AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Hoge Nieuwstraat 8, 2514 EL Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Takeaway.com Group B.V.
Attn: the Management Board
Piet Heinkade 61
1019 GM AMSTERDAM

COURTESY TRANSLATION ONLY

Date
20 August 2024

Our reference
z2022-04011

Contactpersoon
[redacted]

Subject
Decision to impose a reprimand

Dear Management Board,

The Dutch Data Protection Authority (hereinafter referred to as Dutch DPA) has investigated the international transfer of personal data to the United States by Takeaway Group B.V. (hereinafter referred to as Takeaway). The Dutch DPA has established that Takeaway has transferred personal data to Google LLC in the United States in the context of the Google Analytics service. However, Takeaway did not meet the conditions applicable to international transfers of personal data in the period from 18 August 2020 to 1 September 2023, because Takeaway could not rely on one of the transfer instruments regulated in the General Data Protection Regulation during that period (hereinafter referred to as GDPR). Takeaway has thus violated Article 44 of the GDPR.

The Dutch DPA decides to take enforcement action against Takeaway, because with the international transfer of personal data to the United States, Takeaway has undermined the level of protection to be guaranteed for the personal data of data subjects. The Dutch DPA considers this serious and therefore considers it necessary and appropriate to reprimand Takeaway for this. This decision explains the violation and the reprimand. At the end of this decision, we explain what you can do if you do not agree with the decision.

Datum
20 August 2024

Ons kenmerk
z2022-04011

Table of contents

1. Course of the investigation

1.1. Background

1. On 18 August 2020, the Dutch DPA received a complaint filed by non-profit organisation noyb (none of your business; European Centre for Digital Rights) on behalf of Mr [redacted] from Austria (hereinafter referred to as the complainant). The complaint forms part of a series of complaints that noyb has filed with various European data protection agencies. The complainant's complaint is against the use of Google Analytics (hereinafter referred to as Analytics) on the websites of Takeaway, such as «www.thuisbezorgd.nl».

2. The complaint boils down to the fact that personal data is transferred to the United States in the context of the Analytics service without using a valid transfer mechanism as referred to in Chapter 5 of the GDPR.

1.2. Substance of the complaint

3. The complaint states that the complainant visited the website «www.thuisbezorgd.nl» on 17 August 2020. Takeaway has embedded HTML/JavaScript code for Google services on this website, including Analytics. Their use is subject to the Analytics Conditions of Service. Both those conditions and the associated conditions for data processing of Google Ads state that Google LLC is the processor and Takeaway is the controller. The conditions further state that Google, as a processor, stores and processes personal data in the United States.

4. The HAR file sent with the complaint states that personal data was processed and transferred to Google during the complainant's visit to the Takeaway website, including, in any case, the complainant's IP address and cookie data. According to the complainant, his personal data have therefore been transferred and stored in the United States.

5. Under the GDPR, international transfers of personal data must rely on one of the instruments listed in Chapter V of the GDPR. The complainant points out that the Court of Justice of the European Union (hereinafter referred to as the Court) invalidated the adequacy decision taken for the United States ("EU-U.S. Privacy Shield") by judgment of 16 July 2020,[1] so the transfer can no longer rely on that instrument at the time of filing the complaint.

6. Furthermore, the complainant points out that the transfer to a third country cannot rely on the instrument of standard provisions if the country of destination does not provide adequate protection for the personal data transferred under EU law. In the aforementioned judgment, the Court explicitly established that transfers to American companies that fall under § 50 U.S. Code 1881 (4)(b), violate not only the relevant articles of Chapter V of the GDPR, but also Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. According to the complainant, Google should be regarded as a company that falls under the aforementioned provision and is therefore subject to supervision by American intelligence services. According to the complainant, Takeaway is therefore unable to guarantee an adequate level of personal data protection for the data transferred to Google in the United States.

7. The complainant concludes that the transfer by Takeaway violates Chapter V of the GDPR.

1.3. Investigation and procedure

8. The Dutch DPA has seen reason to start a broader investigation into the use of Analytics and the transfer of personal data of Takeaway website visitors. The supervisory authorities' findings were set out in

[1] Judgment of the Court of 16 July 2020 in case C-311/18 (ECLI:EU:C:2020:559), *Schrems II*.

an investigation report dated 7 April 2022.

9. Takeaway was given the opportunity to comment on the report and took advantage of that opportunity by letter dated 15 August 2022. On Tuesday 8 November 2022, Takeaway explained its view verbally. After the opinion hearing, the Dutch DPA asked further questions on 5 December 2022, which Takeaway answered on 6 January 2023. Takeaway also provided an additional opinion.

1.4. Developments after the investigation

10. On 25 March 2022, the European Commission and the United States announced they had reached an agreement in principle on a new Transatlantic Data Privacy Framework. The agreements contained herein form the basis for further legal measures regarding the protection of personal data in data traffic between the European Union and the United States. Following the agreement in principle, the European Commission made another adequacy decision for the United States on 10 July 2023, referred to as "EU-U.S. Data Privacy Framework" (hereinafter referred to as DPF). From that date, personal data can be transferred to parties in the United States that have committed to the DPF through so-called self-certification.

11. In response to questions from the Dutch DPA, Google LLC stated in a letter dated 21 August 2023 that it intends to base the international transfer of personal data from the European Union to the United States on the DPF with effect from 1 September 2023. Since Google LLC has remained registered as a certified participant of the "EU-U.S. Privacy Shield", and participants thereof are automatically brought under the operation of the DPF, no additional (self) certification is required, according to Google LLC.

12. In view of the foregoing, what has been considered in this decision relates to the period from 18 August 2020 (the day on which the investigation started) to 1 September 2023 (the day on which the transfer is again based on a valid adequacy decision).

13. At the time of the investigation, Takeaway used Google Analytics 3 (Universal Analytics). This version is no longer available and has been replaced with Google Analytics 4. The information in this decision only concerns Google Analytics 3. The Dutch DPA has not conducted any investigation into Google Analytics 4.

2. Assessment

14. This section discusses the findings as they follow from the investigation report, Takeaway's opinion of 14 August 2022 (hereinafter referred to as the opinion), the opinion hearing and the supplementary opinion of 6 January 2023 (hereinafter referred to as the supplementary opinion).

2.1. Processing responsibility

Investigation report

15. It follows from sections 2.1 and 2.2 of the investigation report that Takeaway uses Analytics to monitor, evaluate and optimise the use and functioning of its websites. To this end, Takeaway has implemented a JavaScript code, which is executed on the visitor's device when he or she visits the website. Implementing this code is a requirement to use Analytics and requires an active action from Takeaway. In the investigation report, Takeaway has been designated as the controller, because it has been established that Takeaway decides on the purpose of the processing and the means for this.

Takeaway's opinion

16. Takeaway has substantively disputed in its opinion that it is the controller of a number of the websites mentioned in the investigation report. During the opinion hearing it was established that Takeaway is in any case responsible for the websites «www.thuisbezorgd.nl» (the Netherlands), «www.just-eat.dk» (Denmark), «www.just-eat.fr» (France), «www.lieferando.at» (Austria), «www.lieferando.de» (Germany), «www.pyszne.pl» (Poland), «www.takeaway.com/be» (Belgium), «www.takeaway.com/bg» (Bulgaria) and «www.takeaway.com/lu» (Luxembourg).

Assessment and conclusion

17. The Dutch DPA notes that Takeaway is responsible for processing personal data to gain insight into the use and functioning of its websites via Analytics. In view of Takeaway's arguments, this only concerns the websites listed in marginal 16.

2.2. Personal data and processing

Investigation report

18. Section 2.2 of the investigation report determines which categories of personal data have been transferred by Takeaway to the United States. This determination is based on the information submitted with the complaint discussed in section 1.2 (HAR file) on the one hand and on the findings of supervisory authorities of the Dutch DPA itself on the other. The transfer concerns at least the following categories of personal data:

1. information about the browser used by the visitor, operating system, *referrer* and language;
2. tracking ID;
3. screen resolution information;
4. [redacted];
5. [redacted].

Takeaway's opinion

19. Takeaway has not disputed the findings about the processed personal data. In response to questions that arose during the opinion hearing, Takeaway has drawn up an additional document that lists additional categories of personal data transferred to the United States by Takeaway. This document includes (but is not limited to) the following data:

6. [redacted];
7. [redacted];
8. [redacted];
9. [redacted];
10. [redacted].

Assessment and conclusion

20. In the opinion of the Dutch DPA, the data stated in the investigation report and in the document drawn up by Takeaway qualifies as personal data within the meaning of Article 4, opening words and (1) of the GDPR. The Dutch DPA takes the following into account.

Legal framework

21. "Personal data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular on the basis of an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person (compare Article 4, opening words and (1) of the GDPR).

22. In its judgment of 4 May 2023 (ECLI:EU:C:2023:369; *F.F./Österreichische Datenschutzbehörde and CRIF GmbH*), the Court considered that the use of the words "all information" in the definition of the concept of "personal data" indicates that it was the intention of the EU legislator to give a broad interpretation to this concept. The meaning is not limited to sensitive or personal information, but potentially extends to any type of information, both objective and subjective such as opinions or assessments. The only condition is that this information "concerns" the data subject. This condition is met when that information is linked to a specific person because of its content, purpose or effect, according to the Court.

23. According to recital 26 of the GDPR, when determining whether a natural person is identifiable, account should be taken of all means which could reasonably be expected to be used by the controller or by another person to directly or indirectly identify the natural person, for example, selection techniques (in the English text of the GDPR referred to as singling out). To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs

of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The qualification of a piece of data as personal data within the meaning of the GDPR does not require that all information from which the data subject can be identified be held by one and the same person (judgment of the Court of 7 March 2024; ECLI:EU:C:2024:214; *IAB Europe*).

24. According to recital 30 of the GDPR, natural persons may be linked to online identifiers through their device, applications, instruments and protocols, such as (IP) addresses and identification cookies. This may leave traces that, in particular when combined with unique identifiers and other information received by the servers, can be used to create profiles of natural persons and recognise natural persons.

General qualification by controller

25. In its role as controller, Takeaway endorses that the data stated in margins 18 and 19 qualifies as personal data. A different view would also be inconsistent with the processing agreements that Takeaway has concluded with Google for the use of Analytics. After all, these agreements would not be necessary if no personal data was processed.

With regard to the data stated in the report

26. It must be assumed that the aforementioned data is associated with a specific person due to its content. Although some of the data contains information about the device used (information about the browser, operating system and screen resolution), this cannot lead to the conclusion that this data relates exclusively to that device and therefore not to a person. After all, this would ignore the fact that this information concerns the person who used the device. If the device and the user were separated, the data listed in margin 18 would always be non-personal. Such a view would lead to an overly limited meaning of the concept of "personal data", especially since the Court has considered that the intention of the Union legislator was to give a broad meaning to this concept. It also follows from recital 30, stated in margin 24, that the legislator did not have this in mind.

27. As stated in margin 22, it follows from the case law mentioned there that information is personal data if it is linked to a specific person due to its content, purpose or effect. As the previous section concluded that the categories of personal data are already linked to a specific person because of their content, the Dutch DPA will ignore the question of whether this is also the case because of the purpose or effect.[2]

28. The Dutch DPA further notes that the data stated in margin 18 makes the persons concerned identifiable. The data includes unique online identifiers such as [redacted] and cookie identifiers such as the tracking ID and [redacted]. By their nature, these identifiers serve to distinguish visitors to a website from each other (*singling out,* in Dutch "selection techniques") and, for example, to

[2] Within the same meaning, compare Opinion 4/2007 on the concept of personal data of the Article 29 Data Protection Working Party, p. 10-11.

recognise if it is a new or a returning visitor. In accordance with the decision of the European Data Protection Supervisor (hereinafter referred to as the EDPS) of 5 January 2022[3] and the decision of the Austrian supervisory authority (hereinafter referred to as DSB) of 22 December 2021,[4] the Dutch DPA considers unique identifiers in cookies such as those of Analytics as personal data, even if the actual identity of the user in question is unknown.

29. The position of the Dutch DPA is that when distinguishing (singling out) between different visitors by means of unique identifying data, that data in itself constitutes personal data, which is consistent with views in the literature. It states that because the GDPR attempts to limit the risks for data subjects, *singling out* should be sufficient to call it personal data.[5] The reasoning is that the risks of large-scale data collection are not reduced because no name can be linked to a unique online identifier. Therefore, data that facilitates *singling out* should be regarded as personal data.

30. Lastly, the view that unique identifiers for selection techniques constitute personal data is in line with the rationale of the GDPR and the broad interpretation of the material scope of the GDPR in case law.[6] For example, recital 10 of the GDPR states that a high level of protection is desirable. The Court has always confirmed this in its case law.[7] Furthermore, according to the Court, the GDPR must be interpreted in the light of the Charter, in which the right to respect for privacy and the right to the protection of personal data are laid down in Articles 7 and 8. According to settled case law of the Court, the exceptions and limitations to the protection of personal data must remain within the limits of what is strictly necessary.[8]

31. In conclusion, all unique identifiers that can be used to distinguish users should be considered, treated and protected as personal data.[9]

With regard to the information stated in the document drawn up by Takeaway

32. As mentioned, after the opinion hearing, Takeaway prepared an additional document, stating which data is passed on to Google. This includes data that falls outside the regular data collected by Analytics (so called *custom metrics*). This data includes information about [redacted].

[3] EDPS decision of 5 January 2022 in case 2020-1013, p. 13.
[4] Decision of the French supervisory authority (CNIL) of 22 December 2021, p. 4 (the decision can be consulted at <https://www.cnil.fr/sites/cnil/files/atoms/files/decision_ordering_to_comply_anonymised_-_google_analytics.pdf>).
[5] Frederik J. Zuiderveen Borgesius, 'Singling out people without knowing their names', Computer Law & Security Review 32 (2016), p. 267-269.
[6] Judgments of the Court of Justice of 20 May 2003 in case no. C-465/00 (ECLI:EU:C:2003:294; *Österreichischer Rundfunk et all.*; preamble 43), 6 November 2003 in case no. C-101/01 (ECLI:EU:C:2003:596; *Lindqvist,* preamble 88), 7 May 2009 in case no. C-553/07 (ECLI:EU:C:2009:293; *Rijkeboer,* preamble 59), 20 December 2017 in case no. C-434/16 (ECLI:EU:C:2017:994; *Nowak*, preamble 33) and 22 June 2021 in case no. C-439/19 (ECLI:EU:C:2021:504; *Latvijas Republikas Saeima,* preamble 61).
[7] Judgment of the Court of Justice of 16 December 2008 in case no. C-524/06 (ECLI:EU:C:2008:724, preamble 50) and 13 May 2014 in case no. C-131/12 (ECLI:EU:C:2014:317; *Google/Spain* , preamble 66.).
[8] Judgment of the Court of Justice of 7 November 2013 in case no. C-473/12 (ECLI:EU:C:2013:715; *Institut professionnel des agents immobiliers*; preamble 39).
[9] Compare p. 13 of the EDPS decision of 5 January 2022 in case no. 2020-1013.

It requires no further explanation that data about [redacted] is related to an identifiable person according to their content, effect and purpose and is therefore personal data within the meaning of Article 4, opening words and (1) of the GDPR.

33. Furthermore, as a result of this latter conclusion, the unique identifiers and device data discussed above are data relating to an identifiable individual, even if what has been considered about selection techniques is ignored.

Conclusion

34. The data stated in margins 18 and 19 is, individually or in conjunction with each other, personal data within the meaning of Article 4, opening words and (1) of the GDPR. The collection, disclosure by transmission, retention and use thereof constitutes processing within the meaning of Article 4, opening words and (2) of the GDPR.

2.3. Cross-border processing and the competence of the Dutch DPA

Investigation report

35. Section 3.2.2 of the investigation report states that Takeaway focuses on the market of several member states of the European Union (compare margin 16 of this decision) and, in addition to its main establishment in the Netherlands, has establishments in Belgium, Germany, Poland, Bulgaria and Romania. Analytics is also used for websites in other Member States. The report therefore concludes that the processing takes place in the context of activities of establishments in more than one Member State, which constitutes cross-border processing within the meaning of Article 4, opening words and (23) of the GDPR.

Opinion

36. Takeaway has not disputed the conclusion in the investigation report.

Assessment and conclusion

37. As Takeaway is established in the Netherlands, the Dutch DPA is competent to exercise the powers granted to it under the GDPR towards Takeaway. As the Dutch establishment is also Takeaway's main establishment, the Dutch DPA is also the lead supervisory authority within the meaning of Article 56(1) of the GDPR. This conclusion is coordinated with the supervisory authorities involved.

2.4. Transfer of personal data to the United States

2.4.1. Investigation report

38. Section 2.3 of the investigation report states that Google has stated that all data collected through Analytics is stored on servers in the United States and that this constitutes an international transfer of personal data. Takeaway has stated that the transfer is subject to standard provisions within the meaning of Article 46 of the GDPR. Until 27 September 2021, these were the provisions of the standard model contract *'Controller to processor'*.[10] On this basis, Takeaway is the exporter and Google LLC is the importer of personal data. This situation changed with effect from 27 September 2021. From that date, Takeaway has been concluding the standard model contract *'Controller to processor'* with Google Ireland. Not Takeaway, but Google Ireland has since exported the data to Google LLC. This is based on a standard model contract *'Controller to processor'*.[11]

39. Section 2.3.3 of the report discusses the additional measures taken by Takeaway and Google at the time the report was drawn up. These measures consist of a combination of technical, contractual and organisational measures. In summary, the technical measures relate to the encryption of data during traffic and in storage. The contractual and organisational measures relate to, on the one hand, the handling and assessment of received information requests from intelligence services and reporting thereon and, on the other hand, the physical and digital security of Google's data centres. These measures are further described and assessed in section 2.4.6 of this decision.

40. Section 3.4.2 of the investigation report concludes that entering into standard model contracts does not sufficiently guarantee the level of protection of personal data in the United States to allow the transfer to be based on standard provisions alone. Google LLC is a provider of electronic communications services within the meaning of § 50 U.S. Code 1881 (4)(b) and is obliged to provide personal data to the American intelligence services. Therefore, transfer can only occur if adequate additional safeguards are in place. The safeguards put in place by Google were not found to be effective in the report, which means Takeaway cannot rely on the transfer instrument of standard provisions. This means that a transfer of personal data takes place without being based on a valid transfer instrument, as a result of which Takeaway has violated Article 44 of the GDPR. This applies, as stated in margin 12, from 18 August 2020 to 1 September 2023.

2.4.2. Safeguards put in place after the investigation

41. In the opinion and supplementary opinion, Takeaway has put forward that it has taken more additional measures. In summary, this involves implementing a proxy server in the EEA, [redacted]. These additional measures are also discussed in more detail in section 2.4.6.

[10] This model contract corresponds to the provisions published by the European Commission in its decision 2010/87/EU.
[11] This model contract corresponds to the provisions published by the European Commission in its decision 2021/914/EU.

2.4.3. Responsibility for international transfers

Opinion

42. Takeaway first argues that insofar as there is a violation of Article 44 of the GDPR, an incorrect period was taken into account in the investigation report. To this end, Takeaway points out that it contracted with Google LLC until 27 September 2021 and that Takeaway was therefore responsible for the international transfer until that date. However, from that date onward, there has been a transfer from Takeaway to Google Ireland, and subsequently from Google Ireland to Google LLC. Since then, Google Ireland, not Takeaway, has been responsible for the transfer to countries outside the EU. As a result, Takeaway's violation, if any, ended no later than 27 September 2021, according to Takeaway.

Assessment and conclusion

43. It follows from Article 5(2) of the GDPR that the controller is responsible for the entire processing. Pursuant to Article 24(1) of the GDPR, the controller must take appropriate technical and organisational measures to ensure and demonstrate that the processing is carried out in accordance with the GDPR. Although it follows from Article 28(1) of the GDPR that the controller may outsource the processing or part thereof to a processor, this does not alter the fact that in that case the processing in accordance with Article 5(2) of the GDPR remains at the risk of the controller. In view of the aforementioned provisions, this is no different for sub-processors, especially now that according to Article 28(2), of the GDPR, they may only be involved with the consent of the controller.

44. In view of the foregoing, Takeaway, as the controller, is responsible for the processing of personal data, including the international transfer of that data by Google Ireland on behalf of Takeaway to the United States during the period from 18 August 2020 to 1 September 2023. Takeaway is therefore not followed in the argument that the report took into account an incorrect period of the violation.

2.4.4. Applicability of FISA legislation to Google and Analytics data

Opinion

45. Takeaway argues that the investigation report does not sufficiently substantiate that, with regard to Analytics, Google LLC qualifies as an *electronic communications service provider* (hereinafter referred to as ECSP) as referred to in FISA. The provision referred to contains five categories, three of which refer to provisions in other laws. The report fails to mention which of these categories Google falls under.

46. According to Takeaway, the investigation report does not further address the statement that the Analytics data does not qualify as *foreign intelligence information*. According to Takeaway, this is relevant because data that does not qualify as such falls outside the scope of a FISA request for information.

Assessment and conclusion

47. Takeaway's argument that the report does not indicate on what grounds Google LLC qualifies as an ECSP has no factual basis. In section 3.4.2 (margin 87) of the report, it was concluded that Google in any case qualifies as a "provider of electronic communication service", as referred to in 50 U.S. Code § 1881, part b(4)(b).[12] In short, this includes all providers of services that enable users to receive or send voice messages or electronic communications.[13] The Dutch DPA does not rule out that Google LLC also qualifies as an ECSP on the basis of (c) and/or (d).[14] However, it is only important that Google can be regarded as an ECSP, as this circumstance means that it is obliged to cooperate with requests from security services.

48. The fact that Google can be classified as such also follows from the information published by Google itself. Google has set up a website on which it publishes information about requests from police and security services. It follows from the information published that Google receives, among other things, FISA requests.[15] In the period from July 2022 to December 2022 (the most recent for which Google publishes, given the delay in reporting), Google claims to have received between 0 and 499 requests regarding metadata, which related to 106,000 to 106,499 accounts. Google says it has received an equal number of requests related to the content users have created. It follows from receiving and complying with the requests that Google LLC qualifies as an ECSP.

49. Finally, Takeaway's reference to the statement that Analytics data does not qualify as *foreign intelligence information* does not lead to the intended purpose. The definition of that concept is so broad that it cannot be categorically excluded in advance which data does or does not fall under it.

50. The conclusion is that what Takeaway has put forward provides no grounds for a different conclusion than that in the investigation report, that Google LLC qualifies as an ECSP and as such is subject to supervision by American intelligence services as regulated in 50 U.S. Code § 1881a.

2.4.5. Risk-based approach

51. According to Takeaway, the report incorrectly uses an absolute test when assessing the level of protection of personal data in the United States. In the case of an absolute test, it is not important whether

[12] Compare in the same sense the decision of the DSB of 22 December 2021, can be consulted via <https://www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf>, p. 32, and the decisions of the Swedish supervisory authority of 30 June 2023, references DI-2020-11397, DI-2020-11368, DI-2020-11370 and DI-2020-11373 (all par. 2.4.2.2), which can be consulted via <https://www.imy.se/en/news/four-companies-must-stop-using-google-analytics>.
[13] Pursuant to (b), an ECSP is "a provider of electronic communications service, as that term is defined in section 2510 of title 18". The latter provision reads: "'electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.
[14] Pursuant to (c), an ECSP can also be "a provider of a remote computing service, as that term is defined in section 2711 of title 18". The term "remote computing service" is defined there as "the provision to the public of computer storage or processing services by means of an electronic communications system". On the basis of (d), ECSP can also be defined as "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored".
[15] Compare the data at <https://transparencyreport.google.com/user-data/us-national-security>.

the chance of an actual deterioration of the level of protection is large or small, but the mere existence of the risk is decisive. According to Takeaway, a risk-based approach should be used, which not only looks at theoretical risks but also at the likelihood that these risks will materialise. Takeaway is supported by (1) the judgment of the Court of 16 July 2020 (Schrems II),[16] (2) Article 24 of the GDPR and (3) the Recommendations 01/2020 of the EDPB (hereinafter referred to as the Recommendations).[17] Takeaway concludes that only the implementation of the standard provisions is sufficient for lawful transfer, because a risk-based test shows there are only very minor risks involved in transfer to the United States. In this regard, Google argues that it has not received a FISA request for Analytics data in the past fifteen years. The transfer could therefore be based on the standard provisions used and no additional measures were required, according to Takeaway.

52. The substantiation and assessment of each of the three points put forward by Takeaway will be discussed below.

Schrems II Judgment

Opinion

53. According to Takeaway, the conclusion in the investigation report that the level of protection in the United States is insufficient, is based too much on a recital of the Schrems II judgment that is placed out of context. The investigation report attaches a lot of weight to the word "may" in recital 135 of the judgment (emphasis added):

> *"135. Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore,* ***capable*** *of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."*

54. It follows from the investigation report that it does not matter whether the reduction in the level of protection is highly theoretical. According to Takeaway, an "absolute test" is wrongly applied. The Dutch translation of the Court's judgment contains errors and misses important nuances in recitals 126, 131 to 134 and 137, according to Takeaway. If this is taken into account, it is clear, according to Takeaway, that in its judgment, the Court actually advocates a risk-based approach. Although the Court does not specifically mention this, according to Takeaway it should not be concluded from this that the Court does not adopt that approach. After all, the Court does consider that the level of protection of personal data that has been transferred must be "*essentially equivalent*", and leaves it up to the controller to use the law and practices of

[16] Judgment of the Court of 16 July 2020 in case no. C-311/18 (ECLI:EU:C:2020:559; *Schrems II*).
[17] Recommendations 01/2020 on measures complementary to transfer tools to ensure compliance with the level of personal data protection in the Union, version 2.0 (adopted on 18 June 2021).

the third country in question to assess whether this benchmark is achieved. According to Takeaway, this follows from recital 126 of the judgment, in which the Court refers to "the state of law and practices in the third country concerned" in order to "guarantee protection […] in practice". Only if it is impossible in practice to ensure the effective protection of the personal data that has been transferred, if necessary with additional measures, will the Court consider the consequences in recital 135 quoted above.

55. Thus, according to Takeaway, no guarantee is required that access by third parties can *never* occur; the only requirement is that the level of protection required under Union law is guaranteed *in practice*. Only when the laws and the practices of the country in question insufficiently guarantee effective protection, should the controller take additional measures.

Assessment

56. It must be stated first and foremost that the Schrems II judgment does not show that a risk-based test must be applied to determine the level of protection of – in this case – the United States. As Takeaway itself also notes, the Court did not consider this explicitly and unequivocally.[18] Given the very far-reaching consequences of Takeaway's interpretation, it would be expected that a risk-based test was explicitly mentioned in the judgment.

57. Takeaway is also not followed in the interpretation of that judgment. In recital 126 of the judgment, the Court firstly considered that there are situations in which the recipient of a transfer of personal data is, in view of the state of law and practices in the third country concerned, able to ensure data protection. The mere use of the words "law and practices", contrary to what follows from Takeaway's argument, does not show that the Court means by this that a statutory provision can be ignored that, according to European law standards, is contrary to the data protection law guaranteed by the Charter and the GDPR, solely because it has not been established that the danger of that statutory provision has materialised to date. What the Court does explicitly and unequivocally consider in that recital is that the situation in which the law of the third country makes it possible for public authorities to intervene in the rights of data subjects - such as in the United States - is an example in which standard provisions alone may be insufficient to ensure effective protection.

58. It also does not follow from the other recitals pointed out by Takeaway (131 to 134, and 137) that in its judgment the Court intended to override a statutory jurisdiction that is problematic according to European law standards because the problem has not yet materialised. It does not matter whether the English text of the judgment is used or the official Dutch translation, which, according to Takeaway, contains "a number of errors" and "[misses] the nuances of the ECJ's judgment on a number of points".

[18] Although the Court refers to recital 101 in recital 8 of the GDPR, which states that the movement of personal data to and from the Union is necessary for the development of international trade, this recital is only part of the legal framework. This consideration is not part of the actual answer to the preliminary questions about the circumstances under which an international transfer is or is not legally permissible. The same applies to a balancing with other fundamental rights such as freedom of entrepreneurship.

59. In view of the foregoing, the Dutch DPA concludes that the Schrems II judgment does not support Takeaway's argument that the report wrongly concluded that the level of protection in the United States was inadequate at the time of the observed violation.

Article 24 of the GDPR

Opinion

60. Takeaway further points out that the formulation of Article 24 of the GDPR is risk-based. According to the text of that provision, the controller must take appropriate measures to ensure that the processing is carried out in accordance with the GDPR, taking into account "the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". According to Takeaway, the provision has a horizontal scope of application, which means the provision applies to both the standard of proof and compliance with the obligations under the entire GDPR, including the obligations laid down in Chapter V of the GDPR.

61. In further support of the argument that Chapter V must be approached on a risk-based basis, Takeaway points out – in its opinion – the text of Article 44 of the GDPR itself. Under that provision, a lawful transfer of personal data requires a transfer instrument, "subject to the other provisions of this Regulation". According to Takeaway, this phrase is logical, because Chapter V of the GDPR does not stand alone and transfers must comply with the entire GDPR, including Article 24 of the GDPR. This arises from the fact that Chapter V of the GDPR aims to ensure that after transfer, data is stored in a *comparable* manner and not at a higher level.

62. Takeaway also points out the development history of the GDPR. In the European Commission's proposal for what would eventually become the GDPR,[19] Article 22 (now: Article 24) stipulates that the controller shall establish policies and implement appropriate measures to ensure and be able to demonstrate that the processing is performed in accordance with the regulation. A memorandum from the Cypriot Presidency to the Council of 1 March 2013 states that this provision has been amended after a number of Member States objected to the high prescriptive nature of the provision and expressed the view that the provision must stipulate a risk-based approach.[20] That is why the revised draft contains a 'horizontal' clause in Article 22 (now: Article 24), which is accompanied by a more risk-based reformulation of provisions in that chapter. Furthermore, the European Council's explanatory memorandum to the final draft text of the GDPR states that, against the background of the increased accountability of controllers, an approach based on risk analysis has been opted for throughout the regulation. The obligations of the controller and processor are adjusted to the risk of the data processing

[19] Proposal for a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of 25 January 2012, EUR-Lex document 52012PC0011.
[20] Memorandum from the Presidency to the Council of the European Union of 1 March 2013, EUR-Lex document 6607/1/13 REV 1.

they perform.[21] Lastly, Takeaway points out the communication from the European Commission to the European Parliament of 11 April 2016,[22] which states that the proposal maintains and develops the risk-based approach. According to Takeaway, it follows from all this that the risk-based approach also applies to the obligations arising from Chapter V of the GDPR.

Assessment

63. In the situation where the interpretation of a provision of the GDPR is called into question, the precise wording of that provision must first be examined. It is settled case law of the Court that, despite the clear and precise wording of a provision, an interpretation intended to correct the provision and thus extend the relevant obligations of Member States cannot be given.[23] If the wording of the provision is unambiguous, it leaves no room for interpretation because that would deprive the wording of any useful effect.[24]

64. In the situation that a provision of the GDPR does not contain clear and precise wording, for example, because it is openly formulated or does not contain a precise interpretation of the concepts used, the question arises how the provision should be interpreted. After all, a purely textual interpretation is not sufficient. The interpretation must then be made in the light of the context and objectives of the Charter and the GDPR.[25] The history of the Charter and the GDPR may also contain relevant information.[26] Given various possible interpretations, priority is given to the interpretation that best ensures the intended effect of the regulation.[27]

65. It does not follow from the precise wording of Article 44 that this provision must be read in the risk-based manner advocated by Takeaway. On the contrary, the provision explicitly states that transfers may only take place if the conditions laid down in Chapter V of the GDPR are met, and that all provisions of Chapter V must be applied so that the level of protection guaranteed by the GDPR is not undermined. This is important because the legislator has always explicitly and unambiguously stated in a number of other provisions of the GDPR that a risk-based approach applies to the application of those provisions. Compare Articles 25(1), Article 30(5), Article 32(1) and (2), Article 34(1), Article 35(1) and (2) and Article 37(1), opening words and (b) and (c), of the GDPR.[28] Takeaway cannot therefore be followed in its interpretation

[21] Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repeal of Directive 95/46/EC (General Data Protection Regulation), EUR-Lex document ST_5419_2016_ADD_1_REV_1, p. 4.
[22] Communication from the Commission to the European Parliament pursuant to Article 294(6) of the Treaty on the Functioning of the European Union on the position of the Council on the adoption of a regulation of the European Parliament and of the Council on protection of natural persons in relation to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and repealing Directive 95/46/EC, EUR-Lex document 52016PC0214.
[23] Judgment of the Court of Justice of the EU of 15 July 2010 (ECLI:EU:C:2010:429), par. 51.
[24] Judgment of the Court of Justice of the EU of 10 March 2021 (ECLI:EU:C:2021:188), par. 78.
[25] Judgment of the Court of Justice of the EU of 14 June 2017 (ECLI:EU:C:2017:451), par. 26.
[26] Judgment of the Court of Justice of the EU of 03 October 2013 (ECLI:EU:C:2013:625), par. 50.
[27] Judgment of the Court of Justice of the EU of 22 September 1988 (ECLI:EU:C:1988:439), par. 19.
[28] In the same sentence, compare Article 32 of the GDPR with the decision of the Austrian supervisory authority of 22 December 2021 (as mentioned above).

of Article 44, as that interpretation would deprive the provision of its useful effect, despite the aforementioned case law of the Court.

66. Because Article 44 of the GDPR is clear in the opinion of the Dutch DPA, no weight is given to the significance of the system of the GDPR and the history of its development. But even if that were the case, what Takeaway argues would not lead to the interpretation of Article 44 it advocates. The Dutch DPA takes the following into account.

67. Takeaway's argument is based on the idea that Article 24 of the GDPR (which contains a risk-based approach) has a horizontal scope, meaning that this provision applies to all obligations of the controller. According to Takeaway, this also includes obligations under Chapter V of the GDPR. Takeaway points out a report by the then President of the European Council, Cyprus, who, in a written report dated 1 March 2013 on the development of the GDPR, mentioned the task of making specific proposals for a tightened risk-based approach in the text of the then draft regulation.[29] Although it follows from that report that various draft provisions have been reformulated on a risk-based basis, it does not follow from the report that this also applies to Chapter V of the GDPR. On the contrary, it explicitly follows from the report that this mainly concerns Chapter IV of the GDPR ("Controller and processor") and to a limited extent Chapter III ("Rights of the data subject"):

> *"Although Chapter IV of the Regulation provides the most scope for a risk-based approach, the Presidency has sought to introduce elements of this approach in parts of Chapter III (particularly Articles 12, 14 and 15) in order to ensure that rights of data subjects are exercised effectively and efficiently while at the same time improving certainty and transparency."*

68. It also does not unambiguously follow from the phrase "throughout the Regulation, a risk-based approach is introduced" in the Council's explanatory memorandum of 31 March 2016, which Takeaway further points out, that the legislator explicitly envisaged a risk-based approach when applying Chapter V. With Chapter V of the GDPR, the legislator aims to ensure that the level of protection for personal data applicable within the EU "moves" with exported data. The legislator has explicitly prescribed in Article 44 that this level of protection may not be undermined.

69. In view of the foregoing, even when the development history is taken into account, contrary to what Takeaway states, it cannot be concluded that the legislator intended that a risk-based approach be applied when applying Chapter V of the GDPR. That interpretation would actually undermine the explicit requirement that the guaranteed level of protection may not be undermined.

70. Takeaway's argument about Article 24 and its formation does not lead to the conclusion that the report wrongly concluded that the level of protection in the United States was inadequate at the time of the observed violation.

[29] Memorandum from the Presidency to the Council of 1 March 2013, EUR-Lex document number 6607/1/13 REV 1, can be consulted via <https://data.consilium.europa.eu/doc/document/ST-6607-2013-REV-1/nl/pdf>.

EDPB Recommendations 01/2020

Opinion

71. To further substantiate the argument that a risk-based test should be applied, Takeaway points out the method and content of the Recommendations. First of all, Takeaway notes that adjustments have been made to the text of the Recommendations as a result of the public consultation. The consultation version states that organisations should not "rely on subjective factors, such as how likely it is that public authorities will access the data in a manner that is not in accordance with European standards."[30] This passage was removed after the public consultation. Secondly, Takeaway points out margins 1, 2, 3, 4, 5, 43 and 43.3 of the Recommendations. Margin 43 states that the parties concerned must examine the admissibility of the transfer on the basis of the publicly available legislation of the third country, as well as the practices of the public authorities of the third country. Margin 43.3 of the Recommendations states that if the exporter and importer have no reason to believe that relevant and problematic legislation will be applied in practice, it may be decided not to take additional measures.

Assessment

72. The EDPB drew up the Recommendations following the Schrems II judgment. With these Recommendations, the EDPB aims to provide parties that transfer personal data with guidance on the complex task of assessing transfers of personal data to third countries and identifying where additional measures need to be taken. In margins 1 to 5 (which Takeaway points out, among other things), the EDPB states that the right to data protection is active in nature, and that parties who transfer personal data must go beyond mere recognition or passive compliance with this right. The Recommendations emphasise that after transfer, personal data must still be processed in a manner that corresponds to the level of protection under European law. The transfer of personal data to third countries should not be a means of undermining or weakening the protection afforded in the EEA.

73. Margins 43 and 43.3, which Takeaway further points out, are part of section 2.3 of the Recommendations ("2.3. *Assess whether the transfer instrument you use under Article 46 of the GDPR is effective in light of all the circumstances of the transfer*"). This step explains how to determine whether the transfer instrument used (in the case of Takeaway: using the provisions of a standard model contract) offers sufficient guarantees. Margins 32 and further state in detail which aspects must be assessed in any case. Margin 43 discusses the assessment of the law and practices of the third country in question. First of all, it is stated that the assessment must primarily and in particular be based on the legislation that is publicly available. In addition, it is stated that the assessment of the applicable practices in the third country are particularly important in a number of situations. One of those situations, described in margin 43.3, is that "The assessment may show that the relevant legislation in the third country may be problematic and that the data transferred and/or the importer in question falls or may fall within the scope of this problematic legislation." If that is the case, according to the Recommendations it can be decided to:

[30] Consultation version of Recommendations 01/2020 of 11 November 2020, EDPB consultation reference R01/2020.

- suspend the transfer;
- take additional measures to avoid the risk that the laws and/or practices of the third country of the data importer are applied to the importer and/or to the data transferred; or
- continue with the transfer without taking additional measures, if the exporter believes it has no reason to believe that relevant and problematic legislation will be applied in practice to transferred data and/or the importer.

74. In the latter case, a detailed report must demonstrate and document that the legislation is not, in practice, interpreted and/or applied in a manner that would affect the data transferred and the importer, so that the legislation will not prevent the importer from fulfilling its obligations under the transfer instrument of Article 46 of the GDPR. Margins 44 to 47 of the Recommendations state which sources can be used and what requirements are imposed on those sources and the assessment. The sources must, among other things, be relevant, objective, reliable, verifiable and publicly available or otherwise accessible. The exporter must assess and document whether this is the case.

75. Takeaway first stated in its opinion that, prior to the implementation of Analytics, it assessed whether Google could provide sufficient guarantees with regard to, among other things, data protection. Takeaway states that it has assessed security measures and has received a confidential assessment of the level of protection offered by Google. According to Takeaway, this shows that Google does not consider it obvious that it falls under the surveillance laws of the United States with regard to Analytics and that Google claims that it has not received a FISA warrant in fifteen years. After studying this information, Takeaway came to the conclusion that it could implement Analytics.

76. The Dutch DPA believes that merely examining information from the importer in the third country is not sufficient to meet the requirements of Article 46 of the GDPR and the related Recommendations. Apart from the fact that Takeaway does not state that it has demonstrated and documented with a detailed report that the problematic legislation applies to the personal data transferred – which is a first condition – it is not sufficient to refer to a confidential document from the importer. What is required is that the information used in the assessment must be relevant, objective, reliable, verifiable and publicly available or otherwise accessible. That is not the case here.

77. Takeaway's argument about the Recommendations also does not lead to the conclusion that the report wrongly concluded that the level of protection in the United States was inadequate at the time of the observed violation.

Conclusion

78. The Dutch DPA does not follow Takeaway in its argument that the conclusion in the investigation report on the level of protection of personal data in the United States was incorrectly determined because an incorrect assessment method was used. The report rightly concluded that additional measures are necessary to provide a level of protection that is equivalent to the level of protection of the GDPR.

2.4.6. Additional measures

Investigation report

79. The investigation report concludes that the Court does not sufficiently guarantee the level of protection of personal data in the United States to allow the transfer to be based on standard provisions alone. Google is a provider of electronic communications services within the meaning of § 50 U.S. Code 1881 (4) (b) and is obliged to provide personal data to the American intelligence services. Therefore, transfer can only take place if adequate additional safeguards are in place.

80. As mentioned in section 2.4.1, the investigation report found that Takeaway and Google have taken various additional measures. These can be divided into technical, contractual and organisational measures. The technical measures consist of Takeaway [redacted] and obtaining information from Google about the secure transfer of JavaScript and measurement data, HTTP Strict Transport Security (HTST) and encryption of data between Google data centres. Takeaway further points out that Google (with regard to the Analytics service) has an ISO 27001 certificate.

81. The report further mentions that Google states that it has taken additional contractual and organisational measures. Google points out that every request from intelligence services to provide user data is carefully assessed and complies with the law and the proportionality requirement. If permitted, Google will inform the user concerned of the provision. In addition, Google periodically publishes a transparency report, which contains information about requests from security services. Google also publishes its own policy on handling such requests and information about data protection.

82. The report also discusses technical measures that Google is said to have taken. For example, Google states that it has taken safeguards for the protection of data during transport, such as upgrading connections to encrypted connections to prevent passive monitoring. When data is outside Google's control area (for example, traffic between data centres), the data is encrypted. Data is also encrypted in storage. Each data centre is protected with six layers of physical security to prevent unauthorised access. Access to data by staff is limited to what is needed for his or her position. Lastly, Google indicates that Analytics data is pseudonymised. Access by third parties will therefore normally not provide the opportunity to identify a data subject based on that data.

83. The report concluded that these additional measures do not actually prevent or reduce the ability of American intelligence services to gain access. Google is obliged to cooperate with those requests, while the Court has ruled that the legally permissible requests in the United States are not in line with European data protection requirements. With regard to encryption of data "*in transit*" and "*at rest*", it is noted that Google is obliged to hand over the crypto keys to American intelligence services when asked. As long as Google has the ability to access the data in legible text, encryption cannot be an effective measure. Lastly, regarding the anonymisation of IP addresses, it is stated that this happens after the IP address has been transferred to the United States. This means that there is still a possibility that security services have

access to all data.

84. The additional measures taken were therefore not found to be effective in the report, which means Takeaway cannot rely on the transfer instrument of standard provisions. This means that at the time of the period investigated, a transfer of personal data took place without being based on a valid transfer instrument, resulting in Takeaway having violated Article 44 of the GDPR.

Opinion

85. In its opinion, Takeaway has not disputed the conclusion in the investigation report that Google's additional measures are insufficient to prevent or reduce access by the American intelligence services. Instead, Takeaway has pointed out some other additional measures that it has taken itself. Takeaway explained these measures in more detail during the opinion hearing. In response to questions from the Dutch DPA about these measures, Takeaway has discussed the operation of these measures in the supplementary opinion. The measures consist (in summary) of using a proxy server, [redacted].

86. Takeaway's explanation shows that it started using a proxy server [redacted]. The result of this is that there is no direct flow of information between the website visitor and Google. Instead, first, there is a flow of information between the website visitor and Takeaway, and then between Takeaway and Google. This allows Takeaway to determine what information about the website visitor is provided to Analytics.

87. [redacted][31].

Assessment and conclusion

88. The use of a proxy server to exclude direct contact between the website visitor and Google and to filter or change transferred personal data is a measure aimed at the pseudonymisation of personal data as referred to in Article 4, opening words and (5) of the GDPR.

[31] [dropped].

89. As mentioned in the EDPB Recommendations discussed above, pseudonymisation of personal data can be an effective additional measure in the event of an international transfer of personal data.[32] For this to be the case, however, a number of conditions must be met. For example, the data exporter must first transfer the processed personal data in such a way that the personal data can no longer be linked to a specific data subject or used to single out the data subject in a larger group, without additional data. Secondly, this additional data (necessary for re-identification) must be held solely by the exporter and kept separately in an EU Member State or in a third country (in which case such transfer must also be in accordance with Chapter V of the GDPR). Thirdly, the disclosure or unauthorised use of such additional data should be prevented by appropriate technical and organisational safeguards and the exporter should have sole control over the data on the basis of which the pseudonymised personal data can be re-identified. Lastly, the controller must have determined, through a thorough analysis of the personal data in question - taking into account possible information that the public authorities of the receiving country could be expected to have and use - that the pseudonymised personal data cannot be attributed to the data subject, even if such information is merged and compared with the personal data.

90. The Recommendations further state that it should be taken into account that in many situations, a natural person can also be identified on the basis of elements that are characteristic of, among other things, the physical, economic, cultural or social identity of that natural person, their physical location, or their interaction with an Internet service at certain times, even if other identifying information is omitted. This is especially true when the data relates to the use of information services (time of access, order of functions accessed, characteristics of the device used, etc.).

91. The additional measures taken by Takeaway, consisting of using a proxy server [redacted], should in terms of their effectiveness[33] and appropriateness[34] be assessed on the basis of the criterion set out in the previous margins.

92. [redacted]

[32] Margins 85 et seq. of the Recommendations.
[33] As referred to in the Recommendations.
[34] As referred to in recital 20 and provision 14 of Decision (EC) of 4 June 2021 establishing new standard contractual clauses. This 'appropriateness' is understood in relation to its effectiveness according to the standards of the Recommendations and Schrems II. This does not concern 'appropriateness' as laid down in Article 46 of the GDPR, because the latter concept constitutes the relative appropriateness *between the different transfer instruments* for the specific transfer situation.

[redacted][35] [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted].

93. To assess whether the additional measures are effective, it is noted that the degree of identifiability (the likelihood that the data can be linked to a natural person) is related to both the *amount* and the *nature* of the data. Stopping the transfer of certain categories of data [redacted], in itself has an increased protection effect. Nevertheless, Takeaway has continued to pass on a still extensive set of data. In view of the data transferred by Takeaway after implementing the additional measures, the Dutch DPA believes that re-identification cannot be sufficiently ruled out. The Dutch DPA takes into account that:

- [redacted]. In combination with the other data, re-identification is a very real possibility;
- the series of transferred data is still extensive and the sum of the various data makes the chance of identification high. This concerns data such as [redacted] that can be significant when combined in view of the identity elements stated in margin 90; and
- with regard to this data, according to the Recommendations,[36] the possibility that identification takes place through the combination of the pseudonymised data in the hands of Google and additional data in the hands of the American intelligence services must also be taken into account.

94. Since re-identification has not been sufficiently ruled out, Takeaway's use of the proxy server to pseudonymise the data is not sufficient and is therefore not appropriate and effective as an additional measure. Given the remaining uncertainties regarding *ex post* identification by the intelligence services, another opinion would not be consistent with the high level of protection the GDPR aims to guarantee.

95. The conclusion is that the transfer of personal data by Takeaway could not be based on the appropriate safeguards referred to in Article 46 of the GDPR.

3. Violation

96. Section 0 of this decision concludes that Takeaway is the controller for the implementation of Analytics. Section 2.2 concludes that Takeaway processes personal data in this context and that

[35] [redacted].
[36] See margin 85.

international transfer of personal data takes place. Section 0 concludes that in the period from 18 August 2020 to 1 September 2023, Takeaway was responsible for having a valid transfer instrument for the processing as laid down in Chapter V of the GDPR. Section 2.4.6 concludes that the transfer during that period was not based on a valid transfer instrument. This means that Takeaway violated Article 44 of the GDPR during that period.

4. Enforcement measure to be imposed

97. The Dutch DPA is authorised to impose corrective measures, including a warning, reprimand and administrative fine (Article 58(2) of the GDPR). These measures are not mutually exclusive and can therefore be imposed side by side. The question of whether to impose a fine should take due account of the factors set out in Article 83(2) of the GDPR. Those factors include, among other things, the nature, seriousness and duration of the infringement (factor a) and any other aggravating or mitigating circumstance applicable to the circumstances of the case (factor k)

98. With regard to factor a (nature, severity and seriousness of the infringement), the Dutch DPA notes that Takeaway, as stated in margin 96, has transferred personal data to a third country in violation of Article 44 of the GDPR, while that transfer was not based on a valid transfer instrument. This is a serious violation and counts as an aggravating circumstance.

99. However, in the light of factor k (any other circumstance applicable to the circumstances of the case), the Schrems II judgment has created a very specific situation. The Court declared the adequacy decision for the United States invalid, after which it took quite some time before the EDPB issued its Recommendations offering tools to deal with the newly created situation. Furthermore, the Dutch DPA has established that, in addition to the use of standard provisions, Takeaway has taken additional measures in the form of, among other things, a proxy server. [redacted]. Takeaway has thus demonstrably made significant efforts to guarantee the level of protection of personal data. The measures taken actually increase protection, although in the opinion of the Dutch DPA, this is not sufficient to rule out re-identification. The situation created by the Schrems II judgment and Takeaway's efforts to deal with it count as mitigating circumstances.

100. Given the circumstances of this specific case, the Dutch DPA sees reason to refrain from imposing an administrative fine in this case. The Dutch DPA will suffice by imposing a reprimand for the observed violation.

Datum
20 August 2024

Ons kenmerk
z2022-04011

5. Decision

The Dutch DPA imposes a reprimand on Takeaway Group B.V. for violating Article 44 of the GDPR in the period from 18 August 2020 to 1 September 2023 by transferring personal data to a third country during that period, while such transfer was not based on a valid transfer instrument.

Sincerely,
The Dutch DPA,

[redacted]

Remedy clause

If you do not agree with this decision, you can submit a digital or paper notice of objection to the Dutch DPA within six weeks of the day on which the decision was sent. To submit a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Contact, item "Objection or complaint about the Dutch DPA".

Send your paper notice of objection to:

Dutch DPA
(Autoriteit Persoonsgegevens)
Postbus 93374
2509 AJ Den Haag, the Netherlands

Please quote 'Awb objection' on the envelope and use 'notice of objection' in the title of your letter.

Your notice of objection must at least contain:

- your name and address;
- the date of your notice of objection;
- the reference mentioned in this letter (case number); or attach a copy of this decision;
- the reason(s) why you do not agree with this decision;
- your signature.