Republik Österreich
Datenschutz behörde
E-mail: dsb@dsb.gv.at

Barichgasse 40-42
A-1030 Vienna
Tel.: +43-1-52152 302565

GZ: [redacted] : [redacted]

[redacted]
zH noyb - European Center for Digital Rights

Goldschlagstrasse 172/4/3/2
1140 Vienna

Data protection complaint (Art. 77 (1) DSGVO)
[redacted], represented by NOYB/1st [redacted] and 2nd Google LLC

E-mail legal@noyb.eu

T E I L B E C A U S E

S P R U C **H**

The data protection authority decides on the data protection complaint of [redacted] (complainant) of 18 August 2020, represented by NOYB - European Centre for Digital Rechte, Goldschlagstraße 172/4/3/2, 1140 Vienna, ZVR: 1354838270, against 1) [redacted] (first respondent), represented by [redacted] and 2) Google LLC (second respondent), 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA, represented by [redacted], [redacted], for a violation of the general principles of data transfer pursuant to Art. 44 DSGVO as follows:

1. The decision of the data protection authority of 2 October 2020, [redacted], is rectified.

2. The appeal against the first respondent is upheld and it is held that

   a) the first respondent as the responsible party by implementing the tool "Google Analytics" on their website at [redacted] at least on 11 August. 2020 personal data of the complainant (these are at least

unique user identification numbers, IP address and browser parameters) to the second respondent,

b) the standard data protection clauses concluded by the First Respondent with the Second Respondent do not provide an adequate level of protection pursuant to Art. 44 GDPR offer, as

i) Second Respondent qualifies as an electronic communications service provider within the meaning of 50 U.S. Code § 1881(b)(4) and, as such, is subject to U.S. intelligence surveillance pursuant to 50 U.S. Code § 1881a ("FISA 702"); and

ii) the measures taken in addition to the standard data protection clauses mentioned in point 2. b) are not effective as they do not eliminate the possibilities of surveillance and access by US intelligence services,

c) in the present case, no other instrument pursuant to Chapter V of the GDPR can be used for the data transfer referred to in point 2.a) and the first respondent has therefore not ensured an adequate level of protection pursuant to Art. 44 GDPR for the data transfer referred to in point 2.a).

3. The complaint against the second respondent for a breach of the general principles of data transfers pursuant to Art. 44 GDPR is dismissed.

Legal basis: Art. 4 Z 1, Z 2, Z 7, Z 8 and Z 23 lit. b, Art. 5, Art. 44, Art. 46 par. 1 and par. 2 lit. c, Art. 51 para. 1, Art. 56 para. 1, Art. 57 para. 1 lit. d and lit. f, Art. 60 para. 7 and para. 8, Art. 77 para. 1, Art. 80(1) and Art. 93(2) of Regulation (EU) 2016/679 (General Data Protection Regulation, DSGVO), OJ No. L 119, 4.5.2016 p. 1; Sections 18(1) as well as 24(1), (2)(5) and (5) of the Data Protection Act (DSG), Federal Law Gazette I No. 165/1999 as amended; Section 68(2) of the General Administrative Procedure Act 1991 (AVG), Federal Law Gazette 51/1991 as amended.

C O N S I D U C A T I O N

A. Arguments of the parties and course of the proceedings

A.1 In its submission of 18 August 2020, the complainant submitted, in summary, the following:

He had visited the first respondent's website at [redacted] 11 August 2020 at 1:46:00. During the visit, he was logged into his Google account, which was linked to the complainant's email address. The first respondent had embedded HTML code for Google services (including Google Analytics) on its website. In the course of the visit, the first respondent had processed personal data,

namely at least the complainant's IP address and cookie data. In the process, some of these data had been transmitted to the second respondent. Such a transfer of data required a legal basis according to Art. 44 et seq. of the GDPR.

Following the ECJ's judgment of 16 July 2020, Rs C-11/18 ("Schrems II"), the respondents could no longer rely on a data transfer to the US for a
adequacy decision ("Privacy Shield") under Article 45 GDPR. The first respondent was also not allowed to base the data transfer on standard data protection clauses if the third country of destination did not provide an adequate level of protection under EU law.
Protection of personal data transferred on the basis of standard data protection clauses
data . The second respondent was , as a provider of electronic data communications services within the meaning of 50 U.S.Code § 1881(b)(4) and, as such, is subject to surveillance by U.S. intelligence agencies pursuant to 50 U.S.Code § 1881a ("FISA 702"). The Second Respondent actively provides personal information to the U.S. Government pursuant to 50 U.S.Code § 1881a.

Consequently, the respondents were not in a position to ensure adequate protection of the complainant's personal data when his data were transferred to the second respondent. The transfer of the complainant's data to the USA was unlawful. Several enclosures were attached to the complaint.

A.2 In its submission of 22 December 2020, the first respondent made the following points in summary:

The programme code for the Google Analytics tool had been embedded on [redacted] Without consent, however, the code would not be played by the web server. The first respondent was only domiciled in Austria and had no other branches in other Member States. It operated the following European versions of the website, on which the tool was also embedded in the same form: [redacted], [redacted], [redacted] and [redacted].

The tool is used to enable general statistical evaluations of the behaviour of website visitors. However, the tool does not allow the content or search queries to be adapted to a specific website user, as the analysis is carried out anonymously and no reference to a specific user is made possible. User IP addresses are also anonymised before storage or transmission ("IP anonymisation"). The function "anonymizeIP" was set to "true". This guaranteed anonymisation before the data was stored. The code for this tool was currently still available on the websites.

Insofar as the GDPR was applicable, the first respondent was the controller and the second respondent was the processor. A processor agreement had been concluded. As no personal data were transferred, the ECJ's judgment of 16 July 2020 in Case C-311/18 was not relevant. However, in order to take precautions for a possible transfer of personal data to the second respondent - e.g. in the event that IP anonymisation is deactivated due to a data breach - the first respondent had concluded a processor

agreement with the second respondent and included standard data protection clauses (SDC). This had been implemented purely as a precautionary measure. The second respondent had implemented further technical and organisational measures to provide a high level of data protection for the data processed via the tools. Several enclosures were attached to the statement.

A.3 In its observations of 12 February 2021, the complainant submitted, in summary, the following:

The IP address processed first would - if at all - only be anonymised afterwards in a second step. This anonymisation, which may take place after transmission, does not affect the previous processing. The opinion contains a more detailed technical description at this point. If the first respondent was convinced that no personal data were processed, it would be absurd to conclude processing conditions. Several enclosures were attached to the statement. A declaration was requested that the data transfers in question were unlawful within the meaning of Article 44 et seq. of the GDPR.

A.4 The data protection authority requested the second respondent in a decision of 3 May 2021 as follows (formatting not reproduced 1:1):

*"**Subject: I. Data protection complaint pursuant to Article 77(1) of the GDPR against Google LLC; II. Concerning the questionnaire of 9 April 2021***

I. Data protection complaint pursuant to Art. 77 (1) DSGVO against Google LLC

*Please find attached a data protection complaint dated 18 August 2020 pursuant to Art. 77 para. 1 GDPR by MB (complainant), represented by NOYB, an organisation pursuant to Art. 80(1). GDPR, against 1. [redacted] (first respondent) and 2. **Google LLC** (second respondent). In addition, a statement of the first respondent dated 16 December 2020 is submitted.*

The subject of the complaint is the use of the Google Analytics tool by the first respondent on its website. Google LLC is explicitly named as the second respondent. A violation of the requirements for international data traffic (Chapter 5 of the GDPR) is alleged.

You will be given the opportunity to comment on this complaint within a period of three weeks from receipt of this letter.

II. About the questionnaire of 9 April 2021

Google LLC has already completed a questionnaire of the data protection authority on the topic of Google Analytics in a parallel pending complaint procedure on case number DSB-D155.027 and submitted corresponding answers to the data protection authority in a letter dated 9 April 2021.

It is noted that Google's statement of 9 April 2021 is formulated in such a way that the explanations are also transferable to [redacted] complaint proceedings against [redacted] relevant here.

Consequently, the data protection authority plans to grant the parties involved in the present proceedings a hearing on the letter of 9 April 2021 from Google LLC.

If you have any objections to this procedure, you are requested to notify us within a period of three weeks from receipt of this letter.

When making submissions to the data protection authority, please quote reference DSB-D155.026."

A.5. In its statement of 28 May 2021, the first respondent submitted the following in summary:

The programme code for the Google Analytics tool that was the subject of the proceedings had been removed as of 25 May 2021. The use of Google Analytics on the [redacted] website had thus been discontinued. A procedure pursuant to section 24 (6) of the Data Protection Act (informal discontinuation) is suggested.

A.6. In his observations of 8 June 2021, the complainant submitted the following in summary:

The facts of the case were in the past and self-contained, and the removal of the programme code did not change the complainant's complaint. The data in question had already been transmitted in violation of Article 44 et seq. of the GDPR. A corresponding finding was requested.

A.7. By settlement of 25 June 2021, the data protection authority sent the complainant and the first respondent the previously mentioned opinion of the second respondent of 9 April 2021.

A.8. In its statement of 6 August 2021, the first respondent submitted the following in summary:

She had used the free version of Google Analytics. In doing so, she had agreed to the terms of use and the SCC. The data exchange setting had not been activated. Google Signals had also not been used. In connection with the use of Google Analytics, the exemption according to Article 49 (1) of the GDPR had not been relied on.

A.9. In his observations of 13 August 2021, the complainant submitted the following in summary:

The complainant referred to the opinion of 5 May 2021 on the parallel proceedings on case no. DSB-D155.027. As in the parallel proceedings, it could be seen from the HAR file transmitted that the complainant's personal data had been processed and that the data had been transferred to Google LLC in the USA.

A.10. In its statement of 23 August 2021, the first respondent submitted the following in summary:

The first respondent was the operator of the comparison portal [redacted] It operates [redacted] in the following language versions: [redacted] and [redacted].

A.11. In its statement of 2 November 2021, the second respondent submitted the following in summary:

The IP address and the cookie data complained of were not personal data.
Data. The IP anonymisation function had been activated. The data had been sent to the
The complainant could also not be identified. The complainant had not explained which IP address had been used by the internet-connected device with which he had visited the website. It was also unclear whether it had been a dynamic or static IP address.

However, even assuming the existence of personal data, a risk-based approach should be taken when assessing the appropriateness of the transfer to the US. This is clear from the
"Schrems II" FAQ of the EDSA as well as from the decision of the European Commission of 4 June 2021 on the new standard contractual clauses. In the present case, it had to be taken into account that the transmission of the data at issue in the proceedings entailed only a low basic risk, if any at all. There was also no disclosure pursuant to EO 12.333, since the aforementioned
provision does not authorise the U.S. government to compel or even request user data from a U.S. provider, it does not receive requests directed to service providers outside the U.S.. FISA § 702 is also irrelevant in light of the encryption and anonymisation of IP addresses. The second respondent had entered into standard contractual clauses with the first respondent. In addition, it had implemented supplementary measures to complement the standard contractual clauses.

Finally, it should be noted that a violation of Art. 44 et seq. of the GDPR cannot be asserted in the context of a data protection complaint. The data protection authority also has no competence to determine violations of the law in the past. Moreover, Art. 44 et seq. of the GDPR only apply to data exporters.

A.9 In its observations of 3 December 2021, the complainant submitted, in summary, the following:

Personal data had been processed, as evidenced by the enclosures submitted. A statement on the account configuration in the Google account had already been submitted in the parallel proceedings on DSB-D155.027.

The IP anonymisation in question only takes place after the transmission into the sphere of
Google LLC. The fact that this also takes place within the EEA is a mere assertion which the first respondent, as the accountable controller, must prove. Moreover, it was not decisive for the possibility of access by US authorities that personal data actually leave the EEA geographically. 50 U.S. Code § 1881a ("FISA 702") is not limited to data processed geographically in the U.S., but claims global application.

Furthermore, it should be noted that the combination of cookie data and IP addresses in particular could enable tracking and the evaluation of geographical localisation, internet connection and context of the visitor to be linked to the cookie data already described. The GDPR also does not know of any "risk-based approach" in Chapter V. This can only be found in certain articles of the GDPR, such as Art. 32 leg.cit.

Even if the second respondent had not violated Art. 44 et seq. of the GDPR, the provisions pursuant to Art. 28 (3) lit. a and Art. 29 of the GDPR had to be taken into account as a "catch-all provision". If the respondent to the second complaint complies with a corresponding instruction of a US intelligence service, it thereby takes the decision to process personal data beyond the specific order of the respondent to the first complaint pursuant to Art. 28 and Art. 29 GDPR and the corresponding contractual documents. This would make the second respondent itself a controller under Article 28(10) of the GDPR. As a result, the respondent must also comply with the provisions of Art. 5 et seq. of the GDPR. A secret transfer of data to US intelligence services in accordance with US law was undoubtedly not compatible with Art. 5(1)(f) of the GDPR, Art. 5(1)(a) of the GDPR and Art. 6 of the GDPR.

A.10. In its observations of 21 December 2021, the first respondent submitted the following in summary:

As already explained, it had not used Google Signals. As the technical service provider, the second respondent had expressly stated in its statement of 2 November 2021 that IP anonymisation only took place within the EEA. Only in exceptional cases would web servers outside the EEA be used. In the present case, normal operating conditions were present.

A.11. In its statement of 9 February 2022, the second respondent essentially repeated the previous submission.

It was also argued that the complainant's position had particularly serious and far-reaching practical consequences. This position would cause serious damage to Austrian companies operating on the world market as well as to the European economy as a whole. The web browser-related data at issue in the proceedings was not sufficiently specific to "single out" a browser. US intelligence agencies have never issued a FISA 702 order with respect to the type of Google Analytics data at issue.

It was inadmissible to assume the application of a reversal of the burden of proof to the question of the personal reference of the data. The GDPR does not know such a reversal of the burden of proof. Furthermore, this was incompatible with the principles of Austrian procedural law and the presumption of innocence.

Moreover, there is no right of association in Austria under Article 80(2) of the GDPR and this cannot be circumvented by having NOYB mandated by one of its employees for the purpose of conducting a "test case".

Two documents were attached to the statement.

A.9 In its last opinion of 1 March 2022, the complainant essentially repeated its previous submission.

B. Subject matter of the appeal

B.1 On the basis of the complainant's submissions, it can be seen that the subject matter of the complaint is the question whether the first respondent ensured an adequate level of protection pursuant to Article 44 GDPR for the transfer of the complainant's personal data to the second respondent, which was triggered due to the implementation of the Google Analytics tool on its [redacted]website.

Thus, the complainant, inter alia, in statements of 11 February 2021 and 8 June 2021, expressly requested a declaration pursuant to Section 24(2)(5) DPA that the data transfers at issue were unlawful under Article 44 DPA.

B.2 In this context, it must also be clarified whether, in addition to the first respondent (as data exporter), the second respondent (as data importer) was also obliged to comply with Art. 44 GDPR.

B.3 There is no need to rule on the request to impose an immediate ban on the data transfers to the second respondent against the first respondent (as the responsible party), as the latter has removed the Google Analytics tool from its website in the meantime.

B.4 Finally, it should be noted that the partial decision in question does not address the alleged violations of the second respondent pursuant to Art. 5 et seq. in conjunction with Art. 28 (3) lit. a and Art. 29 GDPR. Further investigative steps are necessary in this regard and will be discussed in a further decision.

C. Findings of fact

C.1 The first respondent was in any case the operator of the [redacted]service in August 2020. [redacted] is an online comparison portal where products can be compared with each other. In this way, consumers can find the cheapest provider for a specific product, which is listed by the first respondent.

The first respondent operates the [redacted]website for the Austrian market.
Furthermore, the first respondent [redacted]also operates for the German market ([redacted]), the English-speaking market ([redacted]the Polish market ([redacted]) and the market in the United Kingdom ([redacted]). The first respondent is only established in Austria and has no other establishments in other Member States of the Union.

Evaluation of evidence regarding C.1: The findings made are based on the first respondent's statement of 22 December 2020 (question 2) and were not contested by the complainant. Furthermore, the

findings made are based on an official search by the data protection authority under [redacted] (queried on 18 March 2022).

C.2 The second respondent has developed the Google Analytics tool. Google Analytics is a measurement service that allows clients of the second respondent to measure, among other things, traffic characteristics. This includes measuring the traffic of visitors who visit a specific website. This makes it possible to track the behaviour of website visitors and measure how they interact with a specific website. Specifically, a
Website operators can set up a Google Analytics account and use a dashboard to generate reports on the
website. Similarly, Google Analytics can be used to measure and optimise the effectiveness of advertising campaigns that website owners run on Google ad services.

There are two versions of Google Analytics: a free version and a paid version called Google Analytics 360. In any case, the free version was provided by the second respondent until the end of April 2021. Since the end of April 2021, both Google Analytics versions are provided by Google Ireland Limited.

Evaluation of evidence regarding C.2.: The findings made are based on the statement of the of 9 April 2021 (p. 3 as well as questions 1 and 2) and were not answered on the part of the complainant is not disputed. The second respondent's statement of 9 April 2021 was originally obtained in a parallel proceeding for reference number [redacted] and brought to the attention of the parties to the present proceedings, as the statement concerns general comments on the functioning of Google Analytics.

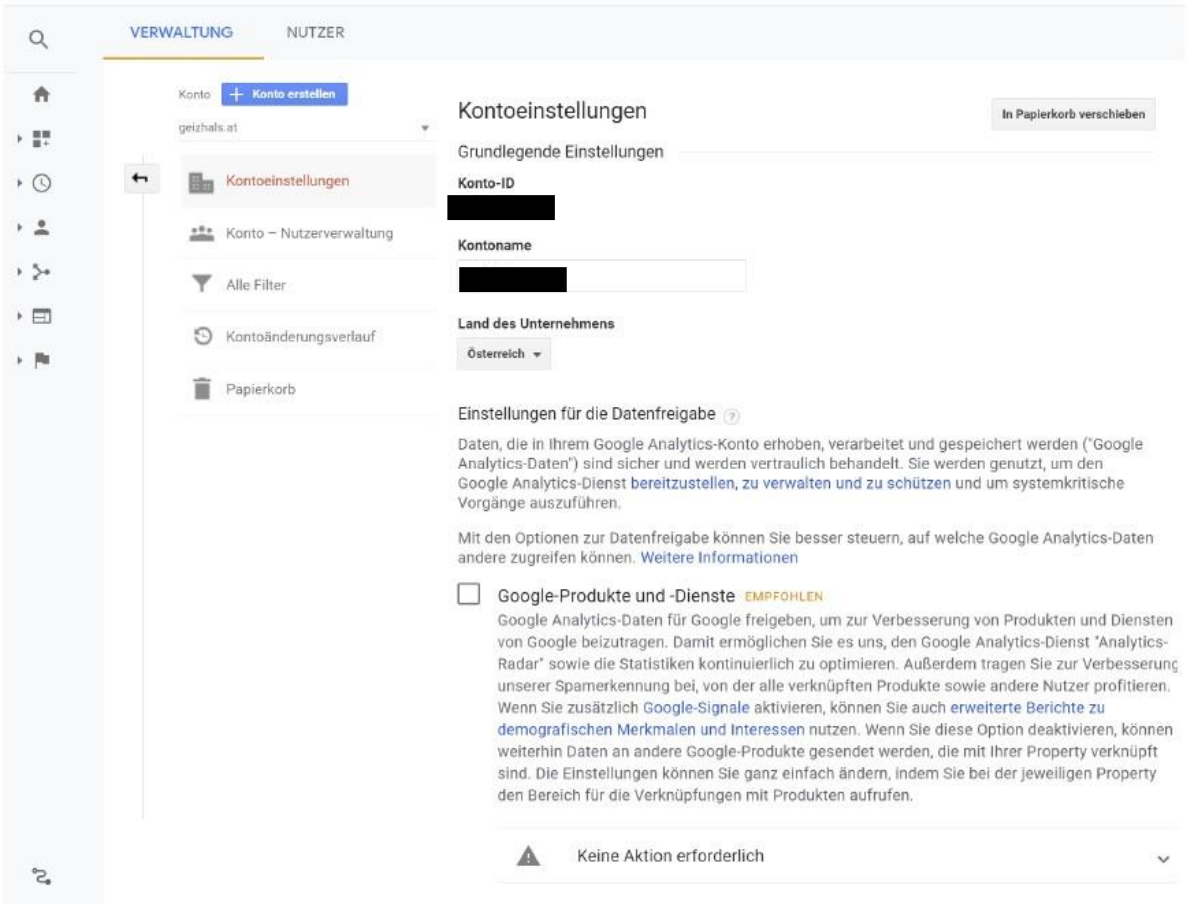
C.3 The first respondent - as website operator - has in any case on the cut-off date of 11 August 2020 decided to use the free version of the Google Analytics tool for their "[redacted]" websites. websites. For this purpose, it has used a JavaScript code ("tag"), which on the part of the
second respondent, built into the source code of its website. The first respondent used the tool to enable general statistical evaluations of the behaviour of website visitors. The additional tool Google Signals was not activated.

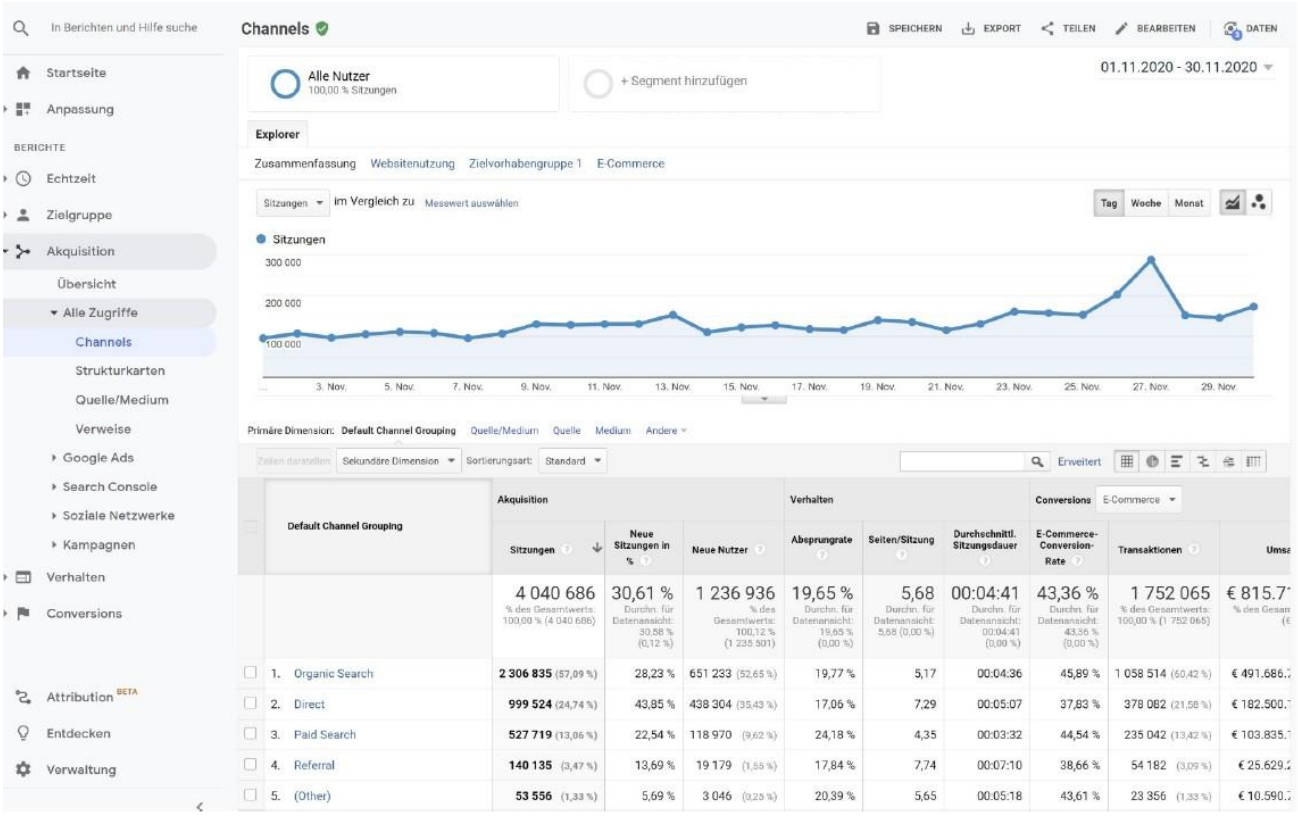
In any case, these evaluations are used by the first respondent to present the content of the [redacted] website according to the general interest in the topic in such a way that the most requested channels are placed in the foreground and the presentation can be adapted according to the topicality of a specific topic.

The first respondent has created a Google Analytics account for this purpose. The Google Analytics account ID with the account name "[redacted]" is [redacted]. The first respondent can carry out the above analyses by logging into the "[redacted]" Google Analytics account and viewing reports on [redacted] s traffic in the dashboard. The
Reports are divided into the categories real-time, target group, acquisition, behaviour and conversions.

The first respondent can select user-defined specifications for the report generation, the second respondent has no influence on this. The second respondent also has no influence on the extent to which the first respondent subsequently uses the reports created.

The dashboard is structured as follows (formatting not reproduced 1:1):





Evaluation of evidence regarding C.3: The findings made are based on the submission of the first respondent of 22 December 2020 and were not contested by the complainant. The screenshots cited were taken from the submitted enclosures . /B and ./D.

C.4. the Google Analytics tool works as follows: When visitors view the [redacted] website, JavaScript code inserted in the source code of the website refers to a JavaScript file previously downloaded to the user's device, which then performs the tracking operation for Google Analytics. The tracking operation retrieves data about the page request by various means and sends this information to the Analytics server via a list of parameters attached to a single pixel GIF image request.

The data collected by Google Analytics on behalf of the website operator originates from the following sources:

- the HTTP request of the user;
- Browser/system information; - (First-party) cookies.

An HTTP request for each website contains details about the browser and computer making the request, such as host name, browser type, referrer and language. In addition, the browser DOM interface (the interface between HTML and dynamic JavaScript) provides access to more detailed browser and system information, such as Java and Flash support and screen resolution. Google Analytics uses this information. Google Analytics also sets and reads

First-party cookies on a user's browsers that allow measurement of the user's session and other information from the page request.

When all this information is collected, it is sent to the Analytics servers in the form of a long list of parameters sent to a single GIF image request (the meaning of the GIF request parameters is described here) to the domain google-analytics.com. The data contained in the GIF request is that which is sent to the analytics servers and then further processed and ends up in the website operator's reports.

The information page of the second respondent on the Google Analytics tool contains the following excerpts (formatting not reproduced 1:1, retrieved on 18 March 2022):

gtag.js and analytics.js (Universal Analytics) - cookie usage

The analytics.js JavaScript library or the gtag.js JavaScript library can be used for Universal Analytics. In both cases, the libraries use *first-party* cookies to:

- Distinguish unique users
- Throttle the request rate

When using the recommended JavaScript snippet cookies are set at the highest possible domain level. For example, if your website address is `blog.example.co.uk`, analytics.js and gtag.js will set the cookie domain to `.example.co.uk`. Setting cookies on the highest level domain possible allows measurement to occur across subdomains without any extra configuration.

Note: gtag.js and analytics.js do not require setting cookies to transmit data to Google Analytics.

gtag.js and analytics.js set the following cookies:

Cookie Name	Default expiration time	Description
`_ga`	2 years	Used to distinguish users.
`_gid`	24 hours	Used to distinguish users.
`_gat`	1 minute	Used to throttle request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named `_dc_gtm_<property- id>`.
`AMP_TOKEN`	30 seconds to 1 year	Contains a token that can be used to retrieve a Client ID from AMP Client ID service. Other possible values indicate opt-out, inflight request or an error retrieving a Client ID from AMP Client ID service.
`_gac_<property-id>`	90 days	Contains campaign related information for the user. If you have linked your Google Analytics and Google Ads accounts, Google Ads website conversion tags will read this cookie unless you opt-out. Learn more.

<u>Evaluation of evidence regarding C.4.</u>: The findings made are based on the second respondent's statement of 9 April 2021 (question 2) in the parallel proceedings for reference number [redacted] *and an official search by the data protection authority at https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage and also https://developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id (both retrieved on 18 March 2022).*

C.5 The respondents entered into a contract entitled "Google Advertising Products Order Processing Terms". This contract was valid in the version of 1 January 2020 at least on 11 August 2020. The contract governs order processing conditions for "Google advertising products". It applies to the provision of processor services and related technical support services to customers of the second respondent. The aforementioned contract in the version of 1 January 2020 (statement of the respondent of 22 December 2020, Annex . /G) is used as the basis for the findings of fact. The said contract was subsequently updated on 12 August 2020 and 16 August 2020.

In addition, the first and second respondents entered into a second contract entitled "Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors". These are standard contractual clauses for international data traffic. This contract (respondent's statement of 22 December 2020, Annex . /K) also forms the basis for the findings of fact.

In the first contract, with regard to the services covered by the "Order processing conditions for Google advertising products", please refer to the link https://privacy.google.com/businesses/adsservices/. Under the aforementioned link, the following is displayed in excerpts (red highlighting on the part of the data protection authority, formatting not reproduced 1:1, queried on 18 March 2022):

Auftragsdatenverarbeitungsbedingungen:

Auftragsverarbeiterdienste

Die folgenden Google-Dienste fallen unter den Anwendungsbereich der Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte:

- Ads Data Hub
- Audience Partner API (frühere Bezeichnung: DoubleClick Data Platform)
- Campaign Manager 360 (frühere Bezeichnung: Campaign Manager)
- Display & Video 360 (frühere Bezeichnung: DoubleClick Bid Manager)
- Erweiterte Conversions
- Google Ad Manager-Auftragsverarbeiterfunktionen
- Google Ad Manager 360-Auftragsverarbeiterfunktionen
- Google Ads Kundenabgleich
- Google Ads Ladenverkäufe (direkter Upload)
- Google Analytics
- Google Analytics 360
- Google Analytics für Firebase
- Google Data Studio
- Google Optimize
- Google Optimize 360
- Google Tag Manager
- Google Tag Manager 360
- Search Ads 360 (frühere Bezeichnung: DoubleClick Search)

Google ist berechtigt, diese Liste gemäß den Bestimmungen der Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte zu aktualisieren.

Arten personenbezogener Daten

In Bezug auf die Auftragsdatenverarbeitungsbedingungen für Google Werbeprodukte (und abhängig davon, welche Auftragsverarbeiterdienste unter der jeweiligen Vereinbarung genutzt werden) können die folgenden Arten personenbezogener Daten personenbezogene Daten des Kunden darstellen:

Auftragsverarbeiterdienste	Arten personenbezogener Daten
Ads Data Hub	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen
Audience Partner API (frühere Bezeichnung: DoubleClick Data Platform)	Online-Kennzeichnungen (einschließlich Cookie-Kennungen) und Gerätekennungen
Campaign Manager 360 (frühere Bezeichnung: Campaign Manager)	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, präzise Standortdaten, vom Kunden vergebene Kennzeichnungen
Display & Video 360	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, präzise Standortdaten, vom Kunden vergebene Kennzeichnungen
Erweiterte Conversions	Namen, E-Mail-Adressen, Telefonnummern, Adressen, vom Kunden bereitgestellte Kennzeichnungen, Online-Kennzeichnungen (einschließlich Internet-Protokoll-Adressen)
Google Ad Manager-Auftragsverarbeiterfunktionen	Verschlüsselte Signale
Google Ad Manager 360-Auftragsverarbeiterfunktionen	Verschlüsselte Signale
Google Ads Kundenabgleich	Namen, E-Mail-Adressen, Adressen und vom Partner bereitgestellte Kennzeichnungen
Google Ads Ladenverkäufe (direkter Upload)	Namen, E-Mail-Adressen, Telefonnummern und Adressen
Google Analytics	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen
Google Analytics 360	Online-Kennzeichnungen (einschließlich Cookie-Kennungen), Internet-Protokoll-Adressen und Gerätekennungen, vom Kunden vergebene Kennzeichnungen

In addition to entering into standard contractual clauses, the second respondent has implemented further contractual, organisational and technical measures. These measures complement the obligations contained in the standard contractual clauses. The measures are described in the second respondent's statement of 9 April 2021 (question 28). This description is used as the basis for the findings of fact.

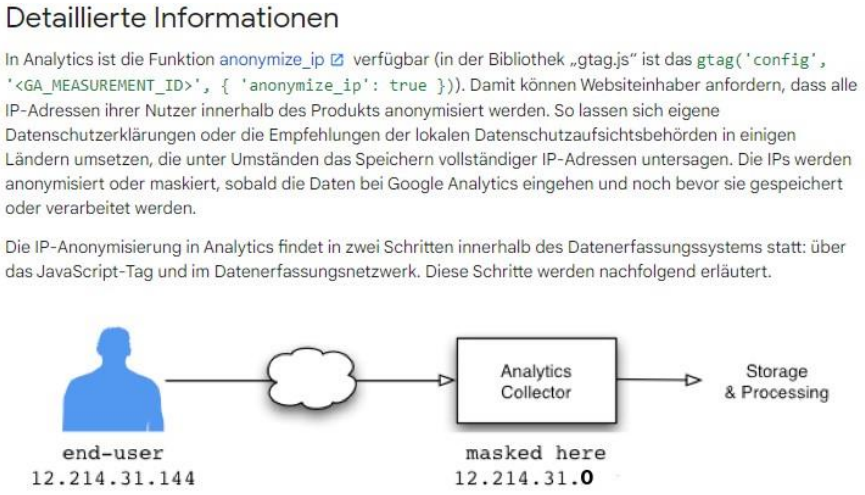
The second respondent regularly publishes so-called transparency reports on data requests from US authorities. These are available at: https://transparencyreport.google.com/user-data/us-national-security?hl=en

Evaluation of evidence regarding C.5: The findings made are based on the first respondent's statement of 22 December 2020, question 15. The enclosures cited are contained in the file and are known to all parties. Furthermore, the findings are based on an official search by the data protection authority at https://privacy.google.com/businesses/adsservices/ (retrieved on 18 March 2022). The findings made with regard to the "additional measures implemented" result from the second respondent's statement of 9 April 2021 (question 28) and the first respondent's statement of 22 December 2020 (question 23). The statement of the second respondent of 9 April 2021, which was obtained in the parallel proceedings on GZ: [redacted] contained in the file in question and is known to all parties. The

The following findings with regard to the transparency reports result from an official search of the Data Protection Authority at https://transparencyreport.google.com/user-data/us-nationalsecurity?hl=en (retrieved on 18 March 2022).

C.6 In the course of using the Google Analytics tool, the possibility is offered to use an "IP anonymisation function". This function was used by the respondent. As part of the embedding of Google Analytics on the website, the "anonymizeIP" function was set to "true". When loading the relevant scripts from Google servers, the full IP address of a website visitor is nevertheless initially transmitted to the second respondent. The IP address is only masked in a second step after it has been received by the Analytics data collection network.

In this regard, the second respondent has published on its website at https://support.google.com/analytics/answer/2763052?hl=de provided the following information (excerpt, formatting not reproduced 1:1):



<u>Evaluation of evidence regarding C.6</u>: The findings made are based on the statement of the first respondent of 22 December 2020 (question 2) and the enclosure . /C submitted therein. It can be seen from Exhibit . /C that the second respondent himself states that the anonymisation of the IP address only takes place in the second step after the data collection. The finding regarding the time of anonymisation of the IP address is furthermore based on the complainant's statement of 11 February 2021 (p. 2 f). Finally, the findings made are based on an official search of the website at https://support.google.com/analytics/answer/2763052?hl=de (queried on 18 March 2022). As can be seen from the legal assessment, it can be left open in the context of the findings of fact whether the IP address of the complainant's terminal was masked inside or outside the EEA area in the case at hand. Findings in this regard could therefore be omitted.

C.7 The complainant visited the [redacted] website at least on 11 August 2020. During the visit, he was logged into his Google account. A Google account is a user account that is used for authentication with various Google online services of the second respondent. For example, a Google account is a prerequisite for using services such as "Gmail" or "Google Drive" (a file hosting service).

Evaluation of evidence regarding C.7: The findings made are based on the complainant's submission of 18 August 2020 (p. 2 f) and were not disputed by the respondents. The findings made with regard to the basic functions of a Google search engine were not disputed by the respondents.
accounts are based on an official search by the data protection authority at https://support.google.com/accounts/answer/27441?hl=de and https://policies.google.com/privacy (both accessed on 18 March 2022).

C.8 In the transaction at issue between the complainant's browser and [redacted] on 11 August 2020, at 01:26:21.206 CET, unique user identification numbers were processed at least in the cookies "_ga" and _"gid". As a result, these
identification numbers on 11 August 2020, at 01:26:23.795 CET to https://www.googleanalytics.com/collect and thus to the second respondent.

Specifically, the following user identification numbers located in the complainant's browser were transmitted to the second respondent (identical values that occurred in different transactions have each been marked in green):

Domain	Name	Wert	Zweck
[redacted]	_ga	[redacted]	Google Analytics
[redacted]	_gid	[redacted]	Google Analytics

These identification numbers contain the UNIX timestamp at the end, which indicates when the respective cookie was set for the first time. The identification number with the UNIX timestamp "1597101359" was set on Tuesday, 11 August 2020 at 01:15:59 CET.

The same values as in the cookie files "_ga" and "gid" were contained in the request payload for the domain www.google-analytics.com/collect (emphasis added by the data protection authority):

[redacted]

With the help of these identification numbers, it is possible for the respondents to distinguish website visitors and also to obtain the information whether it is a new or a returning website visitor of [redacted]

In addition, the following information (parameters) was in any case also transmitted to the second respondent via the complainant's browser in the course of requests to https://www.google-analytics.com/collect (excerpt from the HAR file, request URL https://www.google-analytics.com/collect, excerpt of the request with timestamp 2020-0811T01:26:23.795+02:00):

General

[redacted]

Headers

[redacted]

- Host: www.google-analytics.com

[redacted]

[redacted]

[redacted]

- Headers 677 bytes
- Body 0 bytes
- Total 677 bytes

From these parameters, conclusions can thus be drawn about the browser used, the browser settings, language selection, the website visited, the colour depth, the screen resolution and the AdSense link number are pulled.

The remote address (IPV6 address) [redacted] that of the second respondent.

The IP address of the complainant's device is transmitted to the second respondent as part of these requests to https://www.google-analytics.com/collect.

The content of the HAR file (Annex . /4), which was submitted by the complainant in its submission of 18 August 2020, is used as a basis for the findings of fact.

Evaluation of evidence regarding C.8.: The findings made are based on the submission of the complainant of 18 August 2020 and the HAR file submitted therein, Annex . /4. A HAR file is an archive format for HTTP transactions. The HAR file was reviewed by the data protection authority. The complainant's allegations correspond to the archive data contained therein. The HAR file submitted (or its content) is known to the parties involved. Furthermore, the findings made are based on the complainant's statement of 13 August 2021 and the screenshots contained therein. As already stated above, according to the second respondent, the purpose of the identification numbers is to distinguish users. The established times of cookie setting are calculated from the respective UNIX timestamps. The Unix time is a time definition developed for the Unix operating system and established as a POSIX standard. Unix time counts the elapsed seconds since 00:00 UTC on Thursday, 1 January 1970. The determination with regard to the remote address results from an official Who-Is query of the data protection authority under [redacted] (queried on 18 March 2022).

C.9 To the extent that the Google Analytics tool is implemented on a website, the second respondent has the technical possibility to obtain the information that a certain Google Account user has visited this website (on which Google Analytics is implemented), provided that this Google Account user is logged into the Google Account during the visit.

Evaluation of evidence regarding C.9.: In his statement of 9 April 2021 in the parallel proceedings on case no. DSB-D155.027, the second respondent argued in question 9 that he only receives such information if certain requirements are met, such as the activation of specific settings in the Google account. In the opinion of the data protection authority, this argument is not convincing. If the wish of a Google account user for "personalisation" of the advertising information received can be complied with on the basis of a declaration of intent in the account, then from a purely technical point of view it is possible to receive the information about the website visited by the Google account user. In this context, explicit reference must be made to the accountability under data protection law, which will be discussed in more detail in the legal assessment. For the ascertainment of the facts, this accountability under data protection law means that the
respondent (or in any case the first respondent as the responsible party) - and not the complainant or the data protection authority - must provide sufficient proof. Such sufficient proof - i.e. that from a technical point of view there is no possibility for the second respondent to obtain data - was not provided in this context, especially since it is precisely an essential part of the concept of Google Analytics to be implemented on as many websites as possible in order to be able to collect data. As can be seen from the legal assessment, such a reversal of the burden of proof is explicitly provided for in the GDPR.

C.10. The first respondent removed the Google Analytics tool from its [redacted] website before the conclusion of the present proceedings.

Evaluation of evidence regarding C.10.: The findings made are based on the first respondent's statement of 28 May 2021, which was not contested by the complainant. Furthermore, the findings are based on an official search under [redacted] (retrieved on 18 March 2022).

D. In legal terms, it follows that:

D.1. general

a) The competence of the data protection authority

The European Data Protection Board (hereinafter: EDSA) has already addressed the relationship between the GDPR and Directive 2002/58/EC ("ePrivacy Directive") (see Opinion 5/2019 on the interaction between the ePrivacy Directive and the GDPR of 12 March 2019).

The data protection authority also dealt with the relationship between the GDPR and national implementation provisions in its decision of 30 November 2018, Zl. DSB-D122.931/0003-DSB/2018, dealt with the relationship between the GDPR and the national transposition provision (in Austria now: TKG 2021, Federal Law Gazette I No. 190/2021 as amended).

In principle, it was stated that the ePrivacy Directive (or the respective national implementation provision) takes precedence over the GDPR as *lex specialis.* Article 95 of the GDPR states that the Regulation does not impose any additional obligations on natural or legal persons with regard to processing in connection with the provision of publicly available electronic communications services in public communications networks in the Union, insofar as they are subject to specific obligations laid down in the ePrivacy Directive which pursue the same objective.

However, the ePrivacy Directive does not contain any obligations within the meaning of Chapter V of the GDPR in case of transfer of personal data to third countries or to international organisations.

Against this background, the GDPR applies to such a data transfer and the data protection authority is therefore competent to deal with the complaint in question pursuant to Art. 77(1) GDPR.

b) Regarding Art. 44 GDPR as a subjective right

Based on the previous practice of the data protection authority and the courts, it should be noted that both the lawfulness of data processing pursuant to Art. 5(1)(a) in conjunction with Art. 6 et seq. of the GDPR and the data subject rights postulated in Chapter III of the Regulation can be asserted as a subjective right in the context of a complaint pursuant to Art. 77(1) of the GDPR.

The transfer of personal data to a third country that does not (allegedly) ensure an adequate level of protection within the meaning of Art. 44 GDPR has not yet been the subject of a complaint in the context of a complaint procedure before the data protection authority.

In this context, it should be noted that Article 77(1) of the GDPR (and, incidentally, the national provision of Section 24(1) of the DPA) only requires that *"[...] the processing of personal data relating to them infringes this Regulation*" in order to exercise the right of appeal.

In its judgment of 16 July 2020, the ECJ also assumed that the finding that *"[...] the law and practice of a country do not ensure an adequate level of protection [...]"* as well as *"[...] the compatibility of this (adequacy) decision with the protection of privacy and the freedoms and fundamental rights of individuals [...]" in the* context of a complaint under Art. 77
(1) of the GDPR as a subjective right (cf. the ECJ judgment of 16 July 2020, C‑311/18 para 158).

It should be noted that the question referred for a preliminary ruling in the above-mentioned proceedings does not concern the "scope of the
right of appeal under Article 77(1) of the GDPR"; however, the ECJ has not
The fact that a breach of the provisions of Chapter V of the GDPR in the context of a
complaint under Article 77(1) of the GDPR is obviously considered a necessary precondition. Otherwise, the ECJ would have stated that the question of the validity of an adequacy decision cannot be clarified in the context of an appeal procedure.

Furthermore, to the extent that the second respondent contests the assertion of Art. 44 GDPR as a subjective right - with reference to the wording of Recital 141 of the Regulation - it must be countered that this Recital is linked to the fact that the "rights under this Regulation" are accessible to a complaint under Art. 77(1) GDPR. - it should be noted that this recital is linked to the fact that the "rights under this Regulation" are accessible to a complaint under Article 77(1) of the GDPR (and not, for example, "the rights under Chapter III of this Regulation").

Although the term "rights of a data subject" is used in certain places in the GDPR, this does not mean that other norms in which this formulation is not chosen cannot also be asserted as a subjective right. Most of the provisions of the GDPR are, on the one hand, an obligation of the controller (and partly of the processor), but on the other hand, they can also be asserted as a subjective right of a data subject. For example, it is undisputed that Art. 13 and Art. 14 GDPR establish a subjective right to information, although the right to information is not defined in Art. 12 para. 2 leg. cit. as "their rights" (i.e. "rights of the data subject") and Art. 13 and Art. 14 GDPR are designed according to their wording as a duty of the controller to provide information.

The decisive factor is whether an individual legal position of an affected person is impaired by an alleged infringement. The alleged infringement must therefore have a negative impact on the person concerned and affect him or her.

Apart from that, the recitals are an important instrument for the interpretation of the GDPR, but they cannot be used to reach a result that is in conflict with the text of the Regulation (here, as explained above, the fact that the administrative remedy is generally linked to "the processing") (cf. the ECJ judgment of 12 May 2005, C-444/03 para. 25 and the further case law cited there).

Finally, also according to the national case law of the Administrative Court, it is to be assumed in case of doubt that norms which prescribe an official procedure also and especially in the interest of the person concerned grant him a subjective right, i.e. a right that can be enforced by way of appeal (cf. e.g. VwSlg. 9151 A/1976, 10.129 A/1980, 13.411 A/1991, 13.985 A/1994).

Against the background of the wording of Article 77(1) of the GDPR and the cited case law of the ECJ and the Administrative Court, the interim result is that the obligation for controllers and processors to ensure the level of protection for natural persons guaranteed by the Regulation, which is standardised in Chapter V and in particular in Article 44 of the GDPR, can conversely also be asserted as a subjective right before the competent supervisory authority pursuant to Article 77(1) of the GDPR.

c) The declaratory competence of the data protection authority

In statements dated 11 February 2021 and 8 June 2021, the complainant expressly requested a declaration pursuant to Article 24(2)(5) of the DPA that the data transfers in question were unlawful under Article 44 of the GDPR.

According to the case law of the VwGH and the BVwG, the data protection authority has a declaratory competence with regard to violations of the right to secrecy in
appeal proceedings (as explicitly stated in the decision of the Federal Administrative Court of 20 May 2021, Zl. W214 222 6349-1/12E; implicitly the decision of the Administrative Court of 23 February 2021, Ra 2019/04/0054, in which the Administrative Court dealt with the determination of a past
The court has not addressed the lack of jurisdiction of the authority against which the case was brought).

There are no objective reasons not to use the declaratory competence pursuant to Art. 58(6) of the GDPR in conjunction with Art. 24(2)(5) of the GDPR and Art. 5 of the DPA also for the determination of a violation of Art. 44 of the GDPR, since in the present case, too, inter alia a violation of the law in the past - namely a data transfer to the USA - is complained about and the right to complain pursuant to Article 24(1) of the GDPR - as well as Article 77(1) of the GDPR - is generally linked to a violation of the GDPR.

If the decision in an appeal procedure could only contain instructions pursuant to Article 58(2) of the GDPR, there would be no room for Article 24(2)(5) and Article 24(5) of the GDPR.

Contrary to the view of the respondents, Section 24 (6) of the FADP does not apply to the subject matter of the complaint, since the complaint concerns a data transfer in the past. In other words, the alleged

unlawfulness (here: incompatibility with Art. 44 of the GDPR) of a data transfer that has already been completed is not amenable to a conclusion of proceedings pursuant to Section 24 (6) of the GDPR.

Against the background of these explanations, it can be stated as a further interim result that the declaratory competence of the data protection authority is given in the present complaint proceedings.

d) "serious and far-reaching practical significance" of the decision in question

In his last statement of 9 February 2022, the second respondent summarised that a decision granting the appeal would have serious consequences for the economy.

In this regard, it should be noted that the data protection authority is not permitted to take economic or political considerations into account and that these are only to be taken into account selectively within the framework of the interpretation of the GDPR - for example, within the framework of a balancing of interests pursuant to Art. 6 para. 1 lit. f leg. cit - are to be taken into account.

Rather, the data protection authority has the obligation to take a decision in the context of data protection complaints pursuant to primary law Art. 8(3) EU-GRC and secondary law Art. 58(1)(f) GDPR, taking into account the position of the ECJ in the judgment of 16 July 2020, Case C‗311/18, with regard to the legal situation of the USA.

In its ruling of 16 July 2020, the ECJ explicitly stated that the relevant legal situation in the USA - see below - is not compatible with the fundamental right to data protection pursuant to Article 8 of the EU Directive, which is why the EU-US adequacy decision ("Privacy Shield") was declared invalid.

An economic or political agreement for ensuring data transfers between
Europe and the USA are to be achieved by other bodies - but not by supervisory authorities. The arguments of the second respondent regarding the "serious and far-reaching practical significance" of the decision in question as well as the cited economic studies must therefore remain undecided.

D.2. ruling point 1

The data protection authority suspended the proceedings in question by decision of 2 October 2020, no. D155.026, 2020-0.526.838. D155.026, 2020-0.526.838, until it is determined which authority is responsible for the content of the proceedings (lead supervisory authority) or until a decision is made by a lead supervisory authority or the EDSA.

In the opinion of the data protection authority, the facts of Art. 4 Z 23 lit. b DSGVO are fulfilled, as the first respondent has set up its online comparison portal "[redacted]" - as established - on the Austrian ([redacted]), German (XXXXXXX), Polish ([redacted]) and German ([redacted]) websites.

([redacted]) and English-speaking market ([redacted]) and is indisputably the website operator for all versions of [redacted] Therefore, the procedure was to be conducted in accordance with Art. 56 in conjunction with Art. 60 ff of the GDPR ("One-Stop-Shop").

Subsequently, the data protection authority - as lead supervisory authority - submitted a draft decision to the supervisory authorities concerned pursuant to Art. 60(3) GDPR.

As no relevant and substantiated objections were raised against the draft decision, the suspension decision of 2 October 2020 had to be remedied and communicated to the parties pursuant to Article 60(7) and (8) of the GDPR.

Since ex officio decisions from which no right has accrued to anyone can be revoked or amended both by the authority that issued the decision and, in the exercise of the supervisory right, by the relevant higher authority, and no right to non-decision accrues to a party to the proceedings as a result of a stay of proceedings, the above-mentioned decision of 2 October 2020 was also amenable to revocation pursuant to section 68(2) AVG.

D.2. ruling point 2. a)

a) General information on the term "personal data

The material scope of Art. 2(1) GDPR - and thus the success of this complaint - fundamentally presupposes that "personal data" are processed.

According to the legal definition of Art. 4(1) GDPR, "*personal data means any information relating to an identified or identifiable natural person (hereinafter 'data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

As can be seen from the findings of fact (see points C.3. and C.8.), the first respondent - as operator of the website - implemented the Google Analytics tool on its website. As a result of this implementation - i.e. triggered by the JavaScript code executed when visiting the website - at least the following information was transmitted from the browser of the complainant who visited the [redacted] website to the servers of the second respondent:

- unique online identifiers ("unique identifiers") that identify both the complainant's browser or device and the first respondent (through the first respondent's Google Analytics account ID as website operator);
- the address and HTML title of the website and the subpages visited by the complainant;

- Information on the browser, operating system, screen resolution, language selection and date and time of the website visit;
- the IP address of the device used by the complainant.

It must be checked whether this information falls under the definition of Art. 4 Z 1 DSGVO, i.e. whether it is personal data of the complainant.

b) Identification numbers as "personal data

With regard to the online identifiers, it should be recalled that the cookies in question, "_ga" or "cid" (Client ID) and "_gid" (User ID), contain unique Google Analytics identifiers and were stored on the complainant's terminal device or browser. As noted, it is possible for certain bodies - in this case, for example, the respondents - to distinguish website visitors with the help of these identification numbers and also to obtain information as to whether it is a new or a returning website visitor to [redacted] In other words, it is the use of such identification numbers that makes it possible to distinguish between website visitors, which was not possible before this allocation.

In the opinion of the data protection authority, there is already an encroachment on the fundamental right to data protection pursuant to Article 8 EU-GRC and Section 1 of the Data Protection Act if certain bodies take measures - in this case the assignment of such identification numbers - to individualise website visitors in this way.

A standard of "identifiability" to the effect that it must be immediately possible to associate such identification numbers also with a specific "face" of a natural person - i.e. in particular with the name of the complainant - is not required (cf. in this respect already Opinion 4/2007, WP 136, 01248/07/DE of the former Art. 29 Data Protection Working Party on the
Term "personal data" p. 16 f; cf. the guidance of the supervisory authorities for telemedia providers from March 2019, p. 15).

Such an interpretation is supported by recital 26 of the GDPR, according to which the question of whether a natural person is identifiable *takes into account "[...] any means reasonably likely to be used by the controller or by any other person to identify the natural person, directly or indirectly, such as* singling *out*". Singling out" is understood to mean "picking out from a crowd" (cf. https://www.duden.de/rechtschreibung/aussondern, queried on 18 March 2022), which is in line with the above considerations on the individualisation of website visitors.

In the literature, it is also explicitly argued that a "digital footprint", which makes it possible to clearly individualise devices - and subsequently the specific user - constitutes a personal data (cf. *Karg* in *Simitis/Hornung/Spiecker*, DSGVO Commentary Art. 4 Z 1 Rz 52 mwN). Due to the uniqueness of the identification numbers, this consideration can be applied to the case at hand, especially since - which

will be discussed in more detail below - these identification numbers can also be combined with other elements.

To the extent that the respondents argue that no "means" are used to link the identification numbers at issue here to the person of the complainant, it must again be pointed out that the implementation of Google Analytics on [redacted] segregation within the meaning of recital 26 of the GDPR. In other words: Anyone who uses a tool that makes such segregation possible in the first place cannot take the position that, according to "general discretion", no means are used to make natural persons identifiable.

At this point, it should be noted that the European Data Protection Supervisor (EDPS) also takes the view that "segregation" by marking a terminal device is to be considered as personal data. In his decision of 5 January 2022, GZ: 2020-1013 v. European Parliament, the EDPS stated the following, among other things:

"Tracking cookies, such as the Stripe and the Google analytics cookies, are considered personal data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All records containing identifiers that can be used to single out users, are considered as personal data under the Regulation and must be treated and protected as such." (p. 13, original in English and with further references).

"Tracking cookies such as the Stripe and Google Analytics cookies are considered personal data. data, even if the traditional identity parameters of the tracked users are unknown or have been deleted by the tracker after collection. All data sets that contain identifiers that can be used to single out users are considered personal data under the Regulation and must be treated and protected as such" (translation by the DPA).

It is true that the EDPS has to apply Regulation (EU) 2018/1725, which applies to data processing by Union institutions, bodies, offices and agencies. However, since Article 3(1) of Regulation (EU) 2018/1725 corresponds to the definition of Article 4(1) of the GDPR, these considerations can easily be applied to the case at hand.

As an interim result, it can therefore be stated that the Google Analytics identification numbers in question here already qualify as personal data (in the form of an online identifier) pursuant to Art. 4(1) of the GDPR.

c) Combination with other elements

The fulfilment of the requirement of Art. 4(1) GDPR becomes even more apparent if one takes into account that such identification numbers can be combined with other elements:

Indeed, a combination of all these elements - i.e. unique identification numbers and the other information listed above, such as browser data or IP address - makes it all the more likely that the complainant can be identified (see again recital 30 of the GDPR). The complainant's "digital footprint" is made even more unique by such a combination.

The respondents' arguments about the "anonymisation function of the IP address" can be left aside, since the complete IP address is processed for a certain - albeit very short - period of time on the Google LLC server. This short data processing period is sufficient for the facts of Article 4(2) of the GDPR to be fulfilled. According to the case law of the Federal Administrative Court, it cannot be derived from Article 4(2) in conjunction with Article 6 of the GDPR that a certain "minimum processing period" is to be assumed (cf. the decision of the Federal Administrative Court of 3 September 2019, no. W214 2219944-1).

As will be explained later, this complete IP address can be accessed by US intelligence services - even if in the specific case it was processed on European servers of the second respondent as claimed.

Likewise, the question of whether an IP address in isolation is a personal data can be left open, since - as mentioned - it can be combined with other elements (in particular the Google Analytics identification number). In this context, however, it should be noted that according to the case law of the ECJ, the IP address can constitute a personal data (cf. the judgments of the ECJ of 17 June 2021, C‑597/19, para 102, as well as of 19 October 2016, C‑582/14, para 49) and that it does not lose its characteristic as a personal data merely because the means of identification lie with a third party.

d) Traceability to the complainant

Irrespective of the above considerations, however, a traceability to the complainant's "face" is to be assumed in any case:

It is not necessary that the respondents alone can establish a personal reference, i.e. that they have all the information necessary for identification (cf. ECJ judgments of 20 December 2017, C-434/16, para. 31, and of 19 October 2016, C‑582/14, para. 43). Rather, it is sufficient that anyone - with legally permissible means and reasonable effort - can establish this personal reference (cf. *Bergauer* in *Jahnel*, DSGVO Kommentar Art. 4 Z 1 Rz 20 mVa *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU 58).

Such an interpretation of the scope of application of Art. 4(1) GDPR can be derived - in addition to the cited legal and literature sources - from Recital 26 GDPR, according to which not only the means of the controller (here: the first respondent) are to be taken into account in the question of identifiability, but also those of "another person" (English language version of the regulation: "by another person"). This also follows from the idea of offering data subjects the greatest possible protection of their data.

In particular, the ECJ has also repeatedly stated that the scope of application of the GDPR is to be understood "very broadly" (see, for example, the ECJ judgments of 22 June 2021, C‑439/19, para 61; on the comparable legal situation in this respect, the judgments of 20 December 2017, C‑434/16, para 33, and of 7 May 2009, C‑553/07, para 59).

It is not overlooked that according to Recital 26 of the GDPR, the "likelihood" of anyone using means to directly or indirectly identify natural persons must also be taken into account. In fact, in the opinion of the data protection authority, the term "anyone" - and thus the scope of application of Art. 4(1) GDPR - should not be interpreted so broadly that any unknown actor could theoretically have special knowledge in order to establish a personal reference; this would lead to almost any information falling within the scope of application of the GDPR and a demarcation from non-personal data becoming difficult or even impossible.

Rather, the decisive factor is whether an identifiability can be established with a justifiable and reasonable effort (cf. the decision of 5 December 2018, GZ DSB-D123.270/0009DSB/2018, according to which personal data are not - or no longer - available if the controller or a third party can only establish a personal reference with a disproportionate effort).

In the present case, however, there are certain actors who possess special knowledge which makes it possible to establish a connection to the complainant in the sense of the above and therefore to identify him.

i) This is firstly the second respondent:

As can be seen from the findings of fact, the complainant was, at the time of the [redacted] logged in with his Google account. The second respondent stated that he receives information due to the fact that the Google Analytics tool is implemented on a website. This includes the information that a certain Google account user has visited a certain website (cf. the opinion of 9 April 2021, question 9).

This means that the second respondent at least received the information that a user who was logged into the complainant's Google account had visited the [redacted] website.

Even if one takes the view (which is not required) that the online identifiers listed above must be assignable to a certain "face", such an assignment can in any case be made via the complainant's Google account.

The second respondent's further statements that certain requirements must be met for such an allocation, such as the activation of specific settings in the Google account, are not overlooked (cf. again his statement of 9 April 2021, question 9).

However, if - and this has been convincingly explained by the complainant - the identifiability of a website visitor only depends on whether certain declarations of intent are made in the account, all possibilities for identifiability are present (from a technical point of view). Viewed differently, the second respondent could not comply with a user's wishes expressed in the account settings for "personalisation" of the advertising information received.

In this context, the unambiguous wording of Article 4(1) of the GDPR should be explicitly pointed out, which is linked to the ability ("can be identified") and not to whether an identification is ultimately carried out.

Likewise, explicit reference must be made to the first respondent's accountability obligation under the GDPR - as a controller, see below - to implement appropriate technical and organisational measures in accordance with Article 5(2) in conjunction with Article 24(1) in conjunction with Article 28(1) of the GDPR.
to ensure and provide evidence that the processing (with the help of a processor) is carried out in accordance with the Regulation. This is therefore an obligation to bring.

This also includes proof that a processing operation is not subject to the Regulation, especially since the respondents have concluded contracts under data protection law with regard to Google Analytics, which in turn presuppose the applicability of the GDPR. However, the corresponding evidence was not provided - despite several opportunities to do so.

Unlike Chapter V - see below - Art. 5(2) in conjunction with Art. 24(1) GDPR now actually take a risk-based approach. The higher the risk associated with the data processing, the higher the standard for the evidence to be submitted in order to prove compliance with the GDPR.

In the case at hand, a high risk and therefore a high standard for the burden of proof must be assumed:

In any case, the second respondent also developed the Google Analytics product in order to collect as much information as possible from website visitors. Thus, the latter itself states that due to the fact that Google Analytics is embedded on a website, the latter can receive the information that a certain Google account holder has visited such a website. In other words: In exchange for allowing website operators to use the free version of Google Analytics, the second respondent receives technical possibilities to collect data and further enrich the profiles of Google account holders. Therefore, it cannot be assumed that Google Analytics is a mere web analytics service for website operators.

Based on this high standard for the burden of proof, it is not sufficient to merely claim that the second respondent only receives the information in question when certain settings are selected in the Google account. Further evidence (such as screenshots, more detailed technical descriptions, etc.) was not submitted - despite an extensive investigation.

It is not overlooked that the accountability pursuant to Art. 5(2) in conjunction with Art. 24(1) of the GDPR explicitly applies to the first respondent as the responsible party. However, the affirmative part of the decision in question is directed (only) against the first respondent, which has embedded the Google Analytics product on its website.

As far as the respondent to the second complaint refers to the presumption of innocence pursuant to Art. 48 (1) EU-GRC in this context, it should be noted that the case in question exclusively concerned a complaint procedure pursuant to Art. 77 (1) GDPR and not administrative criminal proceedings. Apart from that, the complaint against the second respondent was dismissed anyway.

If the second respondent finally states that such a "distribution of the burden of proof" is not compatible with Austrian procedural law, it must be countered that this is an explicit provision in the GDPR (accountability). Apart from that, such a "distribution of the burden of proof" is quite common in the legal system - especially in consumer protection law (see, for example, § 924 ABGB or § 11 para. 1 VGG, BGBl. I no. 175/2021; on the close relationship between consumer protection law and the fundamental right to data protection, see also recital 42 GDPR).

ii) Independently of the second respondent, however - and this is of greater relevance to the case - the US authorities must be taken into account:

As the complainant has equally correctly pointed out, intelligence services of the USA use certain online identifiers (such as the IP address or unique identification numbers) as a starting point for the surveillance of individuals. In particular, it cannot be ruled out that these intelligence services have already collected information with the help of which the data transmitted here can be traced back to the person of the complainant.

The fact that this is not merely a "theoretical danger" is demonstrated by the ECJ ruling of 16 July 2020, C‑311/18, which ultimately also declared the EU-US adequacy decision ("Privacy Shield") invalid due to the incompatibility of such methods and access possibilities of the US authorities with the fundamental right to data protection pursuant to Art. 8 EU-GRC.

In particular, this is also shown by the - in the findings of the facts cited - Transparency report of the second respondent showing that data requests are made to the second respondent by US authorities. For example, metadata and content data may be requested from the second respondent.

While it is not misjudged that it is admittedly not possible for the first respondent to check whether such accesses by US authorities occur in individual cases - i.e. per website visitor - and what information US authorities already possess, conversely, this circumstance cannot be held against affected persons, such as the complainant. Thus, it was ultimately the first respondent as website operator who - despite the publication of the aforementioned ECJ judgment of 16 July 2020 - continued to use the Google Analytics tool.

Specifically, the information was transmitted that the complainant had visited a certain website (in this case: a comparison portal in the form of "[redacted]") at a certain time with certain browser settings as

well as a certain IP address using an end device that was marked with a unique Google Analytics identification number.

While it is true in principle that this is (initially) only information about a specific terminal device. However, just as the location data of a vehicle obtained with the help of a GPS tracker can also constitute personal data about the whereabouts of the vehicle driver, the information relevant here constitutes personal data of the person most likely to have used the terminal device.

In the case at hand, this is the complainant, especially since he was (undisputedly) logged into the browser with his personal Google account at the time he accessed the website. There are no indications that the complainant has given his access data to third parties and - as far as can be seen - this has not been claimed by any party.

A standard to the effect that it must be "certain" which natural person has used the terminal device cannot be derived from Art. 4(1) GDPR and is also not required:

In this view, information belonging to a terminal device or an account would always be non-personal data, since it can never be ruled out that the terminal device or access data have been passed on to third parties (such as friends or family members). Such a view would lead to a too narrow scope of application of Art. 4(1) GDPR, which in turn contradicts the case law of the ECJ, which assumes a very broad scope of application.

As a further interim result, it must therefore be noted that the information listed in the findings of fact under C.8. (at least in combination) is personal data pursuant to Art. 4(1) of the GDPR.

e) Distribution of roles

As already explained, the first respondent, as the website operator, took the decision to implement the "Google Analytics" tool on the [redacted] website at the time the complaint was filed. Specifically, it inserted a JavaScript code ("tag") provided by the second respondent into the source code of its website, whereby this JavaScript code was executed in the complainant's browser when visiting the website. In this regard, the first respondent stated that the said tool is used for the purpose of statistical analyses of the website visitors' behaviour (see the statement of 22 December 2020, question 2).

In this way, the first respondent decided on the "purposes and means" of the data processing in connection with the tool, which is why it is (in any case) to be regarded as the controller within the meaning of Article 4(7) of the GDPR.

As far as the second respondent is concerned, it should be noted that the subject matter of the complaint relevant here (only) relates to the transfer of data to the second respondent in the USA. A possible further data processing of the information mentioned in the findings of fact under C.8. (by Google Ireland

Limited or the second respondent) is not the subject matter of the complaint and was therefore not investigated further in this direction.

The data protection role of the second respondent is therefore of no further relevance to the present proceedings, especially since the obligation to comply with Article 44 GDPR applies equally to controllers and processors.

D.3. ruling point 2. b)

a) Scope of Chapter V of the GDPR

First of all, it must be examined whether the first respondent is subject to the obligations standardised in Chapter V of the Regulation.

According to Art. 44 GDPR, any *"[...] transfer of personal data already processed or to be processed after their transfer to a third country or an international organisation [...] shall only be allowed if the controller and processor comply with the conditions laid down in this Chapter and also with the other provisions of this Regulation, including any onward transfer of personal data from the third country or international organisation concerned to another third country or international organisation. All the provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Regulation is not undermined."*.

In the "Guidelines 5/2021 on the relationship between the scope of Art. 3 and the
Guidelines for International Data flows under Chapter V of the GDPR" (currently still in public consultation), the EDSA has identified three cumulative conditions for a "transfer to a third country or an international organisation" within the meaning of Article 44 of the GDPR (ibid., para. 7):

- the controller or a processor is subject to the GDPR for the processing in question;
- that controller or processor ("data exporter") discloses, by transmission or otherwise, personal data which are the subject of this
  another controller, a joint controller or a joint representative of a third party. controller or a processor, openly ("data importer");
- the data importer is located in a third country or is an international organisation, whether or not that data importer is subject to the GDPR in respect of the processing in question pursuant to Article 3.

The first respondent is based in Austria and is the data controller for the operation of the [redacted] website. Furthermore, the first respondent (as a data exporter) disclosed personal data of the complainant by proactively implementing the Google Analytics tool on its [redacted] website and, as a direct consequence of this implementation, a data transfer to the second respondent (to the USA) took place, among others. Finally, the second respondent is based in the USA.

Thus, the requirements (which are quite narrowly defined in the current version of the EDSA guidelines) are met and the first respondent, as a data exporter, is in any case subject to the provisions of Chapter V of the Regulation.

(b) The rules of Chapter V of the GDPR

Subsequently, it must be checked whether the data transfer to the USA has taken place in accordance with the provisions of Chapter V of the GDPR.

Chapter V of the Regulation provides for three instruments to ensure the adequate level of protection required by Art. 44 GDPR for data transfers to a third country or an international organisation:

- Adequacy decision (Art. 45 GDPR);
- Appropriate safeguards (Art. 46 GDPR);
- Exceptions for certain cases (Art. 49 GDPR).

c) Adequacy decision

The ECJ has ruled that the EU-US adequacy decision ("Privacy Shield") - without maintaining its effect - is invalid (see the judgment of 16 July 2020, C‑ 311/18 para 201 f).

The data transfer in question is therefore not covered by Art. 45 GDPR. **d) Appropriate safeguards**

As can be seen from factual finding C.5 , the respondents to the complaint have

Standard Data Protection Clauses (hereinafter: SDC) pursuant to Art. 46(2)(c) of the GDPR for the transfer of personal data to the USA ("Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses [Processors]"). Specifically, at the time of the complaint, the clauses in question were those in the version of the Implementing Decision of the European Commission 2010/87/EU of 5 February 2010 concerning
Standard contractual clauses for the transfer of personal data to processors in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 2010/39, p. 5.

In the aforementioned judgment of 16 July 2020, the ECJ stated that SDCs as an instrument for international data flows are not objectionable in principle, but the ECJ also pointed out that SDCs are by their nature a contract and therefore cannot bind authorities from a third country:

"Accordingly, while there are situations in which the recipient of such a transfer can, in the light of the law and practice in the third country concerned, guarantee the necessary data protection on the basis of the standard data protection clauses alone, there are also situations in which the rules contained in those clauses may not be a sufficient means of ensuring in practice the effective protection of personal

data transferred to the third country concerned. This is the case, for example, when the law of that third country allows its authorities to interfere with the rights of data subjects with regard to those data" (ibid. para. 126).

A more detailed analysis of the legal situation of the USA (as a third country) can, however, be omitted here, as the ECJ has already dealt with this in the cited judgment of 16 July 2020. In doing so, it came to the conclusion that the EU-US adequacy decision is not justified on the basis of the relevant law of the USA and the implementation of administrative surveillance programmes - based, inter alia, on Section 702 of FISA and E.O. 12333 in conjunction with PPD-28 - does not ensure an adequate level of protection for natural persons (ibid. para. 180 ff).

The data protection authority has no doubts that the second respondent qualifies as a provider of electronic communications services within the meaning of 50 U.S.Code § 1881(b)(4) and is therefore subject to surveillance by U.S. intelligence agencies pursuant to 50 U.S.Code § 1881a ("FISA 702"). Accordingly, the second respondent has the obligation to provide personal data to the US authorities pursuant to 50 U.S. Code § 1881a (cf. also the legal opinion of 15 November 2021 commissioned by the DPA). November 2021 on the current status of US surveillance law and surveillance powers by *Vladeck*, question 5 f, according to which the scope of application of FISA 702 is to be understood very broadly and the powers of US authorities extend to all data in the company due to a minor activity within the scope of application of FISA 702).

As can be seen from the Second Respondent's Transparency Report, such requests are also regularly made to the Second Respondent by US authorities (see https://transparencyreport.google.com/user-data/us-national-security?hl=en, accessed on 18 March 2022).

Against this background, the ECJ also stated in the cited judgment of 16 July 2020 that *"[...] standard data protection clauses cannot, by their very nature, provide guarantees going beyond the contractual obligation to ensure compliance with the level of protection required by Union law [...]"* and that "[...] *depending on the situation prevailing in a particular third country, it may be necessary for the controller to take additional measures to ensure compliance with that level of protection"* (ibid. para. 133).

The data transfer in question cannot therefore be based solely on the standard data protection clauses concluded between the respondents (cf. Art. 46(2)(c) GDPR).

e) General information on "additional measures

In its "Recommendations 01/2020 on measures to complement transmission tools for the Ensuring the level of protection of personal data under Union law V. 2.0", the EDSA has stated that in the event that the law of the third country has an impact on the effectiveness of appropriate safeguards (such as SDK), the data exporter must either suspend the data transfer or implement supplementary measures (ibid. para. 28 ff).

According to the EDSA's recommendations, such "additional measures" within the meaning of the ECJ's judgment of 16 July 2020 can be of a contractual, technical or organisational nature (ibid. para. 52):

With regard to contractual measures, it is stated that *they "[...] complement and reinforce the safeguards provided by the transfer instrument and the relevant legislation in the third country, to the extent that the safeguards do not, taking into account all the circumstances of the transfer, fulfil all the conditions necessary to ensure a level of protection substantially equivalent to that prevailing in the EU". Since contractual measures, by their nature, cannot generally bind the authorities of the third country if they are not themselves party to the contract, they must be combined with other technical and organisational measures to ensure the required level of data protection. Just because one or more of these measures has been selected and applied does not necessarily mean that it is systematically ensured that the envisaged transfer meets the requirements of Union law (ensuring a substantially equivalent level of protection)"* (ibid. para. 99).

With regard to organisational measures, it is stated that these are *"[...] internal strategies, organisational methods and standards that controllers and processors may apply to themselves and impose on data importers in third countries. [...] Depending on the specific circumstances of the transfer and the assessment carried out of the legal situation in the third country, organisational measures are necessary to complement contractual and/or technical measures in order to ensure that the level of protection of personal data is substantially equivalent to that ensured in the EEA* (ibid. para. 128).

As regards technical measures, it is stated that these are intended to ensure that *"[...] access to the transferred data by authorities in third countries does not undermine the effectiveness of the appropriate safeguards listed in Article 46 of the GDPR. Even if the access by the authorities complies with the law in the country of the data importer, these measures should be considered if the access by the authorities goes beyond what is a necessary and proportionate measure in a democratic society. These measures aim to eliminate potentially infringing access by preventing the authorities from identifying data subjects, inferring information about them, identifying them in other contexts, or linking the transferred data to other data sets held by the authorities, including data on online identifiers of the devices, applications, tools and protocols used by the data subjects in other contexts* (ibid. para. 79).

Finally, the EDSA has stated that such "additional measures" are to be considered effective within the meaning of the judgment of 16 July 2020 only *"[...] if and to the extent that the measure precisely closes the legal protection gaps that the data exporter has identified in its examination of the legal situation in the third country. If it is ultimately not possible for the data exporter to achieve a substantially equivalent level of protection, it may not transfer the personal data"* (ibid. para. 75).

Applied to the case at hand, this means that it must be examined whether the "additional measures taken" by the second respondent close the legal protection gaps identified in the ECJ ruling of 20 June 2020 - i.e. the access and surveillance possibilities of US intelligence services.

f) "Additional measures" of the second respondent

The second respondent has now implemented various measures in addition to the conclusion of the SDK (cf. its statement of 9 April 2021, question 28).

With regard to the contractual and organisational measures outlined, it is not clear to what extent a notification of the data subject about data requests (should this be permissible at all in individual cases), the publication of a transparency report or a "policy for dealing with government requests" are effective in the sense of the above considerations. Similarly, it is unclear to what extent the "careful examination of any data access request" is an effective measure, as the ECJ has stated in the above-mentioned judgment of 20 June 2020 that permissible (i.e. legal under US law) requests by US intelligence services are not compatible with the fundamental right to data protection under Art. 8 EU-GRC.

As far as the technical measures are concerned, it is also not recognisable - and was also not explained comprehensibly on the part of the respondents - to what extent the protection of communication between Google services, the protection of data in transit between data centres, the protection of communication between users and websites or an "on-site security" actually prevent or restrict the access possibilities of US intelligence services on the basis of US law.

Insofar as the second respondent subsequently refers to encryption technologies - such as the encryption of "data at rest" in the data centres - it must again be given the
Recommendations 01/2020 of the EDSA. Indeed, it states that a data importer (such as the second respondent) subject to 50 U.S. Code § 1881a ("FISA 702") has a direct obligation, with respect to imported data in its possession or custody or under its control, to provide access to or surrender it. This obligation may expressly extend to the cryptographic keys without which the data cannot be read (ibid. para. 81).

As long as the second respondent himself has the possibility to access data in plain text, the technical measures invoked cannot be considered effective in the sense of the above considerations.

The second respondent argues as a further technical measure that as far as *"[...] Google Analytics data for measurement by website owners is personal data, [...] it* must be *considered as pseudonymous"* (cf. its opinion of 9 April 2021, p. 26).

However, this must be countered by the convincing view of the German Data Protection Conference, according to which *"[...] the fact that users are made identifiable, for example via IDs or identifiers, does not constitute a pseudonymisation measure within the meaning of the GDPR. Moreover, the use of IP addresses, cookie IDs, advertising IDs, unique user IDs or other identifiers to (re)identify users do not constitute appropriate safeguards to comply with data protection principles or to safeguard the rights of data subjects. This is because, unlike in cases where data is pseudonymised in order to disguise or delete the identifying data so that the data subjects can no longer be addressed, IDs or identifiers are*

used to make the individuals distinguishable and addressable. Consequently, there is no protective effect. It is therefore not a matter of pseudonymisation in the sense of the German Data Protection Act. Rec 28, which reduce risks for data subjects and assist controllers and processors in complying with their data protection obligations" (cf. the March 2019 guidance of the supervisory authorities for telemedia providers, p. 15).

Furthermore, the second respondent's argument cannot be accepted because the Google Analytics identifier - as explained above - can in any case be combined with other elements and can even be associated with a Google account that is indisputably attributable to the complainant.

The "anonymisation function of the IP address" is not effective, since the data - as explained in more detail above - is processed by the second respondent for at least a certain period of time. Even assuming that the IP address was only processed in servers in the EEA within the period of time, it should be noted that the second respondent can nevertheless be obliged by US intelligence services to hand over the IP address under the relevant law of the USA (cf. EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection [annex] of 10 July 2019, p. 1 f; cf. the already mentioned legal opinion of 15 November 2021 by *Vladeck*, question 8 ff, according to which FISA 702 can also be applied extraterritorially).

Apart from that, the IP address is anyway only one of many "puzzle pieces" of the complainant's digital footprint.

As a further interim result, it must therefore be noted that the "additional measures" in question are not effective, as they do not close the legal protection gaps identified in the ECJ ruling of 20 June 2020 - i.e. the access and surveillance possibilities of US intelligence services.

The data transfer in question is therefore not covered by Article 46 of the GDPR.

D.4. ruling point 2. c)

a) Regarding Art. 49 GDPR

According to the first respondent's own information, the exemption pursuant to Art. 49 GDPR was not relevant for the data transfer in question (cf. the opinion of
16 December 2020).

Consent pursuant to Article 49 (1) (a) of the GDPR was not obtained. The data protection authority also fails to see how any other element of Article 49 of the GDPR is fulfilled.

The data transfer in question cannot therefore be based on Article 49 of the GDPR.

b) Chapter V GDPR does not recognise a risk-based approach

The second respondent subsequently argues - in summary - that the risk of the data transfer to the USA had to be taken into account and that the prosecuting authority applied too strict a standard. These statements are not to be followed:

Such a "risk-based approach" cannot be derived from the wording of Art. 44 GDPR:

Art. 44 GDPR

General principles of data transmission

Any transfer of personal data already processed or to be processed after their transfer to a third country or an international organisation shall only be allowed if the controller and the processor comply with the conditions laid down in this Chapter and with the other provisions of this Regulation, including any onward transfer of personal data from that third country or international organisation to another third country or international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Regulation is not undermined.

On the contrary, it can be deduced from the wording of Art. 44 GDPR that for every data transfer to a third country (or to an international organisation), it must be ensured that the level of protection guaranteed by the GDPR is not undermined.

The success of a complaint of a violation of Art. 44 GDPR therefore does not depend on whether a certain "minimum risk" is present or whether US intelligence services have actually accessed data. According to the wording of this provision, a violation of Art. 44 GDPR already exists if personal data are transferred to a third country without an adequate level of protection.

In connection with those provisions of the GDPR where a risk-based approach is actually to be followed ("the higher the processing risk, the more measures are to be implemented"), the legislator has also explicitly and without doubt standardised this. For example, the risk-based approach is provided for in Art. 24(1) and (2), Art. 25(1), Art. 30(5), Art. 32(1) and (2), Art. 34(1), Art. 35(1) and (3) or Art. 37(1)(b) and (c) GDPR.

Since the legislator has standardised a risk-based approach in numerous places in the GDPR, but not in connection with the requirements of Art. 44 GDPR, it cannot be assumed that the legislator merely "overlooked" this; an analogous application of the risk-based approach to Art. 44 GDPR is therefore excluded.

The reference to the "free movement of data" does not help the complainant's point of view either:

It is undisputed that the GDPR is (also) intended to ensure the free movement of data. However, the free movement of data is subject to the premise that the provisions of the GDPR - including Chapter V - are fully complied with. A softening in the sense of a "business-friendly interpretation" of the provisions

of Chapter V in favour of the free movement of data is not envisaged. Economic interests also played no role in the aforementioned ECJ ruling of 16 July 2020.

The further argumentation that the "risk-based approach was confirmed by the ECJ in its ruling of 16 July 2020" cannot be understood:

In its analysis of the legal situation in the US and the validity of the EU-US adequacy decision, the ECJ did not take a risk-based approach in Chapter V of the GDPR. In fact, such a risk-based approach is not mentioned in the aforementioned judgment.

The respondent to the second complaint apparently derives the following from the wording used by the ECJ
"adequate level of data protection" does not reflect a risk-based approach. This cannot be accepted, as the ECJ used this wording with reference to Recital 108 of the GDPR. It is clear from recital 108 of the Regulation that "adequate level of data protection" means that the rights of data subjects are to be respected in an adequate manner.

With regard to the legal situation of the USA, the ECJ has now assumed that, due to the disproportionate access possibilities of the US authorities, there is no "reasonable" access.
level of data protection" is to be assumed, which is why it finally also Adequacy Decision declared invalid.

The ECJ explicitly did not take into account that the obligations to which a Privacy Shield certified company from the US is subject may be appropriate in individual cases (e.g. because the certified company only receives non-sensitive or non-criminal personal data).

Similarly, the argument that the European Commission in its Implementing Decision (EU) 2021/914, which adopted new standard contractual clauses, "equally clearly advocated a risk-based approach" cannot be understood:

It should be noted that the Implementing Decision (EU) 2021/914 does not contain a risk-based approach either. The current Implementing Decision, which was adopted as a result of the ECJ's judgment of 16 July 2020, requires - on the contrary - that the parties to standard data protection clauses now have to review local laws and obligations in the event of access to the data by public authorities prior to the transfer of data to a third country.

To the extent that the second respondent derives the European Commission's alleged position from (non-binding) recital 20 of the aforementioned implementing decision, it must be countered that recital 20 does not assume a risk-based approach either:

Recital 20 of the aforementioned Implementing Decision correctly points out that in the context of assessing the level of data protection in a third country, the circumstances of the transfer in particular must be taken into account.

Taking the example of the legal situation in the USA, it is necessary to check whether data is transferred to a provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4), otherwise the corresponding access options under FISA 702 do not apply. If Austria were a third country, it would have to be checked prior to data transfers to Austria whether the specific types of data transferred are subject to the scope of application under the (now) State Protection and Intelligence Service Act, Federal Law Gazette I No. 5/2016 as amended, and whether the access options of the State Protection and Intelligence Service Directorate are proportionate.

However, this is (only) an examination of whether the local legal provisions and obligations in the
In the event of access to the data by authorities, the contractual Obligations of the standard data protection clauses and not a risk-based approach in the sense that it is necessary to verify how sensitive or non-sensitive the personal data transferred are.

Moreover, it should be noted that an implementing decision of the European Commission could not in any case impose a completely new content on the provisions of Art. 44 GDPR (cf. on the primacy of the text of the Regulation, for example, the judgment of the ECJ of 12 May 2005, C-444/03, para. 25).

Finally, the reference to the EDSA's Recommendations 01/2020 on measures to complement transfer tools to ensure the level of protection of personal data under EU law does not add anything to the complainant's position:

Thus, the passage in the recommendations cited by the second respondent - as already stated in connection with Implementing Decision (EU) 2021/914 - only states that it is necessary to check whether the problematic laws of the third country apply to each data transfer and not that it is necessary to check how sensitive or non-sensitive the personal data transferred are.

Finally, as far as the second respondent argues that US intelligence services have no interest in the data processed in this case - for example, by stating that the information on the "screen resolution is an industry standard" - it must be countered that it is not a question of a possible interest of US intelligence services, but of their access possibilities.

Irrespective of this, however, it should be noted that the added value of the information lies in particular in the fact that it can be combined (cf. also the definition of "fingerprinting" according to RFC6973 of the Internet Architecture Board, according to which "fingerprinting" is the process by which a observer identifies a device or application instance with sufficient probability based on several information elements). Likewise, for example, the processed IP address alone - as part of the digital

footprint - can be used to find out which internet provider is used and in which region the user of the terminal device is located. **b) Result**

As no adequate level of protection was ensured by an instrument of Chapter V of the Regulation for the data transfer in question from the first respondent to the second respondent (in the USA), there is a violation of Article 44 of the GDPR.

The first respondent was (at any rate) responsible for the operation of the [redacted] website at the time relevant to the complaint, i.e. 14 August 2020. The relevant data protection violation against Article 44 of the GDPR is therefore attributable to the first respondent.

The decision was therefore in accordance with the ruling.

D.5 On remedial powers

In the opinion of the data protection authority, the Google Analytics tool (at least in the version of 14 August 2020) can therefore not be used in accordance with the provisions of Chapter V of the GDPR.

However, it was not necessary to make use of the remedial powers, as the tool was removed before the conclusion of the present complaint procedure.

D.6. ruling point 3

It must be examined whether the second respondent (as data importer) is also subject to the obligations standardised in Chapter V of the Regulation.

Based on the EDSA Guidelines 5/2021 already cited above, it should be noted again that a "transfer to a third country or an international organisation" within the meaning of Art. 44 GDPR only exists if, inter alia, the controller or processor (data exporter) discloses, by transmission or otherwise, personal data which are the subject of such processing to another controller, joint controller or processor (data importer).

This requirement does not apply to the second respondent in the present case, since he (as a data importer) does not disclose the complainant's personal data, but (only) receives it. In other words, the requirements of Chapter V of the GDPR must be complied with by the data exporter, but not by the data importer.

The complainant's argument that a data transfer necessarily presupposes a recipient and that the second respondent is (at least from a technical point of view) part of the data transfer is not overlooked. However, it must be countered that the responsibility under data protection law for a processing operation (from a legal point of view) is nevertheless

"sharing", i.e. there may be a different degree of responsibility depending on the stage of the processing operation (cf. EDSA Guidelines 7/2020 on the concept of controllers and processors, para. 63 et seqq).

In the opinion of the data protection authority, there is therefore no violation of Art. 44 of the GDPR by the second respondent.

Overall, the decision was therefore in accordance with the ruling.

Finally, it should be noted that the question of the (possible) violation of Art. 5 et seq. in conjunction with Art. 28(3)(a) and Art. 29 of the GDPR by the second respondent will be addressed in a further decision.

R E C O R D I N G M E A S U R E S

An appeal against this decision may be filed in writing with the Federal Administrative Court within **four weeks** after service. The appeal **must be lodged with the data protection authority** and must

- the designation of the contested decision (GZ, subject)
- the designation of the authority against which proceedings have been brought,
- the grounds on which the allegation of illegality is based,
- the request and
- contain the information necessary to assess whether the complaint has been filed in time.

The data protection authority has the option of either amending its decision within two months by means of a **preliminary appeal decision** or **submitting** the appeal with the files of the proceedings to **the Federal Administrative Court.**

The appeal against this decision is **subject to a fee. The** fixed fee for a corresponding submission including enclosures is **30 euros**. The fee is to be paid to the account of the Tax Office Austria, stating the purpose of use.

The fee must always be transferred electronically using the function "Finanzamtszahlung". The Austrian Tax Office - Special Responsibilities Department is to be indicated or selected as the recipient (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, the tax number/levy account number 10 999/9102, the levy type "EEE complaint fee", the date of the notice as the period and the amount are to be indicated.

If the e-banking system of your credit institution does not have the "tax office payment" function, the eps procedure in FinanzOnline can be used. An electronic transfer can only be dispensed with if no e-banking system has been used so far (even if the taxpayer has an internet connection). In this case, the payment must be made by payment order, whereby attention must be paid to the correct allocation. Further information is available from the tax office and in the manual "*Electronic payment and notification for payment of self-assessment levies*".

The payment The payment of the **fee** shall be evidenced **to the data protection authority** by means of a payment **voucher** to be attached to the submission or a printout showing that a payment order has been issued. If the fee is not paid or not paid in full, the **competent tax office** shall be **notified.**

A timely and admissible appeal to the Federal Administrative Court has a **suspensive effect.** The suspensive effect may have been excluded in the ruling of the decision or may be excluded by a separate decision.

22 April 2022

For the head of the data protection authority:

[redacted]