Republic of Austria
Data protection authority

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [redacted]

E-mail: dsb@dsb.gv.at

GZ: D155.026
2022-0.029.027

Desk officer: [redacted]

[MACHINE TRANSLATION]

Please note that this decision only revolves around a formal infringement of the processing that took place in August 2020. According to our Austrian Data Protection Act, we have the obligation to formally establish such infringements, if requested by the complainant. We did not exercise our corrective powers because the tool was removed from the website at stake before the conclusion of this case.

Data protection complaint (Art. 77 para. 1 GDPR)
[redacted], represented by NOYB/1. [redacted] and 2.
Google LLC by e-delivery/email “email address”

DECISION

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

1. The decision of the Data Protection Authority of 2 October 2020, Zl. D155.026, 2020-0.526.838, is removed.

2. The complaint against the first respondent is justified and it is established that:

a) the first respondent as responsible by implementing the tool "Google Analytics" on its website at www.[redacted].at has transmitted personal data of the complainant to the second respondent at least on 11 August 2020 (these are at least unique user identification numbers, IP address and browser parameters);

b) the standard data protection clauses adopted by the first respondent with the Second respondent has not provided an adequate level of protection in accordance with Article 44 of the GDPR, since

i) the Second respondent as Supplier electronic Communication services within the meaning of 50 U.S. Code § 1881(b)(4) is qualified and as such is subject to surveillance by U.S. intelligence services pursuant to 50 U.S. Code § 1881a ("FISA 702"), and

ii) the measures taken in addition to those referred to in point 2(b) Standard data protection clauses are not effective as they do not eliminate the monitoring and access possibilities of US intelligence services;

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

3. The complaint against the second respondent for an infringement of the general principles of data transfer pursuant to Article 44 GDPR is dismissed.

Legal bases: Articles 4(1), 2, 7, 8 and 23(b), Article 5, Article 44, Article 46(1) and (2)(c), Article 51(1), Article 56(1), Article 57(1)(d) and (f), Article 60(7) and (8), Article 77(1), Article 80(1) and Article 93(2) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016 p. 1; Sections 18(1) and 24(1), (2)(5) and (5) of the Data Protection Act (DSG), BGBl. I No 165/1999 as amended; Section 68(2) of the General Administrative Procedures Act 1991 (AVG), BGBl. 51/1991, as amended.

REASONS FOR THE DECISION

A. Arguments of the parties and procedure

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

On 11 August 2020, at 1:46:00, he visited the first respondent's website at www.[redacted].at. During the visit, he was logged into his Google account, which was linked to the complainant's e-mail address. The first respondent embedded an HTML code for Google services (including Google Analytics) on its

website. During the visit, the first respondent processed personal data, namely at least the complainant's IP address and cookie data. Some of these data were transmitted to the second respondent. Such a transfer of data requires a legal basis in accordance with Art. 44 et seq. of the GDPR.

According to the judgment of the Court of Justice of 16 July 2020, Case C-11/18 ('Schrems II'), the respondents could no longer rely on an adequacy decision ('Privacy Shield') pursuant to Article 45 GDPR for data transfer to the USA. The first respondent should also not base the transfer of data on standard data protection clauses where, in accordance with Union law, the third country of destination does not ensure adequate protection of personal data transmitted on the basis of standard data protection clauses. The second respondent must be classified as a provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4) and, as such, is subject to supervision by US intelligence services under 50 U.S. Code § 1881a ("FISA 702"). The second respondent actively provides personal data to the U.S. Government pursuant to 50 U.S. Code § 1881a.

Consequently, the respondents are not in a position to ensure adequate protection of the complainant's personal data when his data are transferred to the second respondent. The transfer of the complainant's data to the USA was unlawful. The complaint was accompanied by several annexes.

A.2. With opinion of 22. December 2020, the First respondent summarising the following:

The program code for the Google Analytics tool was embedded on www.[redacted].at. Without consent, however, the code would not be played by the web server. The first respondent is established only in Austria and has no other branches in other Member States. It operates the following European versions of the website, on which the tool is also integrated in the same form: www.[redacted].at, www.[redacted].de, www.[redacted].eu, www.[redacted].co.uk and ♦.

The tool would be used to enable general statistical analyses of the behaviour of the websitevisitors. However, the tool does not allow the content or search queries to be adapted to a specific website user, since the evaluation is carried out anonymously and does not allow any connection to a particular user. User IP addresses would also be anonymised prior to storage or transmission ("IP anonymisation"). The function "anonymizeIP" was set to "true". This ensures anonymisation before storing the data. The code for the tool in question is currently still available on the websites.

If the GDPR is applicable, the first respondent is the controller and the second respondent is a processor. A processor agreement was concluded. As no personal data would be transferred, the judgment of the CJEU of 16 July 2020 in Case C311/18 is not relevant. However, in order to make arrangements for the possible transfer of personal data to the second respondent — e.g. in the event that IP anonymisation is deactivated on the basis of a data breach — the first respondent concluded a processor agreement with the second respondent, as well as standard data protection clauses (SDK). This was implemented purely for precautionary reasons. The second respondent put in place further technical and

organisational measures to provide a high level of data protection for the data processed through the tools. The opinion was accompanied by a number of annexes.

A.3. In a summary of comments of 12 February 2021, the complainant submitted the following:

The first processed IP address would — if at all — be anonymised later in a second step. This possible anonymisation after transfer does not affect the previous processing. The opinion contains a detailed technical description here. If the first respondent is convinced that no personal data will be processed, for example, the conclusion of order processing conditions is absurd. The opinion was accompanied by a number of annexes. It is requested to establish that the data transfers in question were inadmissible within the meaning of Article 44 et seq. of the GDPR.

A.4. The DPA requested the second respondent, with discharge of 3 May 2021, as follows (formatting not reproduced 1:1):

*"**Concerns: I. Data protection complaint pursuant to Art. 77 para. 1 GDPR against Google LLC; II. To the questionnaire of 9 April 2021***

I. Data protection complaint pursuant to Art. 77 para. 1 GDPR against Google LLC

*In the annex you will find a data protection complaint dated 18 August 2020 pursuant to Art. 77 para. 1 GDPR of 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, the first respondent's observations of 16 April 2006 will be submitted. Submitted in December 2020.*

Subject of appeal is the use of the Google Analytics tool by the first respondent on his website. Google LLC is expressly mentioned as a second respondent. A violation of the requirements for international data traffic (Chapter 5 GDPR) is alleged.

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

II. To the questionnaire of 9 April 2021

Google LLC has already completed a questionnaire from the Data Protection Authority on Google Analytics in parallel pending complaints on the number of transactions DSB-D155.027 and submitted corresponding replies to the Data Protection Authority by letter dated 9 April 2021.

It is noted that Google's opinion of 9 April 2021 is formulated in such a way that the explanations are also applicable to the relevant appeal proceedings against the price comparison of [redacted]. Consequently, the Data Protection Authority intends to grant the parties involved in the present proceedings parties to the letter of 9 April 2021 from Google LLC.

If you have any objections to this procedure, you will be asked to notify it within three weeks of receipt of this letter.

Please indicate the business number DSB-D155.026 when submitting your submissions to the data protection authority."

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

The code at issue for the Google Analytics tool was removed on 25 May 2021. The use of Google Analytics on the website www.[redacted].at was discontinued. A procedure under Paragraph 24(6) of the DSG (formless attitude) was suggested.

A.6. In a summary of comments of 8 June 2021, the complainant submitted the following:

It is a matter of fact which is in the past and the removal of the program code does not alter the complainant's complaint. The data in question had already been transmitted in violation of Article 44 et seq. of the GDPR. Such a finding was requested.

A.7. By discharge of 25 June 2021, the DPA transmitted to the complainant and to the first respondent the aforementioned observations of the second respondent of 9 April 2021.

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

She used the free version of Google Analytics. In doing so, it agreed to the terms of use as well as to the SCC. The data exchange setting was not activated. Google Signals were not used either. In connection with the use of Google Analytics, it was not based on the exception provided for in Article 49(1) GDPR.

A.9. In a summary of comments of 13 August 2021, the complainant submitted the following:

Reference was made to the opinion of 5 May 2021 on the parallel procedure with the JCC: DSB-D155.027. As in the parallel proceedings, the transmitted HAR file could be used to detect that personal data of the complainant had been processed and that the data was transferred to the USA to Google LLC.

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

The first respondent is the operator of the [redacted] settlement portal. She operates [redacted] in the following language versions: [redacted].de, [redacted].eu, [redacted].co.uk and [redacted].pl.

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

The IP address at issue and the cookie data are not personal data. The IP anonymisation function was

activated. Nor is the data attributable to the complainant. The complainant did not explain which IP-address used the Internet-connected device with which he visited the website. It is also unclear whether it was a dynamic or static IP address.

However, even assuming that personal data are available, a risk-based approach should be taken when assessing the adequacy of the transfer to the US. This should be derived from the EDPB's "Schrems II" FAQ and from the European Commission's decision of 4 June 2021 on the new standard contractual clauses. In the present case, account must be taken of the fact that the transmission of the data at issue in the proceedings entails — if at all — only a low basic risk. There is also no disclosure in accordance with PO 12.333, as the aforementioned provision does not authorise the U.S. government to enforce or even request user data from a US provider, it does not receive any instructions addressed to service providers outside the U.S.. FISA § 702 is also irrelevant in view of the encryption and anonymisation of IPaddresses. The second respondent concluded standard contractual clauses with the first respondent. In addition, he implemented additional measures to supplement the standard contractual clauses.

Finally, it should be noted that an infringement of Article 44 et seq. of the GDPR cannot be invoked in the context of a data protection complaint. Nor does the DPA have any competence to identify infringements in the past. In addition, Article 44 et seq. of the GDPR applies only to data exporters.

A.9. With comments of 3. In summary, the complainant submitted the following comments on December 2021:

There is a processing of personal data, evidenced by, inter alia, the annexes submitted. For the account configuration in the Google account one already had in parallel proceedings with the GZ: DSB-D155.027 delivered an opinion.

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

In addition, it should be noted that the combination of cookie data and IP addresses in particular could be linked to tracking and the analysis of geographical location, internet connection and context of the visitor with the cookie data already described. The GDPR also has no "risk-based approach" in Chapter V. This can only be found in certain articles of the GDPR, such as Article 32 leg.cit.

Even if the second respondent did not infringe Article 44 et seq. of the GDPR, the provisions pursuant to Article 28(3)(a) and Article 29 of the GDPR must be taken into account as a 'temporary provision'. If the second respondent follows a corresponding instruction from a US intelligence service, he thus makes the decision to process personal data beyond the specific mandate of the first respondent pursuant to

Articles 28 and 29 of the GDPR and the corresponding contractual documents. As a result, the second respondent becomes the person responsible in accordance with Article 28(10) GDPR. Consequently, the second respondent must, in particular, also comply with the provisions of Article 5 et seq. of the GDPR. A secret transfer of data to US intelligence services in accordance with the law of the United States is without doubt incompatible with Art. 5 para. 1 lit. f GDPR, Art. 5 para. 1 lit. a GDPR and Art. 6 GDPR.

A.10. With opinion of 21. December 2021 brought by the first respondent summarising the following:

As already stated, it did not use Google Signals. As a technically used service provider, the second respondent expressly stated in its comments of 2 November 2021 that IP anonymisation takes place in principle only within the EEA. Only in exceptional cases would web servers outside the EEA be used. In the present case, normal operating conditions would be in place.

A.11. By observations of 9 February 2022, the second respondent essentially reiterated the previous arguments.

It was also argued that the position taken by the complainant had particularly serious and far-reaching practical consequences. This position would cause serious damage to both Austrian companies operating on the world market and the pan-European economy. The web browser-related data at issue are not sufficiently specific to 'separate' a browser. U.S. intelligence services have never issued an order under FISA 702 as regards the type of Google Analytics data at issue.

It is inadmissible to accept the application of a reversal of the burden of proof to the question of the personal reference of the data. The GDPR has no such reversal of the burden of proof. Moreover, this is incompatible with the principles of Austrian procedural law and the presumption of innocence.

Furthermore, there is no representative standing under Article 80(2) GDPR in Austria and cannot be circumvented by allowing NOYB to be mandated by one of its employees for the purpose of conducting a 'model procedure'.

The opinion was accompanied by two documents.

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

B. Subject matter of the complaint

On the basis of the complainant's submissions, it is clear that the subject-matter of the appeal is whether the first respondent has ensured an adequate level of protection in accordance with Article 44 of the GDPR for the transfer of the complainant's personal data to the second respondent, which washttp://www.[redacted].at/triggered by the implementation of the Google Analytics tool on its

websitewww.[redacted].at.

For example, in its observations of 11 February 2021 and 8 June 2021, the complainant expressly requested, pursuant to Section 24(2)(5) of the DSG, that the data transfers in question were inadmissible pursuant to Article 44 of the GDPR.

In this context, it is also necessary to clarify whether, in addition to the first respondent (as data exporter), the second respondent (as a data importer) was obliged to comply with Article 44 GDPR.

The request to impose an immediate ban on the first respondent (as the responsible party) on the transfer of data to the second respondent cannot be ruled out, since the latter has temporarily removed the Google Analytics tool from its website.

Finally, it should be noted that the partial notice in question does not deny the alleged infringements of the second respondent pursuant to Article 5 et seq. of Article 28(3)(a) and Article 29 of the GDPR. Further investigative steps are necessary in this respect and will be discussed in a further decision.

C. Findings of fact

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

The first respondent operates the website www.[redacted].at for the Austrian market http://www.[redacted].at/. In addition, the first respondent also operates [redacted] for the German market(www.[redacted].de), the English-speakingmarket (www.[redacted].eu), the Polishmarket (www.[redacted].pl) and the UK market (www.[redacted].co.ukwww.[redacted].co.uk). The first respondent is established only in Austria and has no other establishments in other Member States of the European Union.

Assessment of evidence in relation to C.1.: The findings made are based on the observations of the first respondent of 22 February 2006. December 2020 (Question 2) and was not disputed by the complainant. In addition, the findings made are based on an official search carried out by the Data Protection Authority at www.[redacted].at http://www.[redacted].at/(requested 18 March 2022).

C.2. The second respondent developed the tool Google Analytics. Google Analytics is a measurement service that enables customers of the second respondent to measure traffic characteristics, among other things. This includes measuring the traffic of visitors visiting a specific website. This makes it possible to understand the behaviour of website visitors and to measure how they interact with a specific website. Specifically, a website operator can create a Google Analytics account and view reports about the website using a dashboard. Google Analytics can also measure and optimise the effectiveness of advertising campaigns that website owners carry out on Google ad services.

There are two versions of Google Analytics: A free version as well as a paid version called Google Analytics 360. The second respondent made the free version available until the end of April 2021. Both versions of Google Analytics have been provided by Google Ireland Limited since the end of April 2021.

Assessment of evidence in relation to C.2.: The findings were based on the second respondent's comments of 9 April 2021 (p. 3 and questions 1 and 2) and were not contested by the complainant. The second respondent's observations of 9 April 2021 were originally conducted in parallel proceedings with the CCC: DSB-D155.027 and brought to the attention of the parties to the present proceedings, as the comments are general comments on the functioning of Google Analytics.

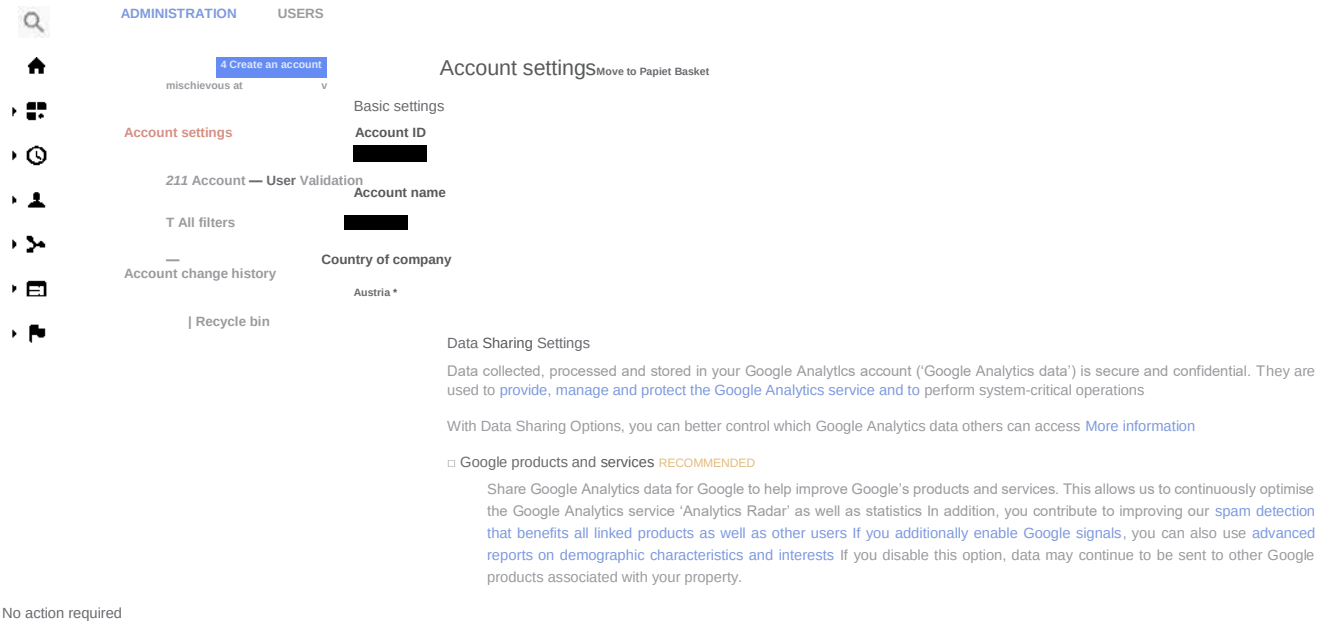
C.3. In any event, the first respondent — as a website operator — took the decision on 11 August 2020 to use the free version of the Google Analytics tool for its [redacted] websites. To this end, it has installed a JavaScript code ("tag") provided by the second respondent in the source code of its website. The first respondent used the tool to enable general statistical analyses of the behaviour of website visitors. The Google Signals add-on tool has not been activated.

Inany case, these analyses are used by the first respondent to present the content of the website www.[redacted].atinhttp://www.[redacted].at/accordance with the general interest of the subject in such a way that the most requested channels can be put in the foreground and the presentation can be adjusted according to the topicality of a specific topic.

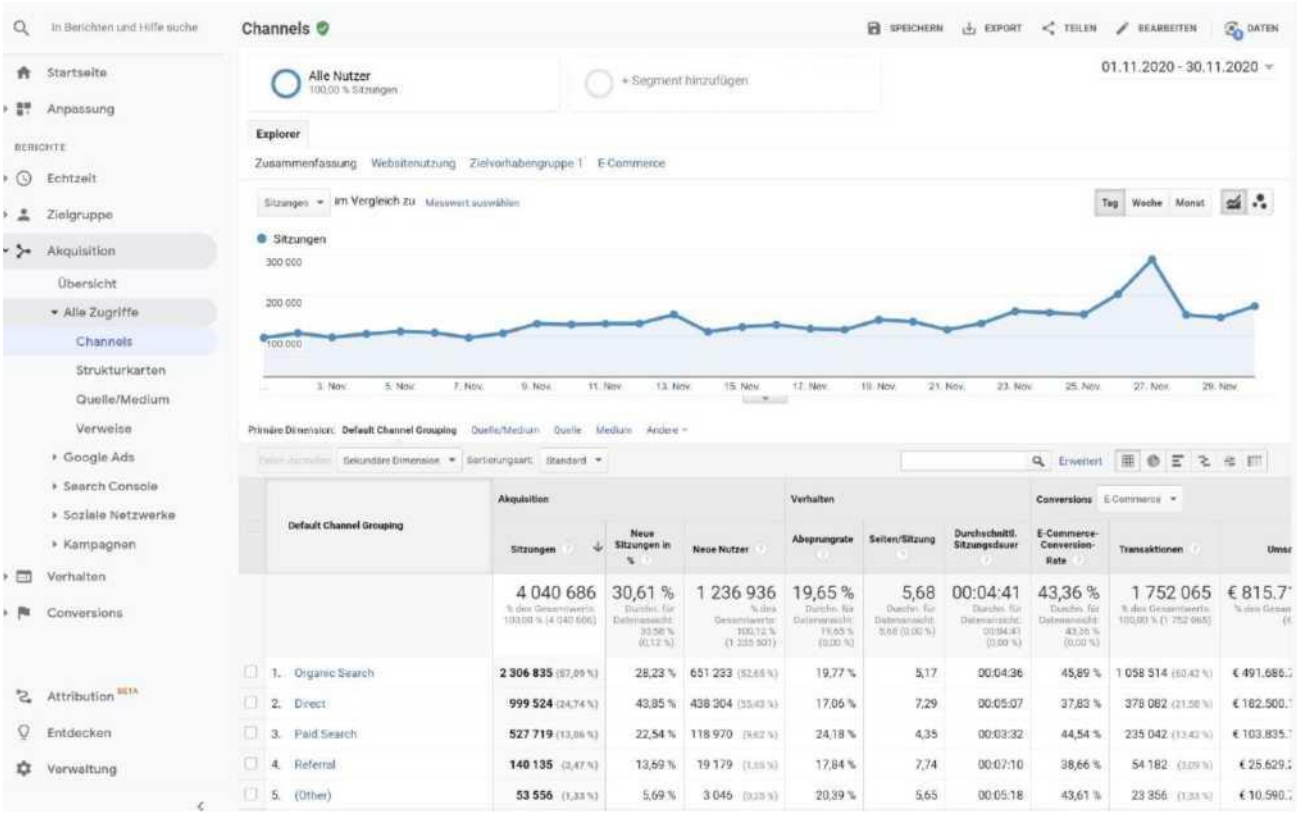
The first respondent created a Google Analytics account for this purpose. The Google Analytics account ID with the account name "[redacted].at" is 109732782. The above evaluations

can be carried out by the first respondent by logging into the "[redacted].at" Google Analytics account and in the dashboard reports on the traffic of www.[redacted].at. The reports are divided into real-time, target groups, acquisitions, behaviors and conversions. The first respondent can select custom requirements for reporting, the second respondent has no influence on this. Nor does the second respondent have any influence on the extent to which the first respondent subsequently uses the reports drawn up.

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



A No action required



Assessment of evidence relating to C.3.: The findings made are based on the submission of the first respondent dated 22. December 2020 and were not contested by the complainant. The above screenshots have been taken from the enclosed Supplement./B and./D.

C.4. The Google Analytics tool has the following functionality: When visitors view the

website www.[redacted].at the JavaScript code inserted in the source code of the website refers to a JavaScript file previously downloaded to the user's device, which then executes tracking operation for Google Analytics. The tracking operation retrieves data via the page request by various means and sends this information to the analytics server via a list of parameters connected to a single pixel GIF image request.

The data collected using Google Analytics on behalf of the website operator comes from the following sources:

- the user's HTTP request;
- Browser/system information;
- (First party) Cookies.

An HTTP request for each website contains details about the browser and the computer that makes the request, such as host name, browser type, referrer and language. In addition, the DOMinterface of the browsers (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 places and reads first-party cookies on a user's browsers that enable the measurement of user 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 are those that are sent to the analytics servers and then processed and end up in the reports of the website operator.

On the second respondent's information page on the Google Analytics tool, extracts of the following information (formatting not reproduced 1:1, requested 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 setthecookie 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. Ifyou have linked your Google Analytics and Google Ads accounts, Google Ads website conversion tags will read this cookie unless you opt-out. Learn more.

Assessment of evidence for C.4.: The findings made are based on the observations of the second respondent of 9 April 2021 (Question 2) in parallel with the CV: DSB-D155.027; and one amnesia Research the Data Protection Authority under https://developers.google.com/analytics/devguides/collection/gajs/cookie-usage and also https://developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id (both queried on 18 March 2022).

C.5. The respondents have entered into a contract entitled "Conditions of Processing for Google Advertising Products". This contract was valid as of 1 January 2020 at least on 11 August 2020. The

contract regulates 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 (opinion of the respondent of 22 January 2020) December 2020, Supplement./G) is based on the factual findings. That contract was subsequently updated on 12 August 2020 and 16 August 2020.

In addition, first and second respondents have 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, too (opinion of the respondents of 22 February 2006). December 2020, Supplement./K) is based on the findings of fact.

In the first contract, with regard to the “Conditions of Processing for Google Advertising Products” covered Categories of data to the Link https://privacy.google.com/businesses/adsservices/ referenced. Under the link mentioned above, extracts of the following are displayed (red emphasis by the DPA, formatting not reproduced 1:1, queried on 18 March 2022):

Order data processing conditions:

Processors' services

The following Google services fall within the scope of the order data processing conditions for Google advertising products:

- Ads Data Hub
- Audience Partner API (former name: DoubleClick Data Platform)
- Campaign Manager 360 (former name: Campaign Manager)
- Display & Video 360 (former designation: DoubleClick Bid Manager)
- Extended conversions
- Google Ad Manager Processor Functions
- Google Ad Manager 360-processor functions
- Google Ads Customer Matching
- Google Ads Retail Sales (direct upload)
- Google Analytics
- Google Analytics 360
- Google Analytics for Firebase
- Google Data Studio
- Google Optimise
- Google Optimise 360
- Google Tag Manager
- Google Tag Manager 360
- Search Ads 360 (former name: DoubleClick Search)

Google is entitled to update this list in accordance with the terms of the order data processing conditions for Google advertising products.

Types of personal data

With regard to the order data processing conditions for Google advertising products (and depending on which processor services are used under the respective agreement), the following types of personal data may constitute the customer's personal data:

Processors' services	Types of personal data
Ads Data Hub	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers
Audience Partner API (former name: DoubleClick Data Platform)	Online markings (including cookie identifiers) and device identifiers
Campaign Manager 360 (former name: Campaign Manager)	Online markings (including cookie identifiers), internet protocol addresses and device identifiers, precise location data, customer-assigned markings
Display & Video 360	Online markings (including cookie identifiers), internet protocol addresses and device identifiers, precise location data, customer-assigned markings
Extended conversions	Names, e-mail addresses, telephone numbers, addresses, markings provided by the customer, onlinemarkings (including Internet protocol addresses)
Google Ad Manager Processor functions	Encrypted signals
Google Ad Manager 360— Processor functions	Encrypted signals
Google Ads Customer Matching	Names, e-mail addresses, addresses and markings provided by the partner
Google Ads Retail Sales (direct upload)	Names, e-mail addresses, phone numbers and addresses
	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers
Goo le Anal ics 360	Online markings (including cookie identifiers), Internet protocol addresses and device identifiers, from Markings awarded to customers

In addition to the conclusion of 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 observations of 9 April 2021 (Question 28). This description is based on 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

Assessment of evidence relating to C.5.: The findings made are based on the observations of the first respondent dated 22. December 2020, question 15. The above supplements are included in the Act and are known to all parties. In addition, the findings made are based on a amnesia Research the Data Protection Authority under https://privacy.google.com/businesses/adsservices/ (requested 18 March 2022). The findings made with regard to the 'additional measures implemented' stem from the second respondent's observations of 9 April 2021 (question 28) and from the observations of the first respondent of 22 April 2021. December 2020 (Question 23). The second respondent's observations of 9 April 2021, which in parallel proceedings with the GZ: DSB-D155.027 is included in the present act and is known to all parties. The finding with regard to the transparency reports results from an official search carried out by the DPA under https://transparencyreport.google.com/user-data/us-national

security?hl=en (requested 18 March 2022).

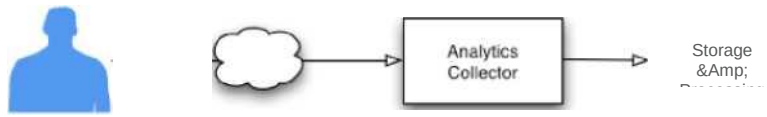
C.6. In the course of the use of the Google Analytics tool, the possibility to use an “IPanonymisation function” is offered. This function was used by the Respondent. As part of the embedding of Google Analytics on the website, the function “anonymizeIP” was set to “true”. However, when loading the relevant scripts of Google servers, the full IP address of a website visitor is transferred to the second respondent. The IP address will only be masked in a second step after it has been entered into the Analytics data acquisition network.

For this purpose: has: the Second respondent to of his Website under https://support.google.com/analytics/answer/2763052?hl=de provided thefollowing information (excerpt, formatting not reproduced 1:1):

Detailed information

Anonymizejp 13 is available in Analytics (in the library “gtag.js” is the gtag (' con-Fig', ' <GA_MEASUREMENT_ID>' j {'anonymize_ip[1]: true})). This enables website owners to request that all IP addresses of their users be anonymised within the product. For example, own privacy statements or the recommendations of local data protection supervisory authorities can be implemented in some countries, which may prohibit the storage of complete IP addresses. The IPs are anonymised or masked as soon as the data is received by Google Analytics and before it is stored or processed.

IP anonymisation in analytics takes place in two steps within the data collection system: via the JavaScript tag and the data acquisition network. These steps are explained below.



Assessment of evidence relating to C.6.: The findings made are based on the observations of the first respondent of 22 February 2006. December 2020 (Question 2) and the annex./C. From Supplement./C, it is clear that the second respondent himself states that the anonymisation of the IP address takes place only in the second step after the collection of data. The finding regarding the date of anonymisation of the IP address is also based on the complainant’s comments of 11 February 2021 (p. 2 f). Finally, the findings made are based on: one amnesia Research the Website under https://support.google.com/analytics/answer/2763052?hl=de (requested 18 March 2022). As can be seen from the legal assessment, it may not be necessary to determine whether the IP address of the complainant’s terminal device was masked within or outside the EEA area in the present case. Findings in this respect could therefore not be made.

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

Assessment of evidence relating to C.7.: The findings were based on the complainant’s submission of

18 August 2020 (p. 2 f) and were not contested by the respondents. The findings made with regard to the basic functions of a Googleaccount are based on an official search carried out by the data protection authority at https://support.google.com/accounts/answer/27441?hl=de https://support.google.com/accounts/answer/27441?hl=de *and https://policies.google.com/privacy*https://policies.google.com/privacy(both consulted on 18 March 2022).

C.8. In the disputed transaction between the complainant's browser and https://[redacted].at/ on 11 August 2020, at 01:26:21.206 CET unique useridentification numbers were processed at least in the cookies "_ga" and _ "gid". Subsequently, on 11 August 2020, at 01:26:23.795 CET, these identification numbers were sent to https://www.google- analytics.com/collectand thus to the second respondent.

Specifically, the following user identification numbers, which are located in the complainant's browser, were transmitted to the second respondent (same values, which each occurred in different transactions, were marked with colors:

Domain	Name	Wert	Zweck
https://[redacted].at/	_ga	GA1.1.165363541.1597101359	Google Analytics
https://[redacted].at/	_gid	GA1.1.1101783526.1597101359	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 included in the request payload for the domain www.google-analytics.com/collect(emphasis added by the DPA):

v=1&_v=j83&aip=1&a=757249675&t=pageview&_s=1&dl=https%3A%2F%2F&ul=de&Amp; de=windows-1252&dt=[redacted]%20 %C3 %96sterreich&sd=24—

bit&sr=1920x1080&vp=1903x910&je=0&fl=32.0 %20r0&_u=QACAAAAB~&jid=&gjid=&cid= 165363541.1597101359 &tid=UA-109732782- 1&_gid=1101783526.1597101359&cd1=Home&z=339628709

These identification numbers make it possible for the respondents to distinguish website visitors and also to obtain information as to whether they are a new or a recurring website visitor to http://www.[redacted].at/ www.[redacted].at.

In addition, the following information (parameter) was also sent to the second respondent via the complainant's browser in the course of inquiries (requests) to https://www.google-analytics.com/collecthttps://www.google-analytics.com/collect (excerpt from the HAR file, Request URL https://www.google-analytics.com/collect https://www.google-analytics.com/collect, excerpt of the request with time stamp 2020-08—
11T01:26:23.795+ 02:00):

General

- Request URL https://www.google-analytics.com/collect
- Request Method GET
- HTTP version HTTP/2
- Remote address 2a00:1450:4016:807:200e

Headers

- Acceptance: */*
- Acceptance encoding: gzip, deflate, br
- Acceptance language: de,en;q=0.5
- Connection: keep-alive
- Content-Length: 303
- Content type: text/plain;charset=UTF-8
- DNT: 1
- Host: www.google-analytics.com
- Origin: https://[redacted].at
- Referer: https://[redacted].at/
- TE: Trailers
- User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0

Size

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

From these parameters, it is possible to draw conclusions about the browser used, the browser settings, language selection, the website visited, the color depth, the screen resolution and the AdSense link number.

The remote address (IPV6 address) 2a00:1450:4016:807:200e is that of the second respondent.

The IP address of the complainant's device is transmitted to the second respondent in thecontextof these

inquiriesto https://www.google-analytics.com/collect.

The content of the HAR file (Annex/4), submitted by the complainant with submission of 18 August 2020, is based on the findings of fact.

*Assessment of evidence relating to C.8.: The findings made are based on the complainant's submission of 18 August 2020 and the HAR file submitted therein, Supplement No/4. A HAR file is an archive format for HTTP transactions. The HAR file has been checked by the Data Protection Authority. The complainant's submissions are in line with the archive data contained therein. The submitted HAR file (or its contents) is known to the parties concerned. In addition, the findings made are based on the complainant's comments of 13 August 2021 and the screenshots contained therein. As stated above, according to the second respondent, the purpose of the identification numbers is to distinguish users. The established dates of cookie setting are calculated from the respective UNIX timestamps. The Unix time is a time definition developed for the Unix operating system and set as the POSIX standard. The Unix time counts the past seconds since Thursday, January 1, 1970, 00:00 UTC. The finding with regard to the remoteaddress results from an official Who Is query by the DPA at*https://ipinfo.io/2a00:1450:4016:807::200e (requested 18 March 2022).

C.9. Insofar as the Google Analytics tool is implemented on a website, the second respondent has the technical possibility to obtain the information that a particular Google account user has visited this website (on which Google Analytics is implemented), provided that this Google account user is logged in to the Google account during the visit.

Assessment of evidence relating to C.9.: In its opinion of 9 April 2021 in parallel proceedings with the JCC: DSB-D155.027 admittedly argued in question 9 that he receives such information only if certain conditions are met, such as the activation of specific settings in the Google account. In the view of the DPA, this argument is not convincing. If a Google account user's wish for "personalisation" of the advertising information received can be met on the basis of a declaration of intent in the account, it is possible, from a purely technical point of view, to obtain the information on the visited website of the Google Account user. In this context, there is an explicit reference to data protection accountability, which will be discussed in more detail in the legal assessment. For the purpose of establishing the facts, this data protection accountability means that the respondent (or, in any case, the first respondent as controller) — and not the complainant or the data protection authority — must provide sufficient evidence. Such sufficient evidence — i.e. that there is no possibility of obtaining data for the second respondent from a technical point of view — 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 expressly provided for in the GDPR.

C.10. The first respondent http://www.[redacted].at/ removed the Google Analytics tool from its website

www.[redacted].at before the outcome of the proceedings at issue.

Assessment of evidence in relation to C.10.: The findings are based on the opinion of the first respondent of 28 May 2021, which was not disputed by the complainant in this respect. In addition, the finding is based on an official search at www.[redacted].at(requested 18 March 2022).

D. From a legal point of view, it follows:

D.1. General information

a) On the competence of the data protection authority

The European Data Protection Board (hereinafter: EDPB) has already dealt with the relationship between GDPR and Directive 2002/58/EC ("e-Privacy Directive") (cf. Opinion 5/2019 on the interaction between the e-Privacy Directive and the GDPR of 12 March 2019).

By decision of 30 November 2018, Zl. DSB-D122.931/0003-DSB/2018, with the relationship between GDPR and the national implementing provision (in Austria now: TKG 2021, BGBl. I No 190/2021 as amended).

It was stated in principle that the e-Privacy Directive (or the respective national implementing provision) of the GDPR acts as *lex specialis*. Thus, Article 95 of the GDPR provides that the Regulation does not impose any additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services on public communications networks in the European Union, in so far as they are subject to specific obligations laid down in the e-Privacy Directive which pursue the same objective.

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

Against this background, the GDPR is applicable to such a data transfer and therefore the data protection authority has competence to deal with the present complaint pursuant to Art. 77 para. 1 GDPR.

b) Article 44 GDPR as subjective right

On the basis of the previous case-law of the data protection authority and the courts, it should be noted that both the lawfulness of data processing pursuant to Article 5(1)(a) in conjunction with Article 6 et seq. of the GDPR and the rights of data subjects postulated in Chapter III of the Regulation can be asserted as subjective right in the context of a complaint pursuant to Article 77(1) GDPR.

The transfer of personal data to a third country which does not guarantee an adequate level of protection within the meaning of Article 44 of the GDPR (as claimed) has not yet been the subject of a complaint procedure before the data protection authority.

In this context, it should be noted that Article 77(1) of the GDPR (and, moreover, also the national provision of Section 24(1) of the DSG) for the exercise of the right of appeal requires only *that " the processing of personal data concerning them infringes this Regulation*".

In its judgment of 16 July 2020, the Court of Justice also held that the finding that *'[i]n the law and practice of a country does not guarantee an adequate level of protection'*, and that *'[t]he compatibility of this (adequacy) decision with the protection of privacy and the freedoms and fundamental rights of persons* may be invoked as a subjective right in*the context of a complaint under Article 77(1) of the GDPR (cf. judgment of the Court of Justice of 16 July 2020, C-311/18, paragraph 158).*

Admittedly, it should be noted that the question referred for a preliminary ruling in the abovementioned proceedings did not concern the 'scope of the right of appeal under Article 77(1) of the GDPR'; however, the ECJ has clearly considered the fact that an infringement of provisions of Chapter V GDPR can also be invoked in the context of a complaint under Article 77(1) GDPR as a necessary condition. From a different perspective, the CJEU would have stated that the question of the validity of an adequacy decision cannot be resolved at all in the context of a complaint procedure.

To the extent that the second respondent also asserts Article 44 GDPR as a subjective right — with reference to the wording of ErwGr 141 leg.cit. — denies that the above-mentioned ErwGr refers to the fact that the 'rights under this regulation' are accessible to a complaint under Article 77(1) of the GDPR (and not: "the rights referred to in Chapter III of this Regulation").

While the GDPR uses the term 'rights of a data subject' at certain points, this does not mean, conversely, that no other norms in which this wording is chosen can also be invoked as subjective law. Most of the provisions of the GDPR are, on the one hand, an obligation of the controller (and partly the processor), but on the other hand can also be invoked as a subjective right to data subjects. For example, it is undisputed that Articles 13 and 14 of the GDPR establish a subjective right of information, even though the right to information is not mentioned in Article 12(2) of the GDPR as "their rights" (i.e. "rights of the data subject") and Article 13 and Article 14 GDPR are designed according to the wording as the informationobligation of the person responsible.

The decisive factor is whether a data subject is affected by an alleged infringement in an individual legal position. The alleged infringement must therefore have a negative impact on and affect the person concerned.

Apart from that, although the ErwGr is an important tool for interpreting the GDPR, they cannot be used to achieve a result contrary to the text of the regulation (as stated above, the fact that the administrative remedy is generally linked to 'processing') (see the judgment of the Court of Justice of 12 May 2005 in Case C-444/03 paragraph 25 and the other case-law cited).

Finally, according to the national case-law of the VwGH, in the event of doubt, it must be assumed that

rules which require administrative action also and precisely in the interests of the person concerned grant him a subjective right, that is to say enforceable by means of a complaint (see, for example, VwSlg. 9151 A/1976, 10.129 A/1980, 13.411 A/1991, 13.985 A/1994).

In the light of the wording of Article 77(1) of the GDPR and the above-mentioned judicature of the CJEU and the VwGH, it should be noted that the obligation laid down in Chapter V and, in particular, the obligation for controllers and processors to ensure the level of protection for natural persons guaranteed by the Regulation can, conversely, also be asserted as subjective right before the competent supervisory authority pursuant to Article 77(1) GDPR.

c) On the competence of the data protection authority to determine

The complainant submitted observations of 11 February 2021 and 8 June 2021 in accordance with § 24(2)(5) DSG expressly requests a declaration that the
Data transfers pursuant to Art. 44 GDPR were inadmissible.

According to the case-law of the VwGH and the BVwG, the data protection authority has a competence to determine breaches of the right to confidentiality in appeal proceedings (for example, the finding of the BVwG of 20 May 2021, Zl. W214 222 6349-1/12E; implicitly the finding of the VwGH of 23 February 2021, Ra 2019/04/0054, in which it dealt with the finding of a breach of professional secrecy in the past, without taking into account the lack of competence of the defendant authority).

There are no objective reasons to use the competence to determine the determination pursuant to Art. 58 para. 6 GDPR in conjunction with § 24 para. 2 point 5 GDPR and paragraph 5 of the DSG for the determination of an infringement of Art. 44 GDPR, since in the present case, among other things, an infringement of law that occurred in the past - namely a transfer of data to the USA — is generally linked to a violation of the GDPR in accordance with § 24 para. 1 DSG — as well as Article 77(1) GDPR.

If the ruling of a decision in a complaint procedure could contain only instructions under Article 58(2) GDPR, there would be no scope for § 24(2)(5) and 24(5) DSG as a result.

Contrary to the opinion of the respondents, Paragraph 24(6) of the DSG is not eligible for the subject-matter of the appeal which is relevant here, since a data transfer is cancelled in the past. In other words: The alleged injustice (here: Incompatibility with Art. 44 GDPR) of a data transfer that has already been completed is not accessible to a conclusion of the procedure pursuant to § 24 para. 6 DSG.

In the light of these considerations, it should be noted, as a further interim conclusion, that the DPA's powers of determination are present in the present appeal procedure.

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

In summary, the second respondent stated in its last observations of 9 February 2022 that a decision

granting the appeal would have serious economic consequences.

In this regard, it should be noted that the data protection authority is prohibited from economic or political considerations and that these considerations are to be taken into account only on a point-by-point basis in the context of the interpretation of the GDPR, for example in the context of a balancing of interests under Article 6(1)(f) of the GDPR.

In accordance with the primary law Art. 8(3) EU-GRC and the secondary law Art. 58(1)(f) GDPR, the Data Protection Authority has on the contrary the obligation to take a decision in the context of data protection complaints, taking into account the position of the Court of Justice in the judgment of 16 July 2020, Case C-311/18, with regard to the legal situation of the USA.

Thus, in its judgment of 16 July 2020, the CJEU expressly stated that the relevant legal situation in the USA — below — is not compatible with the fundamental right to data protection under Article 8 of the EU-CFR, which is why the EU-US adequacy decision ('Privacy Shield') was also declared invalid.

An economic or political agreement to ensure data transfers between Europe and the US has to be reached by other bodies, but not by supervisory authorities. The arguments put forward by the second respondent concerning the 'serious and far-reaching practical significance' of the decision in question and the economic studies cited must therefore be omitted.

D.2. Point 1

By decision of 2 October 2020, Zl. D155.026, 2020-0.526.838, pending the determination of which authority is responsible for the substantive conduct of proceedings (lead supervisory authority) or pending the decision of a lead supervisory authority or the EDPB.

In the opinion of the Data Protection Authority, Article 4(23)(b) GDPR is fulfilled, since the first respondent's online comparison portal [redacted] — as noted — on the Austrian (www.[redacted].at), German (www.[redacted].de), Polish (http://www.[redacted].pl) and English-speakingmarket (www.[redacted].eu) and is undisputed for all versions of [redacted] the website operator. Thus, the procedure under Article 56 in conjunction with Article 60 et seq. of the GDPR ('One-Stop-Shop') was to be conducted.

Subsequently, the data protection authority — as the lead supervisory authority — submitted a draft decision to the supervisory authorities concerned in accordance with Article 60(3) GDPR.

In the absence of any relevant and reasoned objections to the draft decision, the suspension decision of 2 October 2020 had to be corrected and communicated to the parties pursuant to Article 60(7) and (8) of the GDPR.

Since, of its own motion, decisions which do not give rise to a right to a person may be annulled or

altered by the authority which issued the decision or, in the exercise of the supervisory right, by the relevant higher authority, and as a result of a stay of proceedings by a party to the proceedings, no right to a non-decision arises, the above-mentioned decision of 2 October 2020 was also open to a remedy pursuant to Paragraph 68(2) of the AVG.

D.2. Point 2. (a)

a) General information on the concept of "personal data"

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

According to the legal definition of Article 4(1) GDPR, "*personal data is all information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); a natural person 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 specific characteristics that can be identified as an expression of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person shall be regarded as identifiable ".*

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

- unique online 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 visit to the website;
- the IP address of the device used by the complainant.

It is necessary to verify whether this information falls within the definition of Article 4(1) GDPR, i.e. personal data of the complainant.

b) Identification numbers as "personal data"

With regard to the online identifiers, it should be recalled that the cookies "_ga" or "cid" (Client ID) and "_gid" (User ID) contain unique Google Analytics identification numbers and have been stored on the complainant's device or browser. As noted, it is possible for certain bodies — for example the respondents — to distinguish website visitors using these identification numbers and also to obtain information as to whether it is a new or a recurring website visitor to www.[redacted].at. In other words:

Only the use of such identification numbers allows a distinction between websitevisitors, which was not possible before this assignment.

In the opinion of the Data Protection Authority, an interference with the fundamental right to data protection pursuant to Article 8 EU-GRC and § 1 of the DSG already exists if certain bodies take measures — here the assignment of such identification numbers — in order to individualise website visitors in this way.

There is no need for a measure of "identifiability" in such a way that it must immediately be possible to associate such identification numbers with a specific "face" of a natural person, in particular the name of the complainant (see Opinion 4/2007, WP 136, 01248/07/EN of the former Article 29 Working Party on the concept of "personal data", p. 16 f); see the guidance provided by the supervisory authorities for telemedia providers in March 2019, p. 15).

In favour of such an interpretation, ErwGr 26 GDPR argues that the question of whether a natural person is identifiable *takes into account all means likely to be used by the controller or another person in the general discretion to identify the natural person directly or indirectly, such as separating the natural person*. "singling out"). The term 'separate' means 'chosen from a set' (see https://www.duden.de/rechtschreibung/aussondern, questioned on 18 March 2022), which corresponds to the above considerations on the individualisation of website visitors.

The literature also explicitly states that a "digital footprint" which allows devices to be clearly individualised — and subsequently the specific user — is already a personal date (cf. *Karg* in *Simitis/Hornung/Spiecker*, GDPR Comment Art. 4 Z 1 Rz 52 mwN). Due to the uniqueness of the identification numbers, this consideration can be transferred to the present case, especially since these identification numbers can also be combined with other elements — which is to be discussed in greater detail at once.

In so far as the respondents lead to the meeting that no "means" would be used to link the identification numbers at issue here with the complainant's person, it should be pointed out again that the implementation of Google Analytics on www.[redacted].at results inhttp://www.[redacted].at/ a separation within the meaning of the ErwGr 26 GDPR. In other words: If you use a tool that just allows such separation, it is not possible to take the view that, according to "general discretion", no means should be used to make natural persons identifiable.

At this point, it should be noted that the European Data Protection Supervisor (EDPS) is also of the opinion that "separation" by marking a terminal device must be considered as a personal date. Thus, in his decision of 5 January 2022, the EDPS: 2020-1013 against the European Parliament, inter alia:

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."

Tracking cookies such as Stripe and 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 data sets containing identification features that can be used to separate 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 is required to apply Regulation (EU) 2018/1725, which applies to data processing by the 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, those considerations can easily be transposed to the present case.

As an interim result, it should therefore be noted that the Google Analytics identification numbers at issue here are already in principle to be qualified as personal data (in the form of an online identifier) in accordance with Art. 4 Z 1 GDPR.

c) Combination with other elements

The fulfillment of Article 4(1) GDPR becomes even clearer if one takes into account that such identification numbers can be combined with other elements:

By combining all these elements — that is, unique identification numbers and the other information mentioned above, such as browser data or IP address — it is all the more likely that the complainant can be identified (see again ErwGr 30 GDPR). Such a combination makes the complainant's "digital footprint" even more unique.

The respondents' arguments relating to the "anonymisation function of the IPaddress" may be omitted, since the complete IP address is processed at least for a certain — albeit very short — period on Google LLC's server. This short data processing period is sufficient to comply with Article 4(2) of the GDPR. According to the case-law of the BVwG, it cannot be inferred from Article 4(2) in conjunction with Article 6 GDPR that a certain 'minimum processing' must be assumed (cf. the finding of the BVwG of 3 September 2019, Zl. W214 2219944-1).

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

Similarly, the question of whether an IP address is a personal date, viewed in isolation, may be left out, since — as mentioned — it can be combinedwith other elements (in particular the Google Analytics identification number). In this context, however, it should be noted that, according to the ECJ's case-law, the IP address may constitute a personal date (see the judgments of the Court of Justice of 17 June 2021, C-597/19, paragraph 102, and of 19 October 2016, C-582/14, paragraph 49), and that the IP address does not lose its status as a personal date solely because the means of identification lie with a third party.

d) Traceability to the complainant

However, irrespective of the above considerations, there must be no traceability to the complainant's 'face':

Indeed, it is not necessary for the respondents to be able to establish a personal connection on their own, that is to say that all the information necessary for identification is with them (cf. the judgments of the Court of Justice of 20 June 2006). December 2017, C-434/16, paragraph 31, and of 19 October 2016, C-582/14, paragraph 43). Rather, it is sufficient that anyone can — with legally permissible means and reasonable effort — make this personal reference (cf. Bergauer *in* Jahnel*,* GDPR comment Art. 4 Z 1 Rz 20 mVa *Albrecht/Jotzo, The* new data protection law of the EU 58).

Such an interpretation of the scope of Art. 4 Z 1 GDPR can be derived — in addition to the legal and literature sources mentioned — from ErwGr 26 GDPR, according to which, in the case of identification, not only the means of the person responsible (here: the first respondent) but also that of ' another person' (English version of the Regulation: "by another person"). This is also the result of the idea of providing data subjects with the greatest possible protection of their data.

In particular, the CJEU has also repeatedly stated that the scope of the GDPR should be understood "very broad" (see, for example, the judgments of the CJEU of 22 June 2021, C-439/19, paragraph 61; with regard to the comparable legal situation in that regard, the judgments of 20. December 2017, C-434/16, paragraph 33, and of 7 May 2009, C-553/07, paragraph 59).

It is not overlooked that according to ErwGr 26 GDPR it is also to be taken into account with which "probability" anyone uses means to identify natural person directly or indirectly. Indeed, in the view of the Data Protection Authority, the term 'someone' — and thus the scope of Article 4(1) of the GDPR — should not be interpreted so broadly that any unknown actor could theoretically have special knowledge in order to establish a personal relationship; this would result in almost any information falling within the scope of the GDPR and making it difficult or even impossible to distinguish it from non-personal data.

Rather, the decisive factor is whether identification can be made with reasonable and reasonable effort (see the decision of 5. December 2018, GZ DSB-D123.270/0009- DSB/2018, according to which personal data no longer exists if the controller or a third party can only establish a personal connection with a disproportionate effort).

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

i) This is, first of all, the second respondent:

As can be seen from the findings of fact, the complainant was logged in[http://www.[redacted].at/](http://www.[redacted].at/) with his

Google account at the time of the visit to the website www.[redacted].at. The second respondent has stated that the latter receives information due to the fact that the Google Analytics tool is implemented on a website. This includes information that a certain Google account user has visited a certain website (see comments of 9 April 2021, question 9).

This means that the second respondent received at least the information that a user logged in to the complainant's Google account visitedthe websitewww.[redacted].at.

Therefore, even if one takes the (not required) view that the above-mentioned onlineidentifiers must be assigned to a certain "face", such assignment can in any case be made via the complainant's Google account.

It is not overlooked by the second respondent that certain conditions must be met for such an assignment, such as the activation of specific settings in the Google account (see again his opinion of 9 April 2021, question 9).

However, if, as the complainant has stated convincingly, the identification of a website visitor depends only on whether certain declarations of intent are made in the account, there are (from a technical point of view) all possibilities for identification. On a different perspective, the second respondent could not respond to a user's wishes expressed in the account settings for 'personalisation' of the advertising information received.

In this context, it is necessary to make explicit reference to the unequivocal wording of Article 4(1) of the GDPR, which is linked to a skill ('can be identified') and not to whether an identification is ultimately carried out.

Likewise, the accountability of the first respondent as enshrined in the GDPR — as the person responsible for this purpose, should be explicitly mentioned below — in accordance with Article 5(2) in conjunction with Article 24(1) in conjunction with Article 28(1) GDPR, in order to ensure and to be able to prove that the processing (with the assistance of a processor) is carried out in accordance with the Regulation. It is therefore a debt to bring.

This also includes proof that processing is currently not subject to the regulation, especially since the respondents have concluded data protection contracts in relation to Google Analytics, which in turn presuppose the applicability of the GDPR. However, such evidence was not provided, despite the possibilities granted several times.

Contrary to Chapter V — on this point below — Article 5(2) in conjunction with Article 24(1) of the GDPR is now actually based on a risk-based approach. The higher the risk associated with data processing, the higher the standard of evidence to be provided to demonstrate compliance with the GDPR.

In the present case, a high risk and therefore a high standard of proof must be assumed:

In any case, the second respondent developed the product Google Analytics in order to collect as much information as possible from website visitors. Thus, the latter himself states that due to the fact that Google Analytics is embedded on a website, it may receive the information that a certain Google account holder has visited such a website. In other words: In return for the fact that website operators can use the free version of Google Analytics, the second respondent will be given technical possibilities to collect data and further enrich Google account holders' profiles. It cannot therefore be assumed that Google Analytics is a mere web analysis service for websiteoperators.

On the basis of this high standard of proof, it is not sufficient to merely claim that the second respondent receives the information at issue only if certain settings are selected in the Google account. Further evidence (such as screenshots, detailed technical descriptions, etc.) was not provided, despite an extensive investigation.

It is not overlooked that accountability pursuant to Art. 5 para. 2 in conjunction with Art. 24 para. 1 GDPR expressly affects the first respondent as responsible. However, the granting part of the decision in question is (only) directed against the first respondent, who embedded the product Google Analytics on her website.

In so far as the second respondent refers in this context to the presumption of innocence pursuant to Article 48(1) EU-GRC, it must be pointed out that, in the present case, it is exclusively a complaint procedure under Article 77(1) GDPR and not an administrative criminal procedure. Apart from that, the appeal against the second respondent was dismissed.

Finally, if the second respondent states that such a 'distribution of burden of proof' is incompatible with Austrian procedural law, it must be pointed out to him that such a distribution is quite common in the legal order — in particular in consumer protection law — (see, for example, Paragraph 924 of the ABGB or § 11(1) VGG, BGBl. I No 175/2021; the close relationship between the Consumer protection law and the fundamental right to data protection see also ErwGr 42 GDPR).

ii) Regardless of the second respondent, however, and this is of greater relevance on a case-by-case basis, the U.S. authorities must be taken into account:

As the complainant has just as rightly pointed out, US intelligence services take certain Online identifiers (such as: the IP address or unique Identification numbers) als Starting point for monitoring from individuals. In this way, in particular: not it is ruled out that these intelligence services have already collected information that allows the data transmitted here to be traceable to the complainant's person.

The fact that this is not merely a 'theoretical threat' is apparent from the judgment of the Court of Justice of 16 July 2020, C-311/18, which ultimately declared the EU-US adequacy decision ('Privacy Shield')

invalid because of the incompatibility of such methods and possibilities of access by the US authorities with the fundamental right to data protection under Article 8 of the EU-GRC.

In particular, this can also be seen in the second respondent's transparency report, referred to in the findings of fact, which demonstrates that requests for data from US authorities to the second respondent are made. For example, metadata and content data can be requested from the second respondent.

Admittedly, it is not overlooked that the first respondent is of course not able to verify whether such access by US authorities occurs on a case-by-case basis — i.e. per website visitor — and which information is already available by US authorities; conversely, this circumstance cannot be blamed on persons such as the complainant. It was ultimately the first respondent as a website operator who — despite the publication of the aforementioned judgment of the CJEU of 16 July 2020 - continued to use the Google Analytics tool.

Specifically, therefore, the information was provided that the complainant, with a terminal device marked with a unique Google Analytics identification number, at a certain point in time with certain browser settings and a specific IP address, is a specific website (here: a comparison portal in the form of [redacted]).

It is true, in principle, that this is (at first) only information about a particular terminal device. However, just as the location data of a vehicle obtained by means of a GPS tracker may at the same time also constitute personal data on the driver's stay, the relevant information here constitutes personal data of the person most likely to use the terminal device.

This is the complainant's case in the present case, especially since he was (indisputably) logged in with the personal Google account in the browser at the time of accessing the website. There are no indications that the complainant has handed over his access data to third parties and, as far as can be seen, has not been claimed by any party.

A measure to the effect that "security" has to be determined which natural person has used the terminal device cannot be derived from Art. 4(1) GDPR and is not required either:

In this regard, information belonging to an end device or an account would always be non-personal data, since in principle it can never be ruled out that the terminal device or access data has 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 Article 4(1) GDPR, which in turn contradicts the ECJ's judicature, which assumes a very broad scope.

As a further interim conclusion, it should therefore be noted that the information mentioned in the findings of fact under C.8 (in combination in any case) is personal data in accordance with Art. 4 Z 1 GDPR.

e) Role distribution

As already stated, the first respondent, as a website operator, took the decision to implement the Google Analytics tool on http://www.[redacted].at"the website www.[redacted].at. Specifically, it has inserted a JavaScript code ('tag') provided by the second respondent in the source code of her website, thereby running this JavaScript code when visiting the website in the complainant's browser. In this regard, the first respondent stated that the above-mentioned tool is used for statistical analysis of the behaviour of website visitors (see the comments of 22. December 2020, question 2).

As a result, the first respondent decided on the "purposes and means" of the data processing associated with the tool, which is why this (in any case) is to be regarded as the controller within the meaning of Art. 4 Z 7 GDPR.

As regards the second respondent, it should be noted that the subject-matter of the appeal in this case relates (only) to the transfer of data to the second respondent to the USA. A possible further processing of the information referred to in the findings of fact under C.8 (by Google Ireland Limited or the second respondent) is not subject to appeal and has therefore not been determined in this direction.

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

D.3. Point 2. (b)

a) Scope of Chapter V GDPR

First, it is necessary to verify whether the first respondentis subject to the obligations laid down in Chapter V of the Regulation.

Pursuant to Article 44 of the GDPR, any *transfer of personal data which is already being processed or which is to be processed after its transfer to a third country or an international organisation is permitted only if the controller and the processor comply with the conditions laid down in this Chapter and that the other provisions of this Regulation are also complied with; this shall also apply to any onward transfer of personal data from the third country or international organisation concerned to another third country or international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection afforded to natural persons by this Regulation is not undermined.'*

In 'Guidelines 5/2021 on the relationship between the scope of Article 3 and the requirements for international traffic pursuant to Chapter V of the GDPR' (currently still in public consultation), the EDPB identified three cumulative conditions as to when there is a 'transmission to a third country or an international organisation' within the meaning of Article 44 of the GDPR (ibid. paragraph 7):

- the controller or processor is subject to the GDPR for the processing in question;
- the controller or processor ('data exporter') discloses, by transfer or otherwise, personal data which are the subject of such processing to another controller, a joint controller or a processor ('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 processing in question pursuant to Article 3 of the GDPR.

The first respondent is based in Austria and is responsible for the operation of the website www.[redacted].at data protection law. In addition, the first respondent (as a data exporter) disclosed personal data of the complainant by proactively implementing the Google Analytics tool on its website www.[redacted].at http://www.[redacted].at/ and by transmitting data to the second respondent (to the USA) as a direct consequence of this implementation. Finally, the second respondent has its registered office in the USA.

Since all the conditions set out in the EDPB guidelines are met, the first respondent, as the dataexporter, is subject to the provisions of Chapter V of the Regulation.

b) Rules of Chapter V GDPR

Subsequently, it is necessary to verify whether the transfer of data has taken place in accordance with the requirements of Chapter V of the GDPR to the USA.

Chapter V of the Regulation provides for three instruments to ensure the adequate level of protection required by Article 44 of the 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 CJEU has ruled that the EU-US adequacy decision ('Privacy Shield') is invalid without maintaining its effect (see judgment of 16 July 2020, C-311/18, paragraphs 201 f).

The data transmission in question is therefore not covered by Art. 45 GDPR.

d) Appropriate safeguards

As can be seen from fact finding C.5, the respondents have standard data protection clauses (as follows: SDK) pursuant to Art. 46 para. 2 lit. c GDPR for the transfer of personal data to the USA ("Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses". Specifically, at the time of appeal, those clauses were those as amended by Commission Implementing Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors in third countries pursuant to Directive 95/46/EC of the European Parliament and of the Council, OJ 2010/39, p. 5.

In the aforementioned judgment of 16 July 2020, although the CJEU stated that SDK as an instrument for international data traffic could not be criticised, the CJEU also pointed out that SDK by its very nature is a treaty and therefore cannot bind authorities from a third country:

'It follows that there are situations in which, in the light of the legal situation and practice in the third country concerned, the recipient of such a transfer can guarantee the necessary data protection solely on the basis of the standard data protection clauses, but also situations in which the arrangements contained in those clauses may not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, for example, if the law of that third country allows its authorities to interfere with the rights of data subjects with regard to that data' (ibid. paragraph 126).

However, a more detailed analysis of the legal situation of the USA (as a third country) may not be carried out at this point, as the CJEU has already dealt with it in the above-mentioned judgment of 16 July 2020. It concluded that the EU-US adequacy decision does not provide an adequate level of protection for natural persons under the relevant US law and the implementation of official monitoring programmes, inter alia based on section 702 of the FISA and E.O. 12333 in conjunction with the PPD-28 (ibid. paragraph 180 et seq.).

These considerations can be applied to the present case:

For the data protection authority, there is no doubt that the second respondent is to be qualified as an electronic communications service provider within the meaning of 50 U.S. Code § 1881(b)(4) and is therefore subject to supervision by US intelligence services pursuant to 50 U.S. Code § 1881a ("FISA 702"). Accordingly, the second respondent has an obligation to provide the US authorities with personal data pursuant to the 50 U.S. Code § 1881a.

As is apparent from the second respondent's Transparency Report, such requests are also regularly made by US authorities to the latter (seehttps://transparencyreport.google.com/user-data/us-national-security?hl=en, questionedon 18 March 2022).

Against this background, in its judgment of 16 July 2020, the CJEU also stated that ' *standard data protection clauses cannot, by their very nature, provide guarantees that go beyond the contractual obligation to ensure compliance with the level of protection required by EU law'* and that '[t]he *situation*

in a given third country may require the controller to take additional measures to ensure compliance with that level of protection' (ibid., paragraph 133).

The data transmission 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 supplement transfer tools to ensure the level of protection of personal data under Union law V. 2.0', the EDPB stated that if the law of the third country affects the effectiveness of appropriate safeguards (such as SDK), the data exporter must either suspend the transfer of data or implement additional measures (ibid. paragraphs 28 et seq.).

Such "additional measures" within the meaning of the judgment of the CJEU of 16 July 2020 may be contractual, technical or organisational according to the recommendations of the EDPB (ibid. paragraph 52):

With regard to contractual measures, it is stated that *"[t]he guarantees provided by the transfer tool and the relevant legislation in the third country do not meet all the conditions necessary to ensure a level of protection which is substantially equivalent to that in the EU, taking into account all the circumstances of the transfer. As the nature of the contractual measures cannot bind the authorities of the third country in general if they are not party to the contract, they must be combined with other technical and organisational measures in order to ensure the necessary level of data protection. The mere fact that one or more of these measures have been selected and applied does not necessarily mean that it is systematically ensured that the intended transfer meets the requirements of EU law (granting an essentially equivalent level of protection)'* (ibid., paragraph 99).

With regard to organisational measures, it is stated that *"[...)" may be internal strategies, organisational methods and standards that the controllers and processors could apply to themselves and impose on data importers in third countries. Depending on the particular circumstances of the transfer and the assessment of the legal situation in the third country, organisational measures to supplement the contractual and/or technical measures are necessary to ensure that the protection of personal data is substantially equivalent to the level of protection afforded in the EEA* (ibid. paragraph 128).

As regards technical measures, the aim is to ensure that "the access *of authorities in third countries to the data transmitted does not undermine the effectiveness of the appropriate safeguards referred to in Article 46 GDPR. Even if access by the authorities is in accordance with the law in the country of the data importer, these measures must be considered if access by the authorities goes beyond what constitutes a necessary and proportionate measure in a democratic society. These measures aim to exclude potentially infringing access by preventing public authorities from identifying, accessing information about data subjects, identifying them in other contexts or linking the data transmitted to other*

datasets, including data on online identifiers of devices, applications, tools and protocols used by data subjects in other contexts (ibid. paragraph 79).

Finally, the EDPB stated that such 'additional measures' should be regarded as effective within the meaning of the judgment of 16 July 2020 only*if and to the extent that the measure precisely fills the legal gaps identified by the data exporter in his examination of the legal situation in the third country. If the data exporter is ultimately unable to achieve a substantially equivalent level of protection, he or she may not transfer the personal data'* (*ibid.* paragraph 75).

With regard to the present case, this means that it is necessary to examine whether the "additional measures taken" by the second respondent close the gaps in legal protection identified in the ECJ judgment of 20 June 2020, i.e. the access and monitoring 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 (see its observations of 9 April 2021, question 28).

With regard to the contractual and organisational measures set out above, it is not clear to what extent notification of data requests to the data subject (should this be permissible in individual cases), the publication of a transparency report or a "directive for dealing with government requests" are effective in the sense of the above considerations. It is also unclear to what extent the "careful examination of any request for access to data" constitutes an effective measure, since in the aforementioned judgment of 20 June 2020 the CJEU ruled that admissible (i.e. legal) requests from US intelligence services are not compatible with the fundamental right to data protection under Article 8 of the EU Charter.

As far as the technical measures are concerned, it is also not clear — and the Respondent has also not explained — to what extent the protection of communications between Google services, the protection of data in transit between data centres, the protection of communications between users and websites or an "on-site security" actually prevent or restrict the access of US intelligence services on the basis of US law.

If the second respondent subsequently refers to encryption technologies, such as the encryption of 'rest data' in the data centres, the EDPB's recommendations 01/2020 should be re-committed to the respondent. It states that a data importer (such as the second respondent) subject to 50 U.S. code § 1881a ('FISA 702') has a direct obligation to grant access to it or to release it, as regards imported data held or held in his possession or under his control. This obligation may also explicitly cover cryptographic keys without which the data are not readable (ibid. paragraph 81).

As long as the second respondent thus has the possibility of accessing data in plain language, the technical measures introduced at the meeting cannot be considered effective in the sense of the above

considerations.

The second respondent argues that, as a further technical measure, the meeting states that ' *to the extent that '... Google Analytics data are personal data for the measurement of website owners, they must be regarded as pseudonymous'* (see its opinion of 9 April 2021, p. 26).

However, this is counteracted by the German Data Protection Conference's convincing *view that "the fact that users are made identifiable by means of IDs or identifiers does not constitute a pseudonymisation measure within the meaning of the GDPR. In addition, these are not appropriate safeguards to comply with data protection principles or to safeguard the rights of data subjects when IP addresses, cookie IDs, advertising IDs, unique user IDs or other identifiers are used to (re)recognise users. This is because, unlike in cases where data is pseudonymised in order to conceal or delete the identifying data so that the data subjects can no longer be addressed, IDs or identifiers are used to make individual individuals distinguishable and addressable. Consequently, there is no protective effect. These are therefore not pseudonymisations within the meaning of ErwGr 28, which reduce the risks to data subjects and help controllers and processors to comply with their data protection obligations'* (see guidance provided by the supervisory authorities for telemedia providers in March 2019, p. 15).

Moreover, the second respondent's argument cannot be accepted either because the Google Analytics identifier — as explained above — can be combined with other elements and even linked to a Google account which is undisputedly attributable to the complainant.

The "anonymisation function of the IP address" is not effective, as the data is processed at least for a certain period by the second respondent, as explained above. Even assuming that the IP address was processed within the period only in servers in the EEA, it should be noted that under the relevant US law, the second respondent may nevertheless be obliged by US intelligence services to provide the IP address (see in detail the 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).

Apart from this, the IP address is, in any case, only one of many "puzzle parts" of the complainant's digital footprint.

As a further interim conclusion, it should therefore be noted that the 'additional measures' at issue are not effective, since they do not close the legal protection gaps identified in the judgment of the CJEU of 20 June 2020, i.e. the access and monitoring possibilities of US intelligence services.

The data transmission in question can therefore not covered by Art. 46 GDPR.

D.4. Point 2.(c)

a) Article 49 GDPR

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

Consent pursuant to Art. 49 para. 1 lit. a GDPR has not been obtained. Nor is it clear to the data protection authority how any other offence under Art. 49 GDPR should be fulfilled.

The data transfer in question cannot therefore be based on Art. 49 GDPR.

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

The second respondent further submits — in summary — that the risk of data transfer to the US must be taken into account and that the authority in question is too strict. It is not appropriate to follow these arguments:

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

Art. 44 GDPR

General principles of data transmission

Any transfer of personal data which is already being processed or which is to be processed after its transfer to a third country or an international organisation shall be permitted only if the controller and the processor comply with the conditions laid down in this Chapter and comply with the other provisions of this Regulation; this shall also apply to any onward transfer of personal data from the third country or international organisation concerned to another third country or international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection afforded to natural persons by this Regulation is not undermined.

Rather, it must be inferred from the wording of Article 44 GDPR that every data transfer to a third country (or an international organisation) must be ensured that the level of protection guaranteed by the GDPR is not undermined.

The outcome of an infringement of Article 44 GDPR does not therefore depend on whether there is a certain "minimum risk" or whether US intelligence services have actually accessed data. According to the wording of this provision, an infringement of Article 44 GDPR already exists when personal data are transferred to a third country without a corresponding level of protection.

In the context of those provisions of the GDPR, where a risk-based approach is actually to be adopted ("the higher the processing risk, the more measures to be implemented"), the legislator has also explicitly and without doubt regulated this. For example, the risk-based approach is provided for in Article 24(1) and (2), Article 25(1), Article 30(5), Article 32(1) and (2), Article 34(1), Article 35(1) and (3) or Article

37(1)(b) and (c) GDPR.

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

Also the reference on the 'free movement of data' means: for the point of view of the Second respondent nothing to win:

It is completely undisputed that the GDPR should (also) guarantee the free movement of data. However, the free flow of data is under the premise that the provisions of the GDPR — including Chapter V — are fully complied with. There is no provision for softening in the sense of an "economically friendly interpretation" of the provisions of Chapter V in favour of the free movement of data. Economic interests were also irrelevant in the aforementioned judgment of the CJEU of 16 July 2020.

The further argument that the "risk-based approach was confirmed by the CJEU in its judgment of 16 July 2020" cannot be understood:

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

The second respondent seems to derive a risk-based approach from the words 'adequate level of data protection' used by the ECJ. This cannot be accepted, as the ECJ used this sequence of words with reference to ErwGr 108 GDPR. It is clear from ErwGr 108 of the Regulation that 'adequate level of data protection' means that the rights of data subjects must be respected in an appropriate manner.

With regard to the legal situation of the US, the CJEU has now just assumed that due to the disproportionate access possibilities of US authorities, no "adequate level of data protection" can be assumed, which is why it has finally declared the EU-US adequacy decision to be invalid.

The CJEU has not explicitly considered that the obligations to which a US-certified company is subject to a Privacy Shield may nevertheless be appropriate on a case -by-case basis (for example, because the certified company receives only non-sensitive or non-criminal relevant personal data).

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

It should be noted that Implementing Decision (EU) 2021/914 does not include a risk-based approach. The present implementing decision, adopted following the judgment of the Court of Justice of 16 July

2020, presupposes, on the contrary, that, in accordance with Article 14 thereof, the contracting parties to standard data protection clauses must now review the local laws and obligations in the case of access to the data by public authorities prior to the transfer of data to a third country.

In so far as the second respondent derives the alleged position of the European Commission from the (non-binding) ErwGr 20 of the abovementioned Implementing Decision, it must be pointed out that, even in ErwGr 20, no risk-based approach is assumed:

ErwGr 20 of that Implementing Decision correctly seeks to ensure that, when assessing the level of data protection in a third country, account must be taken, in particular, of the circumstances of the transfer.

Based on the example of the legal situation of the USA, it is necessary to verify, for example, whether in individual cases data is transmitted to an provider of electronic communications services within the meaning of 50 U.S. Code § 1881(b)(4), otherwise the corresponding access possibilities of according to FISA 702 are not applicable. If Austria were a third country, it would be necessary to check before data transfers to Austria whether the specific types of data transmitted, for example, fall within the scope of the (now) State Protection and Intelligence Service Act, BGBl. I No 5/2016, as amended, and whether the access possibilities of the Directorate for State Protection and Intelligence Service are proportionate.

However, this is (only) an examination of whether the local legislation and obligations in the case of access by public authorities to the data conflict with 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 way impute a completely new content to the requirements of Article 44 of the GDPR (see, for example, on the primacy of the text of the regulation, the judgment of the Court of Justice of 12 May 2005, C-444/03, paragraph 25).

Finally, the reference to EDPB Recommendation 01/2020 on measures to supplement transmission tools to ensure the level of protection of personal data under EU law cannot help the second respondent’s position:

Thus, as already pointed out in the context of Implementing Decision (EU) 2021/914, the body of the recommendations cited by the second respondent merely states that it is necessary to verify, for each transfer of data, whether the problematic laws of the third country are applied and precisely that it is not necessary to verify the sensitivity or non-sensitive nature of the personal data transferred.

Finally, in so far as the second respondent submits that U.S. intelligence services have no interest in the data processed at all — for example by stating that the information on “screen resolution is an industry standard” — it must be pointed out that it is not a matter of any interest of US intelligence

services, but rather of their means of access.

However, it should be noted that the added value of the information lies in the fact that it can be combined (see also the definition of "fingerprinting" in the Internet Architecture Board RFC6973, according to which "fingerprinting" is the process in which an observer identifies a device or an application body with sufficient probability on the basis of several information elements). For example, the IP address processed — as part of the digital footprint — can be used to determine which internet provider is being used and in which region the user of the device is present.

B) Result

Since an instrument of Chapter V of the Regulation does not guarantee an adequate level of protection for the data in question by the first respondent to the second respondent (in the USA), there is an infringement of Article 44 of the GDPR.

The first respondent was (at any event)http://www.[redacted].at/ responsible for the operation of the website www.[redacted].at at the time of the appeal, namely 14 August 2020. The relevant data protection breach of Art. 44 GDPR is therefore attributable to the first respondent.

It was therefore appropriate to rule on the matter.

D.5. Remedial powers

In the opinion of the Data Protection Authority, the Google Analytics tool (in any case in the version of 14 August 2020) cannot therefore be used in accordance with the requirements of Chapter V GDPR.

However, since the Google Analytics tool was removed from the first respondent's website before the conclusion of the appeal proceedings at issue, no recourse could be made to the remedies.

D.6. Point 3

It is necessary to verify whether the Second Respondent (as a data importer) is also subject to the obligations laid down in Chapter V of the Regulation.

On the basis of the above EDPB Guidelines 5/2021, it should be recalled that a transfer to a third country or an international organisation" within the meaning of Article 44 GDPR exists only if, inter alia, the controller or processor (data exporter) discloses personal data which are the subject of such processing to another controller, a joint controller or a processor (data importer) by transfer or otherwise.

This condition does not apply to the second respondent in the present case, since the latter (as a data importer) does not disclose the complainant's personal data but receives them (only). In other words: The requirements of Chapter V GDPR are to be complied with by thedata exporter, but not by the data

importer.

It is not overlooked by the complainant's reasoning that data transmission necessarily requires a recipient and that the second respondent (from a technical point of view) is part of the data transmission. However, it should be pointed out that data protection responsibility can still be "shared" (from a legal point of view) in the case of a processing operation, i.e. there may be a different degree of responsibility depending on the stage of the processing operation (cf. EDPB Guidelines 7/2020 on the concept of controllers and processors, paragraph 63 et seq.).

The data protection authority therefore considers that there is no infringement of Article 44 GDPR by the secondrespondent.

It was therefore appropriate to rule on the whole.

Finally, it should be pointed out that the second respondent's second respondent's question of the (possible) infringement of Article 5 et seq. in conjunction with Article 28(3)(a) and Article 29 of the GDPR is discussed with a further decision.