as inadmissible.

58 The complaints raised by the applicant in connection with his claims for damages must be examined in the light of those considerations.

The first claim for damages, seeking compensation for non-material damage resulting from infringement of the right of access to information

59 By his first claim for damages, the applicant asks the Court to order the Commission to pay him EUR 800 in compensation for the non-material damage sustained as a result of the infringement of his right of access to information.

60 First of all, the applicant complains that the Commission did not reply to the information request of 1 April 2022 within the prescribed period and failed to communicate to him the reasons for its inaction, contrary to Article 14(3) and (4) and Article 17(1) and (2) of Regulation 2018/1725 and to the principle of transparency laid down in Article 4(1)(a) of that regulation. He also claims that the Commission failed to respect Article 17(1)(c) and (2) of Regulation 2018/1725, in so far as the privacy statement on the CFE website does not include information concerning the transfer of personal data to third countries or any appropriate safeguards for the purposes of such transfer, as required by Article 48 of that regulation. Furthermore, the Commission provided incorrect information in the email of 3 December 2021, in so far as it denied that there had been any transfer of the applicant's personal data to recipients in the United States.

61 Next, the applicant maintains that the Commission's wrongful inaction prevented him from controlling the processing of his personal data, which constitutes non-material damage within the meaning of recital 46 of Regulation 2018/1725. Lastly, he claims that that non-material damage, which he assesses at EUR 800, was directly caused by the Commission's misconduct.

62 The Commission disputes those arguments, contending, in essence, that none of the conditions for establishing non-contractual liability is satisfied in this case.

63 First of all, as regards the condition relating to the unlawfulness of the conduct complained of, it is necessary to ascertain whether the applicant has invoked the infringement of rules of law intended to confer rights on individuals.

64 In that regard, it should be observed that Article 17(1)(c) of Regulation 2018/1725 establishes that a data subject has a right of access to information concerning the recipients to whom his or her personal data have been disclosed, in particular recipients in third countries. That provision thus gives concrete expression to the principle, laid down in Article 4(1)(a) of Regulation 2018/1725, that any information and communication relating to the processing of personal data must be easily accessible.

65 Article 14(3) of Regulation 2018/1725, moreover, sets a time limit of one month for the data controller to reply to requests for information. In addition, Article 14(4) of that regulation requires the data controller, if he or she should decide not to take action on the request, to inform the person making the request, within one month, of the reasons for not taking action and of the possibility of lodging a complaint with the European Data Protection Supervisor (EDPS) and seeking a judicial remedy. Those provisions are therefore rules of administrative procedure that serve to implement the right of access to information concerning the data subject's personal data, by giving concrete expression to, and adapting, that right. Furthermore, those provisions serve to give concrete expression to the right of every person, under Article 41 of the Charter, to have his or her affairs handled within a reasonable time by the institutions and bodies of the European Union.

66 Consequently, Article 4(1)(a), Article 14(3) and (4), and Article 17(1)(c) of Regulation 2018/1725, read together, constitute rules of law intended to confer rights on individuals, within the meaning of the case-law referred to in paragraph 50 above.

67 Next, it is appropriate to consider whether an infringement of those provisions on the part of the Commission has been established in this case.

68 First, the applicant maintains that the Commission infringed Article 17(1)(c) and (2) of Regulation 2018/1725, in so far as the privacy statement that appears on the CFE website does not include information on the transfer of personal data to recipients in third countries, on any appropriate safeguards relating to that transfer or on the identification of contractors as recipients of the data.

69 As stated in paragraph 64 above, Article 17(1)(c) and (2) of Regulation 2018/1725 provides that a data subject has, inter alia, a right to receive information concerning the recipients in third countries to whom his or her personal data have been disclosed and the appropriate safeguards in respect of transfers of data to those recipients.

70 It follows that those provisions establish that the data subject has a right of access to certain information, but do not require that that information must necessarily appear in a given document or in a privacy statement, such as that which appears on the CFE website. In other words, it does not follow from those provisions that the information in question must be disclosed by means of that statement. However, the applicant, like every data subject, retains the right to receive such information by exercising his right of access to information as laid down in Article 17(1)(c) and (2) of Regulation 2018/1725, an issue that is outside the scope of the unlawfulness of which the applicant accuses the Commission, this being limited to the content of the privacy statement (see paragraph 68 above).

71 In any event, in the present case, it is apparent from the wording of that privacy statement, annexed to the application, that it contains information concerning the recipients or categories of recipient to whom the personal data have been or will be disclosed. Thus, it is stated, in particular, in point 7 of that statement that access to the data is 'provided to the authorised personnel of the [Commission] and its contractors responsible for carrying out this processing operation according to the "need to know" principle'. In addition, the applicant's argument that that statement does not contain information about the transfer of personal data to recipients in third countries is based on the assumption that visiting the CFE website involves a transfer of users' personal data to a third country. However, the present claim for damages is based on infringement of the right of access to information, not on infringement of provisions concerning the transfer of personal data to third countries, which, moreover, forms the basis of the second claim for damages.

72 Accordingly, it has not been demonstrated in this case that the Commission infringed Article 17(1)(c) and (2) of Regulation 2018/1725, with regard to the privacy statement on the CFE website.

73 Secondly, the applicant complains that the Commission did not reply to the information request of 1 April 2022 within the prescribed period and failed to provide him with reasons for its inaction, contrary to Article 14(3) and (4) and Article 17(1) and (2) of Regulation 2018/1725 and to the principle of transparency. He also claims that the Commission provided him with incorrect information in the email of 3 December 2021.

74 It should be observed at the outset that the applicant does not put forward any specific argument to support his claim of a breach of the principle of transparency. That argument is not, therefore, independent of the complaint relating to the failure to observe the time limit for replying to the request for information and the obligation to provide reasons for exceeding that time limit.

75 In addition, the applicant's arguments in relation to an infringement of Article 17(1) and (2) of Regulation 2018/1725 and to the fact that the Commission provided him with incorrect information in its email of 3 December 2021 are based on the assumption that visiting the CFE website involves a transfer of users' personal data to a third country. However, as stated in paragraph 71 above, the present claim for damages is based on infringement of the right of access to information, not on infringement of provisions concerning the transfer of personal data to third countries, which forms the basis of the second claim for damages.

76 Accordingly, it has not been demonstrated in the present case that the Commission infringed Article 17(1) and (2) of Regulation 2018/1725.

77 With regard to the applicant's complaint of infringement of Article 14(3) and (4) of Regulation 2018/1725, it is apparent from the case file that the Commission replied to the information request of 9 November 2021 within the period of one month prescribed in Article 14(3) of Regulation 2018/1725 (see paragraphs 5 and 7 above). With regard to the information request of 1 April 2022, the Commission informed the applicant, by email of 30 June 2022, that it considered the information request of 1 April 2022 to be virtually identical to the information request of 9 November 2021 and that it had already replied to the latter by its email of 3 December 2021 (see paragraph 11 above).

78 It follows that, so far as the information request of 1 April 2022 is concerned, the Commission did not observe the one-month time limit prescribed in Article 14(4) of Regulation 2018/1725 (see paragraph 65 above).

79 It is apparent from paragraphs 68 to 78 above that the only unlawful conduct on the part of the Commission that has been established in this case is the failure to observe the time limit prescribed in Article 14(4) of Regulation 2018/1725.

80 Accordingly, irrespective of whether the Commission's failure to observe that time limit constitutes a sufficiently serious breach of a rule of law, it is necessary to examine first of all whether the failure to observe that time limit caused the applicant actual and certain non-material damage, within the meaning of the case-law recalled in paragraph 54 above.

81 As regards the actual non-material damage allegedly suffered, it should be recalled that, while offering evidence is not necessarily held to be a condition for the recognition of non-material damage, it is for the applicant at least to establish that the conduct alleged against the institution concerned was capable of causing him such damage (judgment of 16 July 2009, *SELEX Sistemi Integrati* v *Commission*, C-481/07 P, not published, EU:C:2009:461, paragraph 38; see also judgment of 2 July 2019, *Fulmen* v *Council*, T-405/15, EU:T:2019:469, paragraph 188 and the case-law cited).

82 In the present case, the applicant seeks compensation for non-material damage in the amount of EUR 800, claiming that the Commission's conduct prevented him from controlling the processing of his personal data.

83 However, it must be held that no such non-material damage has been demonstrated in this case. The only unlawful conduct established in this case is that of the Commission's failure to observe the one-month time limit prescribed in Article 14(4) of Regulation 2018/1725 (see paragraph 79 above). As it is, that time limit was not exceeded by more than two months (see paragraph 77 above). Furthermore, the information requests of 9 November 2021 and 1 April 2022 were fundamentally the

same (see paragraphs 5 and 8 above), so that the applicant had already received a reply to at least part of his information request on 3 December 2021, when the Commission replied to the information request of 9 November 2021 (see paragraph 7 above).

84 Moreover, the applicant's argument concerning the provision of incorrect information (see paragraph 75 above) concerns the substance of the information rather than compliance with the procedural rule that was infringed, as has been established in paragraph 78 above, and is not, therefore, relevant for the purpose of demonstrating the non-material damage invoked.

85 It follows that it has not been demonstrated that the Commission's failure to observe the time limit prescribed in Article 14(4) of Regulation 2018/1725 was such as to cause the applicant the non-material damage alleged.

86 Consequently, since one of the cumulative conditions for establishing the European Union's non-contractual liability laid down in the second paragraph of Article 340 TFEU is not satisfied, the applicant's first claim for damages must be dismissed.

The second claim for damages, seeking compensation for non-material damage resulting from the transfers at issue

87 By his second claim for damages, the applicant seeks payment of EUR 400 in compensation for the non-material damage he claims to have sustained because of the transfers at issue referred to in paragraphs 26 to 28 above, that is to say, the disputed transfer at the time of the visit to the CFE website on 30 March 2022, the disputed transfer on signing in to EU Login on 30 March 2022 and the disputed transfer at the time of the visits to the CFE website on 8 June 2022.

88 The applicant claims, in essence, that the transfers at issue were made to recipients established in the United States, a country which does not have an adequate level of protection. The Commission did not indicate any of the appropriate safeguards that might justify those transfers, as provided for in Chapter V of Regulation 2018/1725, and thus infringed Article 46 and Article 48(1) and (2)(b) of that regulation, as well as Articles 7, 8 and 47 of the Charter. The applicant claims that the transfers at issue gave rise to a risk of his data being accessed by the US security and intelligence services and, consequently, caused him non-material damage within the meaning of recital 46 of Regulation 2018/1725, in that he was deprived of his rights and freedoms and prevented from exercising control over his data.

89 The Commission disputes those arguments, contending, in essence, that the conditions for establishing non-contractual liability are not satisfied in this case.

– *Preliminary observations on the provisions relating to the transfer of personal data to a third country*

90 In the first place, it should be noted that, under Article 2(5), Regulation 2018/1725 applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

91 In the second place, the concept of 'personal data' should be interpreted as any information relating to an identified or identifiable natural person, in accordance with point 1 of Article 3 of Regulation 2018/1725.

92 In the third place, it should be observed that the transfer of data constitutes a data 'processing' operation within the meaning of point 3 of Article 3 of Regulation 2018/1725.

93 In the fourth place, it must be observed that 'transfers of personal data to third countries or international organisations' are governed by Chapter V of Regulation 2018/1725, which nevertheless does not define them.

94 However, it is apparent from recital 63 of Regulation 2018/1725 that the transfers covered by Chapter V of that regulation concern personal data transferred from the EU institutions and bodies to controllers, processors or other recipients in third countries or to international organisations.

95 It follows, moreover, from a systematic interpretation of Regulation 2018/1725 that the transfer of personal data to third countries, within the meaning of Article 46 thereof, requires (i) that the data controller concerned belong to an EU institution or body and that he or she is therefore subject to that regulation (Article 1 of Regulation 2018/1725); (ii) that the controller make the personal data available, by transmission or otherwise, to a recipient, including to another natural or legal person (points 3 and 13 of Article 3 of Regulation 2018/1725); and (iii) that that recipient be established in a third country (Article 46 of Regulation 2018/1725), that is to say, a country which is a member of neither the European Union nor the European Economic Area (EEA).

96 In the fifth place, it should be noted that the provisions of Chapter V of Regulation 2018/1725 are intended to guarantee the level of protection of natural persons ensured in the European Union when personal data are transferred to third countries or to international organisations, in accordance with the objective set out in recital 63 thereof.

97 In the sixth place, Article 46 of Regulation 2018/1725 lays down a general principle that any transfer of personal data to a third country or to an international organisation is to take place only if, subject to the other provisions of that regulation, the conditions laid down in Chapter V thereof are complied with by the controller and processor.

98 In the seventh place, as regards the conditions laid down in Chapter V of Regulation 2018/1725, it should be observed that Article 47(1) of that regulation provides that a transfer of personal data to a third country or international organisation may take place where the Commission has decided, by means of an adequacy decision adopted, in particular, pursuant to Article 45(3) of Regulation 2016/679, that the country or the international organisation in question ensures an adequate level of protection and where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out.

99 In that regard, it should be noted that both of the Commission's adequacy decisions concerning the United States have been declared invalid. First, by the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650), the Court of Justice declared invalid Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p.7). Secondly, by the judgment in *Schrems II*, the Court of Justice declared invalid Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016 L 207, p. 1).

100 It follows that, at the time of the transfers at issue, no adequacy decision, within the meaning of Article 47 of Regulation 2018/1725, existed with regard to the United States.

101 In the absence of an adequacy decision of the Commission with regard to the United States, Article 48(1) of Regulation 2018/1725, according to which personal data may be transferred to a third country or to an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, is applicable.

102 The appropriate safeguards referred to in Article 48(1) of Regulation 2018/1725, listed in Article 48(2) and (3) of that regulation, may be provided for, inter alia, by standard data protection clauses adopted by the Commission, in accordance with Article 48(2)(b) of that regulation.

103 However, the standard data protection clauses provided for in Article 48(2)(b) of Regulation 2018/1725 may require the adoption of supplementary measures in order to ensure compliance with the appropriate level of protection, under EU law (see, by analogy, judgment in *Schrems II*, paragraphs 133 and 134).

104 The appropriate safeguards referred to in Article 48(1) of Regulation 2018/1725 may also be provided for, in particular, by contractual clauses, as envisaged in Article 48(3)(a) of that regulation, that have been agreed between the controller or processor, on the one hand, and the controller, processor or the recipient of the personal data in the third country, on the other, subject to authorisation from the EDPS.

105 It should, moreover, be recalled that Articles 7, 8 and 47 of the Charter establish, respectively, the right to respect for private life, the right to protection of personal data and the right to an effective remedy and to a fair trial.

106 In the present case, it must be observed at the outset that the applicant's second claim for damages is based on infringement, by the Commission, of Article 46 and Article 48(1) and (2)(b) of Regulation 2018/1725, as well as of Articles 7, 8 and 47 of the Charter. It is apparent from paragraphs 91 to 105 above that those provisions of Regulation 2018/1725 give concrete expression to fundamental rights, such as those established in Articles 7 and 8 of the Charter, and seek as a whole to ensure that the high level of protection of personal data continues where those data are transferred to third countries or international organisations.

107 It follows that the provisions which the applicant claims, in support of his second claim for damages, have been infringed are intended to protect the individual interest of data subjects and thus constitute rules of law intended to confer rights on individuals, within the meaning of the case-law recalled in paragraph 50 above.

108 It is necessary then to ascertain whether the conditions for establishing the Commission's non-contractual liability are satisfied in respect of each of the three disputed transfers referred to in paragraph 87 above.

109 Given that the disputed transfers referred to in paragraphs 26 and 28 above took place because of the use, by the CFE website, of the content delivery network (CDN) called Amazon CloudFront ('the Amazon CloudFront service'), it is appropriate first of all to examine the conditions for the operation of that service in the context of that website.

– *The operation of the Amazon CloudFront service in the context of the CFE website*

110 In the present case, it is common ground that the CFE website uses the Amazon CloudFront content delivery network and that that network is activated whenever a user visits that website.

111 It is apparent from the case file, in particular from the parties' replies to the measure of organisation of procedure of 21 July 2023 and their submissions and replies at the hearing on 17 October 2023, that, in the first place, the Amazon CloudFront service is an internet service that accelerates the distribution of internet content – in this instance, CFE website content – to users. The Amazon CloudFront service disseminates content through a worldwide network of servers or data centres called 'edge locations' or 'edge servers'.

112 In the second place, the Amazon CloudFront service is based on a routing mechanism that directs the CFE website user's request to the edge server that provides the lowest latency, according to a principle of proximity to the user's terminal, so that content is delivered to the user in the best possible conditions. If, because of technical difficulties in particular, the edge server with the lowest latency is not available, a connection is established with the edge server that provides the second lowest latency, and so on.

113 In the third place, the use of the Amazon CloudFront service for the purposes of the CFE website is based on contract No 2020-1742, signed by the Commission and AWS EMEA, a subsidiary of the US company Amazon.com whose registered office is in Luxembourg (see paragraph 12 above).

114 In the fourth place, in the context of that contract, the Commission opted, as regards the CFE website, for the geographic area 'North America (United States, Mexico, Canada), Europe and Israel'. That means that content from that website is distributed not through Amazon CloudFront's worldwide network of edge locations, but only through those that are in the above mentioned geographic areas, that is, in the United States, in Mexico, in Canada, in Europe and in Israel.

115 In the fifth place, because of the principle of proximity referred to in paragraph 112 above, requests by EU users to visit the CFE website are normally directed to the edge servers of the Amazon CloudFront network in the territory of the European Union, and only rarely directed to servers outside that territory.

116 In the sixth place, as regards the infrastructure of Amazon CloudFront's edge locations network, it is apparent from the case file that this is provided by a number of undertakings, some of which belong to the Amazon group while others are third companies, the list of which can be viewed on Amazon Web Services' website, according to the geographic area concerned. In the case of the geographic area 'North America (United States, Mexico, Canada), Europe and Israel', the relevant undertakings are established in the EU Member States as well as outside the European Union, in particular in the United States, Israel, Mexico, Switzerland or the United Kingdom. Each undertaking uses servers in the country in which it is established and, consequently, the geographic location of the servers involved in the delivery of the Amazon CloudFront service also depends on the location of the undertakings concerned.

117 In the seventh place, the clauses of the contract between the Commission and AWS EMEA provide, inter alia, as follows:

– AWS EMEA must be able to ensure that its data remains at rest and in transit in the territory of the EEA (clause 11.2 of the contract);

– AWS EMEA may not change the location of data processing without the prior written authorisation of the Commission (clause 12.2.3(a) of the contract);

– any transfer of personal data under the contract to third countries or international organisations must fully comply with the requirements laid down in Chapter V of Regulation 2018/1725 (clause 12.2.3(b) of the contract);

– AWS EMEA may not transfer any personal data to a country outside the EEA, unless the Commission has given its prior written authorisation to such transfer and the transfer takes place in compliance with the conditions of Chapter V (clause 1.8.9 of the contract);

– AWS EMEA must notify the Commission of any request for access to personal data and must use all available legal remedies to appeal those requests (clauses 1.8.3, 1.8.4 and 1.8.5 of the contract);

– AWS EMEA must ensure that those measures are also applied when sub-processors are used (clause 1.8.8 of the contract).

118 In the eighth place, the Commission consulted the EDPS on the contractual clauses referred to above, but they were not formally authorised by the EDPS under Article 48(3)(a) of Regulation 2018/1725.

– *Disputed transfer at the time of the visit to the CFE website on 30 March 2022*

119 The applicant submits, in essence, that while visiting the CFE website on 30 March 2022, he noted that some of his personal data, in particular his IP address and information about his browser and terminal, had been transferred to the United States. First, that website uses a content delivery network called 'Amazon CloudFront', operated by Amazon Web Services, a US subsidiary of the US company Amazon.com. Secondly, in the course of that visit, the applicant's personal data were sent to the Amazon CloudFront service, more specifically to Amazon.com's server in Seattle (Washington, United States), the IP address of which is 18.66.192.74. Thirdly, the security key used by the CFE website ('SSL certificate') was provided by Amazon, which is why it may be assumed that Amazon had the opportunity to decrypt all of the applicant's personal data that were transferred to its servers, including his opinions on the future of Europe. Fourthly, the undertaking which provides the Amazon CloudFront service is governed by US law and is therefore obliged to disclose information to the US security and surveillance services, even if the servers are located outside the United States. Furthermore, the Commission had not adopted 'supplementary measures', within the meaning of the judgment in *Schrems II*, in order to guarantee an adequate level of protection of data transferred to the United States.

120 The Commission contests those arguments.

121 So far as concerns the visit to the CFE website on 30 March 2022, it is evident from the case file that the applicant visited the website on that date (see paragraph 3 above) and that, during that visit, a transmission of his IP address and of information about his browser and terminal took place.

122 In that regard, it must be noted that the IP address must be classified as personal data, within the meaning of point 1 of Article 3 of Regulation 2018/1725, since it satisfies both of the conditions laid down in that provision. First, that information relates to a natural person and, secondly, it relates to a person who is identified or identifiable, in this case, the applicant (judgment of 26 April 2023, *SRB* v *EDPS*, T-557/20, under appeal, EU:T:2023:219, paragraph 59; see also, to that effect and by analogy, judgments of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 51, and of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 49). Even 'dynamic' IP addresses – which by nature change over time – correspond to a precise identity at a given point in time, which, in this case, coincides with the point in time at which the visit to the CFE website took place.

123 It has also been demonstrated that the transfer of data referred to in paragraph 121 above was initiated by the CFE website, via the Amazon CloudFront service, to a server the IP address of which is 18.66.192.74.

124 It has further been demonstrated that, at the material time, the IP address 18.66.192.74 was assigned to a server located in Munich (Germany), and that that server belonged to A 100 ROW GmbH, an undertaking established in Germany that was included on the list of undertakings referred to in paragraph 116 above.

125 It follows that, during the visit to the CFE website on 30 March 2022, there was indeed a transfer of the applicant's personal data within the meaning of point 1 of Article 3 of Regulation 2018/1725, including of his IP address.

126 However, it has not been demonstrated in this instance that, during the visit to the CFE website on 30 March 2022, there was a transfer of the applicant's personal data to a third country and, in particular, to the United States.

127 By contrast, it is apparent from paragraphs 121 to 124 above that, during the visit to the CFE website on 30 March 2022, the transfer of the applicant's personal data was initiated by the CFE website, via the Amazon CloudFront service, to a server located in Munich. That server belonged to an undertaking established in Germany, which was part of the network of providers of the Amazon CloudFront service infrastructure, which is provided to the Commission under a contract with AWS EMEA, an undertaking established in Luxembourg.

128 It follows that, during the visit to the CFE website on 30 March 2022, the applicant's personal data were sent to a recipient established in the European Union.

129 In addition, even if it is accepted that the applicant's personal data did not leave EU territory, the data were nevertheless transferred to a server belonging to the network of edge locations of the Amazon CloudFront service, which covers, so far as the distribution of CFE website content is concerned, a network of edge locations that is not confined to the territory of the EEA but extends beyond it (see paragraph 116 above).

130 However, the specific circumstances described in paragraph 127 above do not demonstrate that personal data were transferred to recipients established outside the territory of the EEA, in particular to the United States.

131 The disputed transfer at the time of the visit to the CFE website on 30 March 2022 does not, therefore, amount to a transfer of personal data to a third country, within the meaning of Article 46 of Regulation 2018/1725, given that the concept of transfer to a third country requires that personal data be made available to a recipient established outside the EEA (see paragraph 93 above).

132 The applicant's argument that, as a subsidiary of a US undertaking, AWS EMEA is obliged to transmit personal data to the US authorities, even if the data are stored on EU territory, does not call that finding into question.

133 While it is indeed the case that access by the authorities of a third country, under the legislation of that country, to personal data processed in the EEA constitutes a transfer of personal data to a third country, within the meaning of Article 46 of Regulation 2018/1725, the fact remains that it has not been established that any such access took place in this instance. The applicant has neither demonstrated nor claimed that any of his personal data were transmitted to the US authorities, nor has he demonstrated or claimed that a request was made by those authorities in respect of the data that were transferred to that Amazon CloudFront server in Munich.

134 Accordingly, the applicant's argument does not relate to a direct infringement of the provisions of Chapter V of Regulation 2018/1725, but only to the risk of such an infringement, should AWS EMEA, because of its status as a subsidiary of a US undertaking, be unable to object to a request from the US authorities concerning access to data stored in servers located within the EEA.

135 As it is, the mere risk of access to personal data by a third country cannot amount to a transfer of data, within the meaning of Article 46 of Regulation 2018/1725, as interpreted in paragraph 93 above, since it has not been demonstrated that the applicant's personal data were transmitted or otherwise made available to a recipient established in a third country. In other words, the risk of an infringement of Article 46 cannot be treated as being akin to a direct infringement of that provision.

136 Furthermore, it should be recalled that, in the context of the present claim for damages, the Court's examination involves verifying the conditions for establishing the Commission's non-contractual liability, and in particular the condition relating to unlawful conduct on the part of the Commission, which requires that a sufficiently serious breach of the provisions of Regulation 2018/1725 and of the Charter relied on by the applicant be established.

137 In that regard, the mere risk of an infringement of the provisions of Chapter V of Regulation 2018/1725 cannot in any event be sufficient to establish misconduct on the part of the Commission amounting to a sufficiently serious breach of those provisions.

138 That conclusion is not called into question by the applicant's argument relating to the judgment in *Schrems II*. It should be observed that, in that judgment, the Court ruled on some of the conditions under which transfers of personal data to the United States may take place, and not on those under which such data may be processed within the EEA by subsidiaries of US companies, such as AWS EMEA.

139 It follows from all of the above that, in the case of the disputed transfer at the time of the visit to the CFE website on 30 March 2022, the applicant has not demonstrated that the Commission committed a sufficiently serious breach, within the meaning of the case-law recalled in paragraph 50 above, of Article 46 and Article 48(1) and (2)(b) of Regulation 2018/1725 or of Articles 7, 8 and 47 of the Charter.

140 Consequently, since one of the cumulative conditions for establishing the European Union's non-contractual liability provided for in the second paragraph of Article 340 TFEU is not satisfied, the Court must dismiss the second claim for damages with regard to the disputed transfer at the time of the visit to the CFE website on 30 March 2022, and there is no need to examine the applicant's other arguments.

– *Disputed transfer at the time of the visits to the CFE website on 8 June 2022*

141 The applicant claims that, while visiting the CFE website on 8 June 2022, his personal data, including his IP address, were transferred to Amazon CloudFront servers in the United States. According to the applicant, those transfers do not arise from his activity as a user of the website, but are the result of the operation of the Amazon CloudFront service, in the context of which the risk of data being transferred to the United States is inherent in the worldwide infrastructure underpinning that service. The applicant's situation is no different from that of an EU citizen who visits the CFE website while, for example, on a business trip to the United States. The Commission did not exercise all due care and attention in ensuring that data were not transferred to the United States, in so far as it opted for a content delivery network based on a worldwide structure, instead of a purely European hosting solution.

142 According to the applicant, that transfer of personal data caused him non-material damage within the meaning of recital 46 of Regulation 2018/1725, in so far as he lost control of his data, which were transferred to the United States and were liable to be monitored unlawfully by the US authorities, and in so far as he was deprived of his rights and freedoms.

143 The Commission contests those arguments.

144 As a preliminary point and in the light of the applicant's arguments, it should be recalled that, in the context of the present claim for damages, the Court is not directly examining the lawfulness of the Commission's decision to use the Amazon

CloudFront service for the distribution of CFE website content; rather, it is verifying the conditions for establishing the Commission's non-contractual liability with regard to the disputed transfer at the time of the visits to the CFE website on 8 June 2022.

145 In the present case, the Court considers it appropriate to deal first of all with the condition relating to the existence of a causal link between the Commission's alleged misconduct and the non-material damage invoked.

146 It is apparent from the case-law recalled in paragraph 55 above that the condition relating to the causal link concerns the existence of a sufficiently direct causal nexus between the conduct of the institution complained of and the damage, the burden of proof of which rests on the applicant, so that the conduct complained of must be the determining cause of the damage.

147 Furthermore, it is apparent from the case-law that the causal link required for engagement of the European Union's non-contractual liability under the second paragraph of Article 340 TFEU is established where the damage is the direct consequence of the wrongful act in question (judgment of 28 June 2007, *Internationaler Hilfsfonds* v *Commission*, C-331/05 P, EU:C:2007:390, paragraph 23).

148 As regards the direct nature of the causal link, the Court has previously held that the injury must result directly from the alleged illegality and not from the applicant's choice as to how to react to the allegedly unlawful act. The view has thus been taken that the mere fact that the unlawful conduct constituted a necessary condition (*conditio sine qua non*) for the damage to arise, in the sense that the damage would not have arisen in the absence of such conduct, is not sufficient to establish a sufficiently direct causal link within the meaning of the case-law of the European Union (see, to that effect and by analogy, judgments of 30 November 2011, *Transnational Company 'Kazchrome' and ENRC Marketing* v *Council and Commission*, T-107/08, EU:T:2011:704, paragraph 80 and the case-law cited, and of 23 May 2019, *Remag Metallhandel and Jaschinsky* v *Commission*, T-631/16, not published, EU:T:2019:352, paragraph 52 and the case-law cited).

149 It thus follows from the case-law that no such causal link is demonstrated when the loss invoked is the direct consequence of the applicant's own decision or free choice and cannot, therefore, be attributed to the institution or body concerned (see, to that effect and by analogy, judgments of 28 June 2007, *Internationaler Hilfsfonds* v *Commission*, C-331/05 P, EU:C:2007:390, paragraphs 22 to 29; of 17 February 2017, *Novar* v *EUIPO*, T-726/14, EU:T:2017:99, paragraphs 31 and 32; and of 28 February 2018, *Vakakis kai Synergates* v *Commission*, T-292/15, EU:T:2018:103, paragraph 173 and the case-law cited).

150 In the present case, it is necessary, therefore, to examine whether the conduct of the Commission that is complained of, that is to say, the use of the Amazon CloudFront service as the content delivery network for the CFE website, is the direct cause of the non-material damage claimed, consisting in a loss of control over the applicant's personal data which were transferred to the United States when he visited the CFE website on 8 June 2022.

151 In that regard, first, it is apparent from the case file and from the parties' replies to the questions put at the hearing that, on 8 June 2022, the applicant was in Munich and visited the CFE website a number of times. During those visits, successive connections were established from the applicant's IP address to various servers of the Amazon CloudFront service that are geographically remote from each other. Thus, at 7.13 a connection was established to a server in Munich; at 11.13, to a server in London (United Kingdom); at 12.56, to a server in Hillsboro (Oregon, United States); at 13.05, to a server in Newark; and, at 19.12, to a server located in Frankfurt am Main (Germany).

152 Secondly, it is apparent from the case file that the applicant's IP address was transferred to the various servers of the Amazon CloudFront service referred to in paragraph 151 above, including those located in the United States.

153 Thirdly, it must be recalled that the applicant's IP address constitutes personal data.

154 Fourthly, it must be noted that, on 8 June 2022, the CFE website logged 4 548 views and 18 different IP addresses. Of those, just one IP address, namely the applicant's, established a connection to servers outside the European Union, that is, in the United States and in the United Kingdom. In that regard, it should be noted that it has been neither demonstrated nor claimed that, on 8 June 2022, the Amazon CloudFront service for the CFE website may have had technical or other problems that would have prevented its routing mechanism from operating normally according to the principle of proximity, which redirects requests from users of the CFE website to the edge server providing the lowest latency depending on the user's geographical location (see paragraph 112 above).

155 Fifthly, as regards the circumstances of the connections established from the applicant's IP address to servers in the United States, on the one hand, it is apparent from the case file and from the parties' replies at the hearing that the applicant maintains that those connections resulted from the operation of Amazon CloudFront and not from any manipulation on his part. On the other hand, the Commission states that those connections were atypical and can only be accounted for by some technical manipulation on the part of the applicant.

156 In that regard, it should be noted that the circumstances described in paragraph 151 above demonstrate that the various locations of the servers to which the applicant's IP address connected could not have been accounted for by the applicant's physical relocation on the same day, which would have been impossible in view of the distances and timings involved. Furthermore, no malfunction of the Amazon CloudFront service has been either demonstrated or alleged, and it may therefore be concluded that, on 8 June 2022, that service was operating on the basis of the principle of proximity to the user's terminal, with its routing mechanism directing requests from users of the CFE website to the edge server providing the lowest latency (see paragraph 154 above).

157 Accordingly, the connections that were established from the applicant's IP address to servers located in the United States, when he was in Germany, cannot be attributable to the normal operation of the Amazon CloudFront service; rather, they were attributable to a technical adjustment made by the applicant to change his apparent location, by presenting himself in the digital sphere as though he were, on the same day, in various places near Munich, London, Hillsboro, Newark and Frankfurt am Main, one after the other.

158 It follows that it is indeed the operation of the Amazon CloudFront service, with its routing mechanism which functions according to the principle of proximity and which covers a geographic area greater than the territory of the EEA, including in particular the United States (see paragraphs 112 and 114 above), that made it possible for the applicant's IP address to connect, during visits to the CFE website, to Amazon CloudFront servers located in the United States.

159 However, although the Commission's use of the Amazon CloudFront service is a necessary condition for the transfers of personal data to the United States referred to in paragraph 152 above, that is not sufficient, in the circumstances of the present case, to establish a sufficiently direct causal link between the non-material damage invoked by the applicant and the Commission's allegedly unlawful conduct, consisting in the use of such a service contrary to the provisions of Chapter V of Regulation 2018/1725.

160 In fact, it is the applicant's conduct that must be regarded as being the direct and immediate cause of the non-material damage claimed, and not the alleged misconduct on the part of the Commission in using the Amazon CloudFront service.

161 Thus, it is the applicant who created the conditions required to trigger connections to servers located in the United States through the operation of the Amazon CloudFront service. It is the applicant's conduct that caused the routing mechanism of the Amazon CloudFront service to redirect his requests to visit the CFE website to servers located in the United States, those being the servers that had the lowest latency in relation to what appeared, in the digital sphere, to be the applicant's location, albeit that it was not his actual location.

162 Moreover, the applicant is not justified in behaving in such a way as to trigger a certain outcome (namely the transfer of his personal data to a third country), only subsequently to claim compensation for damage allegedly caused by that outcome, which was in fact directly caused by his conduct. Accordingly, contrary to the applicant's contention, in the context of a claim for damages such as that in this case, his situation cannot be assessed in the same way as that of a user who, having actually travelled to the United States, may have accessed the CFE website from within that country.

163 It follows from all of the above that, with regard to the disputed transfer at the time of the visits to the CFE website on 8 June 2022, a sufficiently direct causal link between the Commission's allegedly unlawful conduct and the non-material damage invoked has not been demonstrated.

164 Since one of the cumulative conditions for the European Union's non-contractual liability is not satisfied, the Court must dismiss the claim for damages with regard to the disputed transfer at the time of the visits to the CFE website on 8 June 2022, and there is no need to examine the other conditions for establishing such liability.

– *Disputed transfer on signing in to EU Login on 30 March 2022*

165 The applicant claims that, on 30 March 2022, when he registered for the 'GoGreen' event available on the CFE website, his IP address and information about his browser and his terminal were transferred to Meta Platforms, an undertaking established in the United States, which owns the social networking site, Facebook. While registering, the applicant was redirected to the EU authentication service, EU Login, which offers, inter alia, the ability to sign in via various social media. The applicant opted to sign in via his Facebook account and, when he clicked on the hyperlink redirecting him to Facebook, that link, he claims, resulted in the transmission of his IP address to Facebook. The applicant states that he had accepted only Facebook's 'essential cookies'. Other personal data of the applicant's, namely his email address, his first and last names and his profile picture, were collected by Facebook using cookies, notably the 'sb' cookie, and transferred to Meta Platforms' servers. He argues that it is apparent from the case-law that website operators which use Facebook on their websites, as the Commission does, are jointly responsible with Facebook for complying with EU data protection law. The Commission therefore shares responsibility for the placement of cookies stored by Facebook. The applicant claims to have lost control of his personal data that were transmitted to Facebook and to have been deprived of his rights and freedoms, which constitutes non-material damage within the meaning of recital 46 of Regulation 2018/1725.

166 The Commission contests those arguments. It contends, in essence, that it neither carried out nor initiated transfers of data to Meta Platforms. It argues that it was not mandatory to proceed via EU Login when registering to participate in the 'GoGreen' event and, even when using EU Login, the applicant would have had various authentication options, including options that did not require the use of a social media account. It was therefore the applicant's choice to sign in to the EU Login service with his Facebook account, and it was therefore the applicant, not the Commission, who initiated access to the Facebook website. Furthermore, from a technical perspective, authentication via Facebook is an option that functions via the hyperlink displayed on the EU Login website, which does not contain the user's personal data. Contrary to the applicant's contention, data collected by the cookies used by Facebook are not transferred to the Commission on signing in to EU Login and are not the Commission's responsibility. Those cookies resulted from exchanges between Facebook and the applicant, on the basis of the consent given by the applicant, and the Commission is not involved in those exchanges. In addition, the Commission maintains that the case-law invoked by the applicant is not applicable in this case and that, in any event, the applicant's argument as to the joint responsibility of the Commission and Meta Platforms is a new plea in law that was raised for the first time at the stage of the reply and is consequently inadmissible.

167 In the present case, it is appropriate first of all to examine the facts surrounding the disputed transfer on signing in to EU Login on 30 March 2022, taking into account the material that is evident from the case file and the parties' replies to the questions put by the Court at the hearing and in the measure of organisation of procedure of 9 February 2024.

168 In that regard, it should be noted that the 'GoGreen' event, which was organised by a body based in the Netherlands, was announced on the CFE website. It was possible to register for that event, inter alia, on the CFE website, through the EU Login service.

169 The applicant chose to register on the CFE website using EU Login.

170 EU Login is the Commission's user authentication service, which protects hundreds of EU-related websites and applications (apps). In the present case, signing in to EU Login, for the purpose of registering for the 'GoGreen' event, was intended to ensure that that registration came from a verified email address, reducing the risks associated with the registration of fake users or identity theft.

171 A number of sign-in options are displayed on the EU Login webpage. The first option is to sign in to EU Login directly, either by completing the sign-in details for an existing EU Login account, or by creating an account for that service. The second option is to use an electronic identity card, 'eID', available to citizens of certain Member States. The third option, which is available for a limited number of services, is to use an existing account held by the user on Facebook, Twitter or Google, by clicking on the corresponding hyperlink displayed on the EU Login website.

172 The possibility of signing in to EU Login through a Facebook account stems from the fact that the Commission considered it appropriate to give users the choice of signing in to EU Login through existing accounts on platforms in order to offer them quicker and easier access, as well as the possibility of authentication without the need to set up an EU Login account, so as not to multiply the number of accounts and entities with which users are required to share their personal data. Furthermore, the Commission considered Facebook to be reliable for the purpose of verifying users' email addresses, given the measures Facebook has put in place. Nevertheless, the hyperlink through which users can sign in via an existing Facebook account is available on EU Login only for websites or apps requiring only a basic level of security.

173 The applicant selected the option of signing in to EU Login through his Facebook account, using the 'Sign in with Facebook' hyperlink displayed on the EU Login website ('the "Sign in with Facebook" hyperlink').

174 The 'Sign in with Facebook' hyperlink contains a link to a website that is external to the Commission. When a user activates that hyperlink by clicking on it, access is given via the hyperlink to a URL address of the Facebook website, that is to say, to an individual address of that website.

175 Access to the Facebook website's URL address results in communication between the user's browser and that website, in which the browser transmits the user's IP address to the website concerned. That transmission is similar to that which arises when a user enters the URL address of a particular website in his or her browser directly, in so far as the IP address necessarily has to be communicated by any internet user wishing to access a website.

176 By means of the 'Sign in with Facebook' hyperlink, EU Login sends certain information to Facebook that is necessary for the authentication process, as in the following example:

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 More specifically, the information contained in the 'Sign in with Facebook' hyperlink is as follows:

– first, 'client_id=1200572836629487' contains a 'unique identification code' which identifies EU Login as an application. This identification number is the same for any user wishing to proceed with authentication on EU Login using Facebook;

– secondly, 'redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthCallback' contains the general URL address of EU Login, which is the address to which Facebook must redirect users after they have consented to their personal data being transmitted to EU Login by Facebook;

– thirdly, 'scope=email' contains the data which Facebook must transmit to EU Login in order to ensure the user's successful authentication, in particular the user's email address and first and last names, as indicated on the Facebook site when he or she set up a Facebook account;

– fourthly, 'state=useFacebook' indicates that the long chain of characters that follows is a random security value that is used to avoid security attacks and is valid for a limited period only. That random security value is randomly generated by EU Login and acts as a passphrase, which Facebook must repeat when transmitting data to EU Login, so that EU Login knows that the email address and first and last names communicated relate to the user who initiated the authentication process. Once the period has expired or the user has already been authenticated, the security value can no longer be used; and

– fifthly, 'response_type=code' indicates that the transmission of data to EU Login by Facebook is also accompanied by a unique code. That unique code includes the random security value mentioned above. The unique code is equivalent to a unique registration number or a series number which authenticates the data transmitted to EU Login by Facebook.

178 Once the user has accessed Facebook's URL address, he or she will be on Facebook's website, on which, first of all, a window is displayed asking the user to accept Facebook's use of cookies. Next, if cookies are accepted, another window opens in which the user's name and the password for the user's Facebook account can be entered. Lastly, once connected to his or her Facebook account, the user can authorise Facebook to use cookies placed on other apps and websites, by responding to the question 'Allow Facebook to use cookies and similar technologies placed on other apps and websites?'. If the user consents to that use, he or she will then be invited to consent to Facebook providing EU Login with the first and last names, profile picture and email address linked to his or her Facebook account. Furthermore, throughout that process, the user can interrupt authentication through his or her Facebook account by selecting the 'Cancel' option. In that case, the user will be redirected to the EU Login website, where the page with the sign-in options is again displayed.

179 In the present case, when the applicant clicked on the 'Sign in with Facebook' hyperlink, his web browser accessed the URL address of the Facebook website and, consequently, communicated his IP address to that website. Next, once he was on the Facebook website, the applicant selected the options enabling Facebook to use only essential cookies, then signed in to his Facebook account and, lastly, authorised Facebook to communicate to EU Login his first and last names, profile picture and email address, as entered on his Facebook account.

180 Once the applicant had granted those authorisations, Facebook redirected him to the EU Login website, in accordance with the information contained in the 'Sign in with Facebook' hyperlink (see first and second indents in paragraph 177 above).

181 At the same time, Facebook communicated to EU Login the random security value and unique code mentioned in the fourth and fifth indents in paragraph 177 above. First, that communication from Facebook informed EU Login that the personal data which Facebook was making available to it concerned the user who had initiated the authentication process, that is, in this case, the applicant. Secondly, it enabled EU Login to access, for a limited period, the personal data referred to in the third

indent in paragraph 177 above, that is to say, inter alia, the applicant's first and last names and email address, as entered on his Facebook account. Those data were transmitted to EU Login by Facebook via an encrypted connection between them. EU Login authenticated the applicant's email address on the basis of the data made available by Facebook.

182 It should, moreover, be pointed out that the social networking site Facebook is owned by Meta Platforms, an undertaking established in the United States.

183 It should also be noted that the display of that hyperlink on the EU Login website is governed by the general terms and conditions of the Facebook platform, available at 'https://developers.facebook.com/terms'.

184 It is in the light of those considerations that the Court must examine whether the conditions for establishing non-contractual liability on the part of the Commission have been satisfied.

185 The applicant submits, in essence, that when he signed in to EU Login on 30 March 2022, there was a transfer of his personal data, including his IP address, to servers of Facebook, a social networking site owned by an undertaking established in the United States. That transfer was, he claims, contrary to Article 46 of Regulation 2018/1725 and caused him non-material damage consisting in a loss of control of his data and in his being deprived of his rights and freedoms.

186 As a preliminary point, it should be recalled that, as is apparent from paragraph 95 above, a transfer of personal data to a third country, within the meaning of Article 46 of Regulation 2018/1725, requires that an EU institution, body, office or agency make personal data available, by transmission or otherwise, to a recipient established in a third country, that is to say, a country which is a member of neither the European Union nor the EEA.

187 In the present case, it has been demonstrated that, first, of the various options for signing in to EU Login, the applicant chose to sign in with his Facebook account. Secondly, the 'Sign in with Facebook' hyperlink contains a link to a URL address of the Facebook website. Thirdly, when the applicant activated that hyperlink by clicking on it, his browser accessed the URL address of the Facebook website and then transmitted his IP address to Facebook (see paragraphs 173 to 175 above).

188 It follows that, by means of the 'Sign in with Facebook' hyperlink displayed on the EU Login webpage, the Commission created the conditions for the applicant's IP address to be transmitted to Facebook. That IP address constitutes the applicant's personal data (see paragraph 122 above), which, by means of that hyperlink, was transmitted to Meta Platforms, an undertaking established in the United States. That transmission amounts, therefore, to a transfer of personal data to a third country, within the meaning of Article 46 of Regulation 2018/1725.

189 It has also been established in this case that, at the time of that transfer of data, on 30 March 2022, no adequacy decision, within the meaning of Article 47 of Regulation 2018/1725, existed with regard to the United States (see paragraph 100 above).

190 In the absence of an adequacy decision of the Commission with regard to the United States, personal data may be transferred to a third country or to an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available, in accordance with Article 48(1) of Regulation 2018/1725 (see paragraph 101 above).

191 In the present case, the Commission has neither demonstrated nor claimed that there was an appropriate safeguard, in particular a standard data protection clause or contractual clause adopted in accordance with the conditions laid down in Article 48(2) and (3) of Regulation 2018/1725 (see paragraphs 102 to 104 above). By contrast, it has been demonstrated that the displaying of the 'Sign in with Facebook' hyperlink on the EU Login website is entirely governed by the general terms and conditions of the Facebook platform (see paragraph 183 above).

192 Consequently, the Commission created the conditions for a transfer of the applicant's personal data to a third country to proceed, without, however, complying with the conditions laid down in Article 46 of Regulation 2018/1725.

193 It must therefore be concluded, without any examination of the applicant's other arguments being required, that the Commission committed a sufficiently serious breach, within the meaning of the case-law recalled in paragraph 50 above, of Article 46 of Regulation 2018/1725 in relation to the disputed transfer on signing in to EU Login on 30 March 2022.

194 The Court must, therefore, consider whether the other conditions for establishing the Commission's non-contractual liability, relating to damage and a causal link, are satisfied in the present case.

195 The applicant claims that the unlawful transfer of his IP address to an undertaking established in the United States caused him non-material damage consisting in a loss of control of his data and in his being deprived of his rights and freedoms.

196 In that regard, it must be held that, under Article 65 of Regulation 2018/1725, not only 'material damage' but also 'non-

material damage' suffered as a result of an infringement of that regulation gives rise to a right to compensation, without any reference being made to any threshold of seriousness (see, to that effect and by analogy, judgment of 4 May 2023, *Österreichische Post (Non-material damage in connection with the processing of personal data)*, C-300/21, EU:C:2023:370, paragraphs 45 and 51).

197 In the present case, the non-material damage invoked by the applicant must be considered to be actual and certain, within the meaning of the case-law recalled in paragraph 54 above, in so far as the transfer referred to in paragraph 188 above, which was contrary to Article 46 of Regulation 2018/1725, put the applicant in a position of some uncertainty as regards the processing of his personal data, in particular of his IP address.

198 In addition, there is a sufficiently direct causal link, within the meaning of the case-law recalled in paragraph 55 above, between the infringement by the Commission of Article 46 of Regulation 2018/1725 and the non-material damage suffered by the applicant.

199 In the circumstances of the present case, the amount of the non-material damage caused by the Commission must be assessed on an equitable basis at EUR 400.

200 Therefore, the Commission must be ordered to pay the sum of EUR 400 to the applicant for the non-material damage sustained as a result of the disputed transfer on signing in to EU Login on 30 March 2022.

Costs

201 Pursuant to Article 134(3) of the Rules of Procedure of the General Court, the parties are to bear their own costs where each party succeeds on some and fails on other heads. However, if it appears justified in the circumstances of the case, the Court may order that one party, in addition to bearing its own costs, pay a proportion of the costs of the other party.

202 In the present case, the applicant has failed on the first and second heads of claim and on part of the third head of claim. However, the third head of claim has been upheld in part, and the Commission ordered to pay the damages sought by the applicant in compensation for the non-material damage which he sustained as a result of the disputed transfer on signing in to EU Login on 30 March 2022. In those circumstances, the Commission should be ordered to bear its own costs and to pay one half of the costs incurred by the applicant. The applicant must bear one half of his own costs.

On those grounds,

THE GENERAL COURT (Sixth Chamber, Extended Composition)

hereby:

1. **Dismisses the action as inadmissible with regard to the claim for annulment;**

2. **Declares that there is no longer any need to adjudicate on the claim for a declaration that the European Commission unlawfully failed to define its position on Mr Thomas Bindl's information request of 1 April 2022;**

3. **Orders the Commission to pay Mr Bindl the sum of EUR 400 in compensation for the non-material damage sustained;**

4. **Dismisses the claim for damages as to the remainder;**

5. **Orders the Commission to bear its own costs and to pay one half of the costs incurred by Mr Bindl;**

6. **Orders Mr Bindl to bear one half of his own costs.**

Costeira Kancheva Öberg

Zilgalvis Tichy-Fisslberger

Delivered in open court in Luxembourg on 8 January 2025.

[Signatures]

Table of contents

---

* Language of the case: German.