Republik Österreich
Datenschutz behörde

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

E-mail: [redacted]

GZ: D155.027
2021-0.586.257

Clerk: [redacted]

[redacted]
zH NOYB - European Center for Digital Rights

Goldschlagstrasse 172/4/3/2
1140 Vienna

Data protection complaint (Art. 77 Para. 1 GDPR)
[redacted] /1. [redacted] Verlags GmbH (formerly: [redacted] at GmbH), 2. Google LLC (101 Dalmatians)

by email delivery / email [redacted]

PARTIAL DECISION

SPEECH

The data protection authority decides on the data protection complaint from (complainant) of [redacted] August 18, 2020, represented by NOYB - European Center for Digital Rights, Goldschlagstraße 172/4/3/2, 1140 Vienna, ZVR: 1354838270, against 1) [redacted] Verlag GmbH (formerly: [redacted] at GmbH) (First Respondent), represented by [redacted] and 2) Google LLC , 1600 amphitheater Parkway, Mountain View, CA 94043, USA (Second Respondent), represented by [redacted] because of a violation of general Principles of data transfer according to Art. 44 GDPR as follows:

1. The decision of the data protection authority of October 2, 2020, Zl. D155.027, 2020-0.527.385, is Fixed .

2. The complaint against the First Respondent will granted and it is found that

a) the first respondent as the person responsible by implementing the tool "Google Analytics" on her website at www. [redacted] at least on August 14th

2020 submitted personal data of the complainant (these are at least unique user identification numbers, IP address and browser parameters) to the second respondent,

b) the standard data protection clauses that the first respondent concluded with the second respondent do not offer an adequate level of protection in accordance with Art. 44 GDPR, since

i) the Second Respondent as providers electronic Communications services within the meaning of 50 US Code § 1881 (b) (4) and, as such, is subject to surveillance by US intelligence agencies pursuant to 50 US Code § 1881a ("FISA 702"), and

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

c) In the present case, no other instrument according to Chapter V of the GDPR can be used for the data transmission listed in point 2.a) and the respondent therefore does not guarantee an adequate level of protection for the data transmission referred to in point 2.a) in accordance with Art. 44 GDPR has.

3. The complaint against the Second Respondent because of a violation of the general principles of data transmission according to Art. 44 GDPR rejected .

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

REASON

A. Arguments of the parties and course of the procedure

A.1. theComplainant brought in his submission dated August 18, 2020 summarized the following:

On August 14, 2020, at 10:45 a.m., he visited the Respondent's website at www. [redacted] at / visited. During the visit he was logged into his Google account, which with the complainant's email address, [redacted], be linked. the First Respondent embedded an HTML code for Google services (including Google Analytics) on its website. In the course of the visit, the first respondent processed personal data, namely at least the complainant's IP address and cookie data. Some of this data was transmitted to the second respondent. Such data transfer requires a legal basis in accordance with Art. 44 ff GDPR.

According to the judgment of the European Court of Justice of July 16, 2020, Case C-11/18 ("Schrems II"), the respondents could no longer rely on an adequacy decision ("Privacy Shield") according to Art. 45 GDPR for a data transfer to the USA support. The Respondent should also not base the data transmission on standard data protection clauses if the third country of destination does not guarantee adequate protection of the personal data transmitted on the basis of standard data protection clauses in accordance with Union law. The Second Respondent was to be qualified as a provider of electronic communications services within the meaning of 50 US Code § 1881 (b) (4) and as such was subject to surveillance by US secret services according to 50 US Code § 1881a ("FISA 702"). The Second Respondent is submitting the US Government under US 50

As a result, the respondents are not in a position to ensure adequate protection of the complainant's personal data when his data are transmitted to the second respondent. The transmission of the complainant's data to the USA is unlawful. Several enclosures were attached to the complaint.

A.2. With an opinion ofDecember 16, 2020 brought the First Respondent summarized the following:

The first respondent is only based in Austria. She is responsible for the decision to use the tool on the website [redacted] at embed. The tool is used to to enable general statistical evaluations of the behavior of the website visitors. However, the tool does not allow the content to be adapted to a specific website user, since the

Evaluation is carried out anonymously and no reference to a specific user is made possible. User IP addresses would also be anonymized before being stored or transmitted ("IP anonymization"). The so-called user agent string is used to inform the server about the system specification with which the user is accessing the server. Without reference to a person, only the device, operating system and version, browser and browser version and the device type would be displayed. In the best case, it can be assigned to a specific device, but never to a specific person using the device. The processing of the anonymous statistics takes place predominantly in data centers in Europe, but also by the second respondent on servers outside the EEA.

If the GDPR is applicable, the first respondent is responsible and the second respondent is a processor. A processor agreement has been concluded. Since no personal data would be transmitted, the judgment of the ECJ of July 16, 2020 in case C311 / 18 is not applicable. However, in order to take precautions for any transfer of personal data to the second respondent

- e.g. in the event that IP anonymization is deactivated due to a data breach - the first respondent concluded a data processing agreement with the second respondent, including standard data protection clauses (SDK). This was implemented purely for reasons of caution. The second respondent took further technical and organizational measures to offer a high level of data protection for the data processed via the tools. Several enclosures were attached to the opinion.

A.3. With an opinion ofJanuary 22, 2021 brought the Complainant summarized the following:

In the case of a processor in a third country, a breach of anonymization cannot be enforced or determined. In case of doubt, 50 USC § 1881a applies and not an advertising text on the Google website. The personal data processed first would only be anonymized afterwards in a second step. Any anonymization that may have taken place after the transfer does not affect the previous processing. The statement contains a more detailed technical description at this point.

Apart from that, the complainant not only relied on the processing of his IP address, but also other personal data, such as cookie data. At the time of the website visit, he was logged into his private Google account. "Google" cookies have been set. In order to prevent a violation of Art. 44 ff GDPR, a complete removal of the tool is necessary and a switch to another tool without data transmission to the USA is recommended. If the Respondent was convinced that no personal data would be processed, the conclusion of order processing conditions would be absurd. Several enclosures were attached to the opinion.

A.4. With an opinion ofApril 9, 2021 transmitted the Second Respondent his answers to the questionnaire of the data protection authority.

A.5. With an opinion ofMay 4, 2021 brought the First Respondent in relation to the respondent's statement of April 9, 2021, summarized the following:

The First Respondent only uses the free version of Google Analytics. Both the terms of use and the SDK had been approved. The Google Analytics 4 version was not implemented, and the data release setting was not activated. The code was embedded with the anonymization function. The second respondent is only used as a processor. The Respondent issued the instructions via the settings of the Google Analytics user interface and via the global website tag. Google Signals is not used. The first respondent did not have its own authentication system and did not use a user ID function. Currently, one does not rely on the exception regulation of Art. 49 Para. 1 GDPR.

A.6. With an opinion ofMay 5, 2021 brought the Complainant in relation to the respondent's statement of April 9, 2021, summarized the following:

The complaint is directed against the first and second respondents. Google Ireland Limited is not a party to the proceedings. The data protection authority was directly responsible for the second respondent, who had violated Art. 44 ff GDPR. The second respondent, as a processor, is the norm addressee of Chapter V GDPR. The second respondent stated that all data collected by Google Analytics would be hosted in the USA.

At least some of the cookies set when you visited the website on August 14, 2020 would contain unique user identification numbers. In the transaction between the complainant's browser and https: // tracking. [redacted]at, which was started on the stated date, the user identification numbers "_gads", _ "ga" and "_gid" were set. These numbers were subsequently transmitted to https://www.google-analytics.com/. The numbers are "online identifiers" which serve to identify natural persons and which are specifically assigned to a user. With regard to the IP address, it should be noted that Chapter V GDPR does not provide for any exceptions for "subsequently anonymized data". It should be assumed that the complainant's IP address was not even anonymized in all transactions. The application for the imposition of a fine is withdrawn, this is now a suggestion.

A.7. With an opinion ofJune 10, 2021 brought the Second Respondent summarized the following:

The active legitimation of the complainant was not established because it had not been proven that the transmitted data were personal data of the complainant. The cookies in question are first-party cookies under the domain [redacted] at had been set. They are therefore cookies from the first respondent and not from the second respondent. Accordingly, these are not unique Google Analytics cookie IDs per user that are used on multiple websites that use Google Analytics. A user has different cid numbers for different websites. It was not found that the numbers in question would make the complainant identifiable. At this point, the submission contains further technical information on the cookies used. With regard to the IP address, it should be checked whether the IP address of the device connected to the Internet can actually be assigned to the complainant and whether the person responsible or "another person" has the legal means to receive connection owner information from the provider in question .

As a processor, the second respondent provided the website operator with numerous configuration options for Google Analytics. On the basis of the information received, it should be noted that the Respondent configured Google Analytics as stated. Due to a possible configuration error, the respondent did not activate the IP anonymization function in all cases. Under normal operating conditions and to the extent that users based in the EU are affected, a web server is located in the EEA, which is why IP anonymization is generally carried out within the EEA. In the present case, normal operating conditions were present.

On August 14, 2020, the account [redacted] the web & app activities Setting activated. However, the account did not choose to include activities from websites that used Google services. Since the first respondent stated that he had not activated Google signals either, the second respondent was therefore not in a position to determine that the user of the account was [redacted] visited this website.

With regard to international data traffic, it should be noted that - even under the assumption that the complainant's personal data were involved - their nature was limited in terms of quantity and quality. Insofar as the transmitted data can be classified as personal data at all, it would also be pseudonymous data. Standard contractual clauses had been concluded with the Respondent, and additional measures had been implemented. The second respondent did not disclose any user data in accordance with EO 12333. FISA § 702 is irrelevant in the present case in view of the encryption and anonymization of IP addresses. Art. 44 ff GDPR could not be the subject of a complaint procedure under Art. 77 Para. 1 GDPR, why the complaint should be rejected in this regard. Art. 44 ff GDPR are also not applicable with regard to the second respondent as a data importer.

A.8. With comments fromJune 18 and 24, 2021 brought the First Respondent summarized the following:

As part of an asset deal, the website is effective February 1, 2021www. [redacted]at on the [redacted] GmbH in Munich. Subsequently, the first respondent from at GmbH was in [redacted] [redacted] Verlags GmbH has been renamed. In addition, got the first respondent instructed the second respondent to immediately delete all data collected via the Google Analytics properties. The configuration error in connection with the IP anonymization function has been fixed. In the meantime, the second respondent had confirmed the final deletion of all data and an attachment would be submitted as evidence. It is suggested to discontinue the procedure in accordance with Section 24 (6) DSG.

A.9. With comments fromJuly 9, 2021 brought the Second Respondent summarized the following:

In the opinion of the European Data Protection Committee (EDPB), an adequacy assessment is not limited to the examination of the legal provisions of the third country, but must also take into account all specific circumstances of the transfer in question. This is relevant to the present case. The pseudonymization is here - in line with the EDSA guidelines
- an effective complementary measure. It is not to be expected that US authorities would have additional information that would enable them to identify the data subjects behind the first party cookie values "gid" and "cid" or behind an IP address. The complainant had also not requested a declaration that his rights had been violated in the past.

A.10. With comments fromJuly 9, 2021 brought the Complainant summarized the following:

There is a processing of personal data, this is evidenced among other things by the submitted attachments. If, in the end, the only prerequisite for the identification of a website visitor is whether he or she submits certain declarations of intent in his or her account (such as the activation of "Ad personalization"), then all possibilities of identifiability would be available to the second respondent. Otherwise, the Second Respondent would not be able to comply with the user's wishes for "personalization" of the advertising information received, as expressed in the account settings.

The UUID (Universally Unique Identifier) in the _gid cookie with the UNIX time stamp 1597223478 was set on Wednesday, August 12, 2020 at 11:11 and 18 seconds CET, that in the cid cookie with the UNIX time stamp 1597394734 was set on Friday, August 14th August 2020 at 10:45 and 34 seconds CET. It follows that these cookies are used before the visit to which the complaint is made

and longer-term tracking has taken place. To the best of his knowledge, the complainant did not immediately delete these cookies and the website [redacted] at too visited repeatedly.

The second respondent misunderstood the broad understanding of the GDPR when assessing the existence of personal data. The specific IP address used can no longer be determined by the complainant either. However, this is irrelevant, since the UUID in the cookies is already clearly linked to a person. In particular, the combination of cookie data and IP address allows tracking and the evaluation of geographical localization, Internet connection and context of the visitor, which can be linked to the cookie data already described. This would also include data such as the browser used, the screen resolution or the operating system (“device fingerprinting”).

In the context of the complaint, it is more relevant that US authorities use data that can be easily identified by secret services, such as the IP address, as a starting point for monitoring individuals. It is the standard procedure of secret services to "move on" from one date to another. When the complainant's computer keeps coming back to the IP address of [redacted] surfaced on the Internet, this could be used to improve the work of the [redacted] spying on and targeting the complainant. In another
In the second step, other identifiers would then be searched for in the data, such as the UUIDs mentioned, which in turn enables the individual to be identified for monitoring in other locations. In this context, US secret services are “another person” within the meaning of recital 26 GDPR. The complainant is working [redacted], but also had a relevant role as a model complainant in these efforts.
According to US law, monitoring of the complainant according to 50 USC § 1881a (as well as of all other persons entrusted with this complaint) is legally possible at any time. Even with the application of the supposed “risk-based approach”, the present case is a prime example of a high risk.

The E-Mail adress [redacted] was to be assigned to the complainant who had the surname of a marriage [redacted] borne up to. The old Google account will, however still used. It is not explained to what extent the undisputed data is linked, evaluated or the result of an evaluation is simply not displayed to the user.

In addition, Chapter V GDPR does not know a "risk-based approach". This can only be found in certain articles of the GDPR, such as Art. 32 leg.cit. The new standard contractual clauses in the Implementing Decision (EU) 2021/914 are not relevant to the facts due to their lack of temporal validity. A “transmission” is not a unilateral act by a data exporter; every “transmission” also requires the data to be received. Accordingly, Chapter V of the GDPR is also for the

Second respondent applicable, it is a matter of joint action by the data exporter and importer.

Even if the second respondent did not violate Art. 44 ff GDPR, the provisions of Art. 28 Para. 3 lit. a and Art. 29 GDPR should be taken into account as a "fallback rule". If the second respondent followed a corresponding instruction from a US secret service, he would make the decision to process personal data beyond the specific order of the first respondent in accordance with Art. 28 and Art. 29 GDPR and the corresponding contractual documents. This makes the second respondent himself the person responsible in accordance with Art. 28 (10) GDPR. As a result, the second respondent has to comply in particular with the provisions of Art. 5 ff GDPR. A secret transfer of data to US secret services in accordance with US law is undoubtedly not compatible with Art. 5 Para. 1 lit. f GDPR, Art. 5 Para. 1 lit.

A.9. With the last opinion ofAugust 12, 2021 brought the Second Respondent summarized the following:

The complainant had not shown his active legitimation to lodge a complaint. He had not answered any questions raised by the second respondent about the identifiability of his person on the basis of the IP address. With regard to the _gid number and cid number, it should be noted that there was no directory in order to make the complainant identifiable. The fact that recital 26 GDPR mentions “segregation” as a possible means of identification does not change the understanding of the words “identify” or “identification” or “identifiability”.

The ability of the complainant to be identified presupposes at least that his identification is possible on the basis of the data in question and by means that, according to the general judgment, would probably be used. This has not been established and cannot be assumed and, on the contrary, is even improbable, if not even impossible. The fact that the second respondent had entered into processor agreements does not mean that the data that are the subject of these proceedings are personal data, nor that they are the data of the complainant.

The complainant's view that the data transfer should not be assessed according to a risk-based approach (“all or nothing”) should not be upheld. This is not in line with the GDPR and can be seen in Recital 20 of the Implementing Decision (EU) 2021/914 of the European Commission. This can also be seen in the different versions of the EDSA recommendation 01/2020. Even if US authorities can "legally" access the above numbers at any time, it should be checked how likely this is. The complainant had not put forward any convincing arguments as to why or how

"Cookie data" in connection with his visit to a publicly accessible Austrian website that is used by many, such as the "Foreign Intelligence Information" in question, and could thus become the goal of the purpose-limited data collection according to § 702.

B. Subject matter of the complaint

Based on the submission of the complainant, it can be seen that the subject of the complaint is in any case the question,

- whether the First Respondent has implemented the Google Analytics tool on its website www. [redacted] at personal data of the complainant has forwarded the second respondent and,
- whether for this data transmission a adequate level of protection was guaranteed in accordance with Art. 44 GDPR.

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

The request to impose an immediate ban on the transmission of data to the second respondent against the first respondent (as the person responsible) is not to be discussed since - as will be explained below - responsibility for the operation of the website www. [redacted] at in the course of the complaint procedure (but only after the Complaint-relevant data transmission) to the [redacted] GmbH with Based in Munich passed over is. With regard to the imposition of such a ban, the data protection authority would have to bring the case to the competent German supervisory authority.

Likewise, the application for the imposition of a fine is not to be discussed, since this was withdrawn by the complainant with a statement of May 5, 2021 and this is now to be understood as a suggestion.

Finally, it should be noted that with the present partial notification not the alleged violations of the second respondent in accordance with Art. 5 ff in conjunction with Art. 28 Para. 3 lit. a and Art. 29 GDPR are discussed. In this regard, further investigative steps are necessary and will be discussed in a further notification.

C. Factual Findings

C.1. In any case, on August 14, 2020, the first Respondent was the website operator of www. [redacted] at. In the Austrian version of " [redacted] if it is an at is only in Information portal on the subject of health. The website www. [redacted] German Language offered. The First Respondent did not operate any other versions of the website

www [redacted] at in the EU. The first respondent is also only based in Austria and has no further branches in other EU countries. For Germany there is a German version of " [redacted] at www. [redacted] de, but not on the part of the First Respondent was operated.

Assessment of evidence re C.1. : The findings made are based on the respondent's statement of December 16, 2020 (questions 1 to 3) and were therefore not disputed by the complainant.

C.2. On February 1, 2021, the website www. [redacted] at as part of an asset deal on the [redacted] GmbH based in Munich. Subsequently, the first respondent became from [redacted] at GmbH [redacted] [redacted] publishing company GmbH renamed. the First Respondent has the website www. [redacted] at until August 2021 for the [redacted] GmbH supervised. The First Respondent has ceased to be the operator of www since August 2021. [redacted] at and no longer makes the decision about whether to use the Google Analytics tool.

Assessment of evidence re C.2. : The findings are based on the respondent's statement of June 18, 2021 and were therefore not disputed by the complainant. In addition, the findings are based on an official search by the data protection authority in the commercial register for Zl. FN 186415 s.

C.3. The second respondent developed the Google Analytics tool. Google Analytics is a measurement service that enables customers of the second respondent to measure traffic properties. This also includes measuring the traffic of visitors who visit a specific website. This makes it possible to understand the behavior of website visitors and measure how they interact with a specific website. Specifically, a website operator can create a Google Analytics account and view reports on the website using a dashboard. Google Analytics can also be used to measure and optimize the effectiveness of advertising campaigns that website owners carry out on Google advertising services.

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

Evaluation of evidence re C.3. : The findings are based on the opinion of the second respondent dated April 9, 2021 (p. 3 as well as questions 1 and 2) and were therefore not disputed by the complainant.

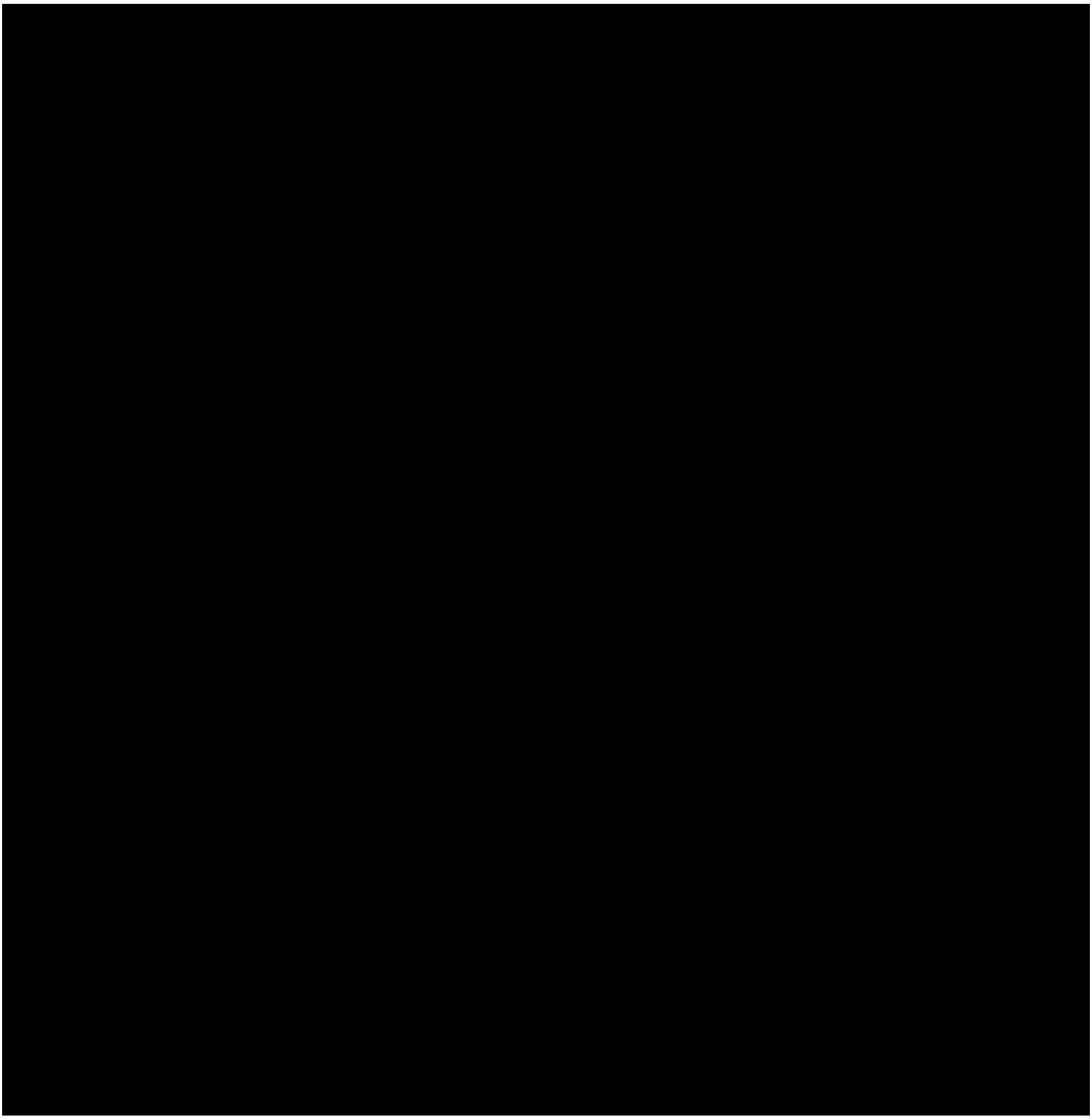
C.4. The first Respondent - as the website operator - has at least the deadline of August 14th

In 2020 made the decision to use the free version of the Google Analytics tool for the website www. [redacted] at to use. For this purpose, it has a JavaScript code ("tag") that the Second respondent is made available, built into the source code of their website. The First Respondent used the tool to enable general statistical evaluations of the behavior of website visitors. The additional tool Google Signals has not been activated.

In any case, these evaluations are used by the Respondent to improve the content of the website www. [redacted] at to be presented in accordance with the general interest in the topic, that the channels that meet the most demand are placed in the foreground and the presentation can be adapted depending on the topicality of a specific topic.

The first respondent has set up a Google Analytics account for this purpose. The Google Analytics account ID with the account name " [redacted] reads [redacted] The above evaluations can the First Respondent by logging into the "and in the dashboard [redacted] Google Analytics account reports on traffic from www. [redacted] at can see. Reports are divided into the categories real-time, target group, acquisition, behavior and conversions. The first respondent can select user-defined specifications for the report generation, the second respondent has no influence on this. The second respondent also has no influence on the extent to which the first respondent subsequently uses the reports that have been created.

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



Evaluation of evidence re C.4. : The findings are based on the submission of the First Respondent on December 16, 2020 and were not disputed by the Appellant. The mentioned screenshots were taken from Enclosures ./1 and ./10, the presentation of the reporting is detailed in Enclosure ./1.

C.5. The Google Analytics tool works as follows: When visitors visit the website

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

The data that is 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 making the request, such as host name, browser type, referrer and language. In addition, the browser's DOM interface (the interface between HTML and dynamic JavaScript) provides access to more detailed browser and system information, such as Java and Flash support and screen resolution. Google Analytics uses this information. Google Analytics also sets and reads first-party cookies on a user's browsers, which enable the measurement of the user session and other information from the page request.

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

On the information page of the second respondent on the Google Analytics tool, the following information can be found in extracts (formatting not reproduced 1: 1, requested on December 22, 2021):

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

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

- Distinguish unique users
- Throttle the request rate

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

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

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

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

Assessment of evidence re C.5. : The findings are based on the opinion of the second respondent dated April 9, 2021 (question 2) and an official search by the data protection authority at https:// developers.google.com/analytics/devguides/collection/gajs/cookieusage and https: // developers.google.com/analytics/devguides/collection/gtagjs/cookies-user-id (both accessed on December 22, 2021).

C.6. First and second respondents have entered into a contract entitled “Processor Conditions for Google Advertising Products”. The version of August 12, 2020 of this contract was valid at least on August 14, 2020. The contract regulates order processing conditions for "Google advertising products". It applies to the provision of order processing services and related technical support services for customers of the second respondent. The above-mentioned contract in the version dated August 12, 2020 (Appendix ./7) is used as the basis for the determinations of the facts.

In addition, first and second respondents have a second contract on August 12, 2020

with the title "Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors". These are standard contractual clauses for international data traffic. The above-mentioned second contract in the version dated August 12, 2020 (Appendix ./11) is also used as a basis for the findings of the facts.

With regard to the data categories listed in Appendix 1 of the second contract, reference is made to the link https://privacy.google.com/businesses/adsservices/. The following is shown in extracts under the link mentioned (highlighted in red by the data protection authority, formatting not reproduced 1: 1, requested on December 22, 2021):

Auftragsdatenverarbeitungsbedingungen:

Auftragsverarbeiterdienste

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

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

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

Arten personenbezogener Daten

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

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

In addition to the conclusion of standard contractual clauses, the second respondent implemented further contractual, organizational and technical measures. These measures complement the obligations contained in the standard contractual clauses. The measures are described in the second respondent's statement of April 9, 2021, question 28. This description is used as the basis for the determinations of the facts.

the Second Respondent released regularly so-called Transparency reports ("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 re C.6. : The findings made are based on the respondent's statement of December 16, 2020, question 15. The cited enclosures ./7 and ./11 are included in the file and are known to all parties involved. In addition, the findings are based on official research by the data protection authority at https://privacy.google.com/businesses/adsservices/ (requested on December 22, 2021). The findings made with regard to the "additionally implemented measures" result from the second respondent's statement of April 9, 2021 (question 28). The statement of the second respondent dated April 9, 2021 is contained in the file and is known to all parties involved. The finding with regard to the transparency reports results from an official research by the data protection authority at https:

C.7. When using the Google Analytics tool, the option of using an "IP anonymization function" is offered. In any case, this function was not correctly activated on August 14, 2020 on www. [redacted] at implemented.

Assessment of evidence re C.7. : The findings are based on the respondent's statement of June 18, 2021. In it, the respondent admits that the "IP anonymization function" mentioned was not properly implemented due to a code error.

C.8. The complainant visited the website www. [redacted] at. During the visit, he was logged into his Google account, which was linked to the E-mail address [redacted] is linked. The email address belongs to the Complainant. The complainant had the last name in the past [redacted]

A Google account is a user account that is used to authenticate the second respondent with various Google online services. A Google account is a prerequisite for using services such as “Gmail” or “Google Drive” (a file hosting service).

Assessment of evidence re C.8. : The findings are based on the complainant's submission of August 18, 2020 (p. 3) and were not disputed by the respondents. The determinations made with regard to the basic functions of a Google account are based on an official research by the data protection authority at https://support.google.com/accounts/answer/27441?hl=de and https:// policies.google.com / privacy (both accessed on December 22, 2021).

C.9. In the transaction between the complainant's browser and https: // tracking. [redacted] at / were unique users on August 14, 2020 at 12:46: 19.344 CET Identification numbers are set at least in the cookies "_ga" and _ "gid". As a result, these identification numbers were transmitted to https://www.google-analytics.com/ and thus to the second respondent on August 14, 2020 at 12:46: 19.948 CET.

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

Domain	Name	Wert	Zweck
https://tracking.[redacted].at/	_ga	GA1.2.1284433117.1597223478	Google Analytics
https://tracking[redacted]at/	_gid	GA1.2.929316258.1597394734	Google Analytics
https://tracking.[redacted]at/	_gads	ID=d77676ed5b074d05:T=1597223569:S=ALNI_MZcJ9EjC13lsaY1Sn8Qu5ovyKMhPw	Google Werbung
https://www.google-analytics.com/	_gid	929316258.1597394734	Google Analytics
https://www.google-analytics.com/	cid	1284433117.1597223478	Google Analytics

These identification numbers each contain a UNIX time stamp at the end, which shows when the respective cookie was set. The identification number in the _gid cookie with the UNIX time stamp "1597394734" was set on Wednesday, August 14, 2020 at 11:11 and 18 seconds CET, the one in the cid cookie with the UNIX time stamp "1597223478" was set on Friday, August 12 August 2020 at 10:45 and 34 seconds CET.

With the help of these identification numbers, it is possible for the respondents to differentiate between website visitors and also to receive information as to whether they are new or returning website visitors from www. [redacted]at acts.

In addition, the following information (parameters) was also transmitted to the second respondent via the complainant's browser in the course of requests to https://www.google-analytics.com/collect (excerpt from the HAR file, request URL https://www.google-analytics.com/collect, extract of the request with time stamp 2020-08- 14T10: 46: 19.924 + 02: 00):

general

- Request URL https://www.google-analytics.com/collect
- Request method GET
- HTTP VersionHTTP / 2
- Remote Address 172.217.23.14

Headers

- Accept: image / webp, * / *
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US, de; q = 0.7, en; q = 0.3
- Connection: keep-alive
- Host: www.google-analytics.com

- Referer: https: // www. [redacted] at/
- TE: Trailers
- User-Agent: Mozilla / 5.0 (Windows NT 10.0; Win64; x64; rv: 79.0) Gecko / 20100101 Firefox / 79.0

Query Arguments

- _gid: 929316258.1597394734
- _s: 1
- _u: QACAAEAB ~
- _v: j83
- a: 443943525
- cid: 1284433117.1597223478
- de: UTF-8
- dl: https: // www. [redacted] at/
- German: [redacted] at homepage - your independent health portal
- ea: /
- ec: scroll depth
- el: 25
- gjid:
- gtm: 2wg871PHBM94Q
- each: 0
- yid:
- ni: 0
- sd: 24-bit
- sr: 1280x1024
- t: event
- tid: UA-259349-1
- ul: en-us
- v: 1
- vp: 1263x882
- z: 1764878454

Size

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

From these parameters, conclusions can be drawn about the browser used, the browser settings, language selection, the website visited, the color depth, the screen resolution and the AdSense linking number.

The remote address 172.217.23.14 is that of the second respondent.

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

The findings of the facts are based on the content of the HAR file (enclosure ./4), which was submitted by the complainant with the submission of August 18, 2020.

Assessment of evidence re C.9. : The findings are based on the complainant's submission of August 18, 2020 and the HAR file presented therein, enclosure ./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 arguments are consistent with the archival data contained therein. The HAR file submitted (or its content) is known to those involved. In addition, the findings are based on the complainant's statement of May 5, 2021 (p. 8 ff) and the screenshots contained therein. As stated above, according to the second respondent, the purpose of the identification numbers is to distinguish users. The times determined when the cookies were set are calculated from the respective UNIX time stamps. The Unix time is a time definition that was developed for the Unix operating system and established as the POSIX standard. Unix time counts the last few seconds since Thursday, January 1st, 1970, 00:00 UTC. The determination with regard to the remote address results from an official Who-Is query of the data protection authority at https://who.is/whois-ip/ip-address/172.217.23.14 (queried on December 22, 2021).

C.10. Insofar as the Google Analytics tool is implemented on a website, the second respondent has the technical option of receiving information that a specific Google account user has visited this website (on which Google Analytics is implemented), provided that this Google account user User is logged into the Google account during the visit.

Evaluation of evidence re C.10. : In his statement of April 9, 2021, the second respondent submitted to question 9 that he would only receive such information if certain conditions were met, such as the activation of specific settings in the Google account. In the opinion of the data protection authority, this argument is not convincing. If the request of a Google account user for "personalization" of the advertising information received can be met on the basis of a declaration of intent in the account, there is, from a purely technical point of view, the possibility of receiving the information via the visited website of the Google account user. In this context, express reference is made to the data protection law

Accountability to be indicated, which will be further elaborated in the context of the legal assessment. For the establishment of the facts, this accountability under data protection law means that the respondent (or at least the first respondent as the person responsible) - and not the complainant or the data protection authority - must provide sufficient evidence. Such sufficient evidence - that is, that from a technical point of view, there is no possibility of data receipt for the second respondent - was not provided in this context, especially since it is an essential part of the concept of Google Analytics to be implemented on as many websites as possible in order to contain data to be able to collect.

C.11. In the course of the proceedings, the first respondent instructed the second respondent to use all data collected via Google Analytics Properties for the website www. [redacted] at to delete. The second respondent has confirmed the deletion.

Assessment of evidence re C.11. : The determinations made are based on the respondent's statement of June 18 and 24, 2021 as well as the submitted copy of the correspondence between the first and second respondents.

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

D.1. General

a) To the competence of the data protection authority

The European Data Protection Committee (hereinafter: EDSA) has already dealt with the relationship between the GDPR and Directive 2002/58 / EC ("e-Data Protection Directive") (see Opinion 5/2019 on the interaction between the e-Data protection RL and the GDPR of March 12, 2019).

Also the Data protection authority has himself With notice from the November 30, 2018, Zl. DSB-D122.931 / 0003-DSB / 2018, dealt with the relationship between the GDPR and the national implementation provisions (in Austria now: TKG 2021, Federal Law Gazette I No. 190/2021 as amended).

It was fundamentally stated that the e-Data Protection Directive (or the respective national implementation provision) of the GDPR as *lex specialis* going on. Art. 95 GDPR stipulates that the regulation does not impose any additional obligations on natural or legal persons with regard to processing in connection with the provision of publicly accessible electronic communication services in public communication networks in the Union,insofar as they are subject to special obligations set out in the e-Data Protection Directive that pursue the same goal .

In the e-Data Protection Directive, however, there are no obligations within the meaning of Chapter V of the GDPR for the case of the transmission of personal data to third countries or to international organizations.

It should be noted at this point that the responsibility for the operation of the website www. [redacted] at first after of the data transfer relevant to the complaint on August 14, 2020 to a German society has passed over.

Against this background, the GDPR must be applied to such data transmission and thus there is a Jurisdiction the data protection authority to handle the complaint in question according to Art. 77 Para. 1 GDPR.

b) On Art. 44 GDPR as a subjective right

Based on the previous rulings of the data protection authority and the courts, it should be noted that both the legality of the data processing according to Art. 5 Para. 1 lit. a in conjunction with Art. 6 ff GDPR and the data protection rights postulated in Chapter III of the regulation as a subjective right in A complaint according to Art. 77 Para. 1 GDPR can be asserted.

The transfer of personal data to a third country, which in the sense of Art. 44 GDPR (allegedly) no adequate level of protection guaranteed , has not yet been the subject of a complaint in the context of a complaint procedure before the data protection authority.

In this context, it should be noted that Art. 77 Paragraph 1 GDPR (and otherwise also the national provision of Section 24 Paragraph 1 DSG) only requires the right to lodge a complaint, *that "[...] the processing the personal data concerning them against this regulation violates*".

In its judgment of July 16, 2020, the ECJ also assumed that the finding that *"[...] the law and practice of a country do not guarantee an adequate level of protection [...]"* such as *"[...] the compatibility of this (adequacy) decision with the protection of privacy and the freedoms and fundamental rights of persons [...] "* can be asserted as a subjective right in the context of a complaint according to Art. 77 (1) GDPR (cf. the judgment of the ECJ of July 16, 2020, C 311/18 margin no. 158).

It should be noted that the question referred in the procedure mentioned did not deal with the "scope of the right to lodge a complaint under Art. 77 (1) GDPR"; However, the ECJ has the fact that a violation of the provisions of Chapter V GDPR can also be asserted in the context of a complaint under Art. 77 (1) GDPR, asnecessary requirement deems. If you looked at it differently, the ECJ would have said that the question

the validity of an adequacy decision cannot be clarified in the context of a complaint procedure.

Insofar as the second respondent also asserts Article 44 GDPR as a subjective right - with reference to the wording of recital 141 leg.cit. - denies this, it must be countered that the recital mentioned is linked to the fact that the "right according to this regulation "are accessible to a complaint according to Art. 77 (1) GDPR (and not for example:" the rights according to Chapter III of this Ordinance ").

Although the term "rights of a data subject" is used in certain places in the GDPR, this does not mean, conversely, that other standards in which this formulation is not chosen cannot be asserted as a subjective right. Most of the provisions of the GDPR are on the one hand an obligation of the controller (and partly of the processor), but canon the other hand can also be asserted as a subjective right of data subjects. For example, it is undisputed that Art. 13 and Art. 14 GDPR justify a subjective right to information, although the right to information is not specified in Art. 12 Para. 2 leg. Cit. is listed as “your rights” (ie “rights of the person concerned”) and Art. 13 and Art. 14 GDPR as informationduty of the person responsible.

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

Apart from this, the recitals are an important instrument for interpreting the GDPR, but they cannot be used to arrive at a result that contradicts the text of the regulation (here, as explained above, the fact that the administrative legal remedy general linked to “processing”) (cf. the judgment of the ECJ of May 12, 2005, C-444/03 margin no. 25 and the further case law cited there).

Finally, according to the domestic judicature of the VwGH in doubt It can be assumed that standards that prescribe an official procedure, also and especially in the interest of the person concerned, grant them a subjective right that can be enforced through the appeal process (cf. for example VwSlg. 9151 A / 1976, 10.129 A / 1980, 13.411 A / 1991, 13.985 A / 1994).

Against the background of the wording of Art. 77 (1) GDPR and the cited case law of the ECJ and the VwGH, it should be noted as an interim result that the norms in Chapter V and in particular that in Art. 44 GDPR Obligation for controllers and processors to ensure the level of protection for natural persons guaranteed by the regulation, and vice versa as subjective right can be asserted before the competent supervisory authority in accordance with Art. 77 Para. 1 GDPR.

c) On the determination competence of the data protection authority

According to the judicature of the VwGH and the BVwG, the data protection authority comes a Assessment competence with regard to violations of the right to secrecy in Complaints procedure (as expressly the decision of the BVwG of May 20, 2021, Zl. W214 222 6349-1 / 12E; implicitly the decision of the VwGH of February 23, 2021, Ra 2019/04/0054, in which this is concerned with the determination of an in lying in the past Breach of confidentiality has dealt with without taking up the lack of competence of the authority concerned).

There are no objective reasons not to use the determination competence according to Art. 58 Paragraph 6 GDPR in conjunction with Section 24 Paragraph 2 Z 5 GDPR and Paragraph 5 GDPR for the determination of a violation of Art. 44 GDPR, as in the present case, among others a past violation - namely a data transfer to the USA - is complained about and the right to lodge a complaint in accordance with Section 24 (1) GDPR - as well as Art. 77 (1) GDPR - is generally linked to a violation of the GDPR. When the verdict of a notice in one Complaints procedure namely, could only contain instructions according to Art. 58 Para. 2 GDPR, there would be no room for § 24 Para. 2 Z 5 and 24 Para. 5 DSG.

Contrary to the opinion of the respondents, Section 24 (6) DSG cannot be considered for the subject of the complaint that is relevant here, as data is transmitted in the past is criticized. In other words: The alleged unlawfulness (here: incompatibility with Art. 44 GDPR) of a data transfer that has already been completed is not accessible to the conclusion of a procedure in accordance with Section 24 (6) GDPR.

Against the background of these statements, it should be noted as a further interim result that the data protection authority's determination competence is given in the present complaint procedure.

D.2. Ruling point 1

As stated, the data protection authority continued the procedure in question with a decision of October 2, 2020, Zl. D155.027, 2020-0.527.385, until it was determined which authority is responsible for the procedural management (lead supervisory authority) or until the decision a lead supervisory authority or the EDPB.

Based on the results of the investigation, it should be noted that cross-border data processing within the meaning of Art. 4 Z 23 in conjunction with Art. 56 Para. 1 GDPR with regard to the subject of the complaint - data transfer to the USA in August 2020 - not available and the "one-stop-shop" mechanism according to Art. 60 GDPR therefore does not apply:

According to its own statements (see statement of December 16, 2020, question 2), the respondent is neither established in more than one Member State (Data processing within the meaning of Art. 4 Z 23 lit. a GDPR in the context of the activities of branches in more than one member state can therefore not exist), nor does the data transfer and thus the processing of personal data of the first respondent significant impact on data subjects in more than one Member State (Art. 4 Z 23 lit. b leg. Cit.).

With regard to the effects of the present data processing, the factual findings show that the target audience of the relevant website www. [redacted] at namely, people (primarily) resident in Austria, also because the website www. [redacted] de gives its own version for the German audience. According to the First respondent (see the statement of December 16, 2020, question 2) was this (at least in August 2020) only for the Austrian version of www. [redacted] at responsible.

The theoretical possibility that German-speaking people from a Member State other than Austria can access www. [redacted] at can access the fact "Effects on data subjects in more than one member state ”according to Art. 4 Z 23 lit. b GDPR not to be justified. In the event of a different view, every complaint against the operator of a website - regardless of the intended target audience of the website - would have to be dealt with in accordance with the rules of Art. 60 ff GDPR. This would become ato widen Interpretation of Art. 4 No. 23 lit. b GDPR (and consequently to an overly broad scope of the “one-stop shop”), which - in the opinion of the data protection authority - cannot be intended by the legislator.

The complaint related to the here relevant subject of the complaint to be treated exclusively by the Austrian data protection authority in accordance with Art. 55 Paragraph 1 GDPR.

Since official notices from which no one has a right can be revoked or changed, both by the authority that issued the notification and by the relevant higher authority when exercising the supervisory right, and as a result of a suspension of proceedings by a party In the course of the procedure, there is no right of non-decision, the above-mentioned notification of October 2, 2020 was available for rectification in accordance with Section 68 (2) AVG.

D.2. Ruling point 2. a)

a) General information on the term "personal data"

The material scope of Article 2 (1) GDPR - and thus the success of this complaint - fundamentally requires that "personal data" be processed.

According to the legal definition of Art. 4 No. 1 GDPR, "*personal data any information that relates to an identified or identifiable natural person (hereinafter referred to as "data subject"); asidentifiable is a natural person who is directly or indirect , especially by means of Assignment to an identifier such as a name, to an identification number, to location data, to a Online identifier or can be identified with one or more special features that express the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person can be ".*

As can be seen from the factual findings (see point C.9.), The Respondent has
- as the operator of the website - implemented the tool Google Analytics on your website. As a result of this implementation - i.e. triggered by the JavaScript code executed when visiting the website - at least the following information was received from the complainant's browser, which accessed the website www. [redacted] at, transmitted to the second respondent's server:

- Unique online identifiers ("unique identifier"), which both the browser or the device of the complainant and the first respondent (through the Google Analytics Account Identify the ID of the first respondent as the website operator);
- the address and the HTML title of the website and the sub-pages that the complainant visited;

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

It must be checked whether this information falls under the definition of Art. 4 No. 1 GDPR, i.e. whether it is personal data of the complainant.

b) Identification numbers as "personal data"

With regard to the online identifiers, it should be recalled that the cookies "_ga" or "cid" (Client ID) and "_gid" (User ID) contain unique Google Analytics identification numbers and are stored on the device or in the The complainant's browser was dropped. As noted, it is possible for certain bodies - here the respondents, for example - to use these identification numbers to distinguish website visitors and also to receive information as to whether they are new or returning website visitors to www. [redacted] at acts. With
In other words: Only the use of such identification numbers enables website visitors to be differentiated before this assignment was not possible.

In the opinion of the data protection authority, there is already an interference with the basic right to data protection in accordance with Art. 8 EU-GRC and Section 1 DSG when certain bodies take measures - here the assignment of such identification numbers - to allow website visitors to do so individualize .

A measure of the "identifiability" to the effect that it must be possible to immediately add such identification numbers with a certain "Face" of a natural person - in particular with the name of the complainant - is to be brought into connection not (cf. also Opinion 4/2007, WP 136, 01248/07 / DE of the former Art. 29 data protection group on the term “personal data” p. 16 f; cf. the guidance of the supervisory authorities for providers of telemedia from March 2019, p. 15).

Recital 26 GDPR speaks in favor of such an interpretation, according to which, when asked whether a natural person can be identified, *"[...] all means are taken into account that are likely to be used by the controller or another person according to general discretion to directly or indirectly identify the natural person, such as the Weed out "*(English language version of the regulation: "singling out"). The term “sorting out” means “searching out of a crowd” (cf. https://www.duden.de/rechtschreibung/aussondern, queried on December 22, 2021), which corresponds to the above considerations on the individualization of the website - corresponds to visitors.

In the literature it is also expressly stated that a "digital footprint", which allows devices - and subsequently the specific user - to be clearly individualized, represents a personal date (cf. *Meager* in *Simitis / Hornung / Spiecker*, GDPR comment Art. 4 no. 1 margin no. 52 mwN). This consideration can be transferred to the present case due to the uniqueness of the identification numbers, especially since - which will be discussed in more detail below - these identification numbers can also be combined with other elements.

Insofar as the respondents point out that no “means” would be used to link the identification numbers in question with the person of the complainant, they must again be countered that the implementation of Google Analytics on www

[redacted]. at a segregation within the meaning of Recital 26 GDPRhas the consequence . In other words: who used a tool that did such a weeding just made possible in the first place cannot take the position of not using any means according to “general discretion” to make natural persons identifiable.

As an interim result, it should be noted that the Google Analytics identification numbers in question here can be personal data (in the form of an online identifier) in accordance with Art. 4 No. 1 GDPR.

c) Combination with other elements

The fulfillment of the requirements of Art. 4 Z 1 GDPR becomes even more clearly recognizable if one takes into account that the identification numbers can be combined with other elements:

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

The respondents' submissions relating to the "anonymization function of the IP address" can remain open since the respondents have admitted that this function was not implemented correctly (at the time at which the complaint was made) (cf., for example, the respondent's statement of June 18, 2021).

Likewise, the question of whether an IP address isolated is considered a personal date, remain open, as this - as mentioned - with further elements (in particular the Google Analytics identification number) combined can be. In this context, it should be noted that according to the case law of the European Court of Justice, the IP address can represent a personal date (see the judgments of the European Court of Justice of June 17, 2021, C 597/19, margin no. 102, as well as of October 19, 2016, C 582 / 14, margin no.49) and this does not lose its character as personal data simply because the means of identifying it are with a third party.

Finally, the data protection authority points out that it is an essential part of the Concept of Google Analytics (at least in the free version) is to be implemented on as many websites as possible in order to collect information about website visitors. Accordingly, it would be with the basic right to data protection according to Art. 8 EU-GRC or § 1 DSG incompatible to exclude the applicability of the GDPR to data processing related to the Google Analytics tool - in which individual website visitors are individualized using the Google Analytics identification number.

d) Traceability to the complainant

Regardless of the above considerations, it can be assumed that it can be traced back to the “face” of the complainant - such as his name:

Because it is not It is necessary that the respondents can each individually establish a personal reference, i.e. that all the information required for identification is with them (see the judgments of the ECJ of December 20, 2017, C-434/16, margin number 31, as well as October 19 2016, C 582/14, margin no.43). Rather, it is sufficient thatanyone - by legally permissible means and

reasonable effort - can establish this personal reference (cf. *Bergauer* in *Jahnel*, GDPR Comment Art. 4 no. 1 margin no. 20 mVa *Albrecht / Jotzo*, The new data protection law of the EU 58).

Such an interpretation of the scope of Art. 4 No. 1 GDPR can be derived - in addition to the legal and literature sources cited - from Recital 26 GDPR, according to which not only the means of the person responsible (here: the first respondent) must be taken into account when it comes to the question of identifiability, but also those “one others Person "(English version of the regulation:" by another person "). This also results from the idea of offering data subjects the greatest possible protection for their data.

The ECJ has repeatedly stated that the scope of the GDPR "very far "is to be understood (see for example the rulings of the European Court of Justice of June 22, 2021, C 439/19, margin no.61; for a comparable legal situation, the rulings of December 20, 2017, C 434/16, margin no May 2009, C 553/07, margin no.59).

It is not overlooked that, according to Recital 26 GDPR, it must also be taken into account with what "probability" someone uses means to directly or indirectly identify natural persons. In fact, in the opinion of the data protection authority, the term “someone” - and thus the scope of Art. 4 no. 1 GDPR - is indeednot to be interpreted so broadly that any stranger Actor could theoretically have special knowledge in order to establish a personal reference; This would mean that almost all information falls within the scope of the GDPR and a differentiation from non-personal data would be difficult or even impossible.

Rather, the decisive factor is whether identifiability can be established with justifiable and reasonable effort (cf. the decision of December 5, 2018, GZ DSB-D123.270 / 0009- DSB / 2018, according to which personal data is no longer available if the person responsible or a third party can only establish a personal reference with disproportionate effort).

In the present case, however, there is now particular Actors who have specialist knowledge that makes it possible, in the sense of the above, to establish a reference to the complainant and therefore to identify him.

First of all, this is the Second Respondent :

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

This means that the second respondent has at least received the information that the user of the Google account [redacted] the website www. [redacted] at has visited.

Even if one takes the view that the online IDs listed above must be assignable to a certain "face", such an assignment can in any case via the Google account of the complainant.

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

However, if - and this was convincingly stated by the complainant - the identifiability of a website visitor only depends on whether certain declarations of intent are made in the account, then they all lie (from a technical point of view) opportunities for an identifiability. Looking at it differently, the Second Respondent may not be able to comply with a user's wishes for “personalization” of the advertising information received, as expressed in the account settings.

In this context, reference should be made expressly to the unambiguous wording of Art. 4 Z 1 GDPR, which is addressed to a Be able is linked to (“can be identified”) and not to whether an identification is ultimately also carried out.

Likewise, it is expressly anchored in the GDPR accountability to inform the respondent - as the person responsible, further below - to use suitable technical and organizational measures in accordance with Art. 5 Paragraph 2 in conjunction with Art. 24 Paragraph 1 in conjunction with Art. 28 Paragraph 1 GDPR to ensure and to be able to provide evidence of this that the processing (with the help of a processor) in accordance with the regulation . It is therefore an obligation to deliver.

This also includes proof that processing is currently not subject to the regulation. One such was - despite several possibilities granted -not provided .

Regardless of the second respondent, however - and this is of greater relevance on a case-by-case basis - the US authorities to consider:

As the complainant has also rightly pointed out, US intelligence services take certain online identifiers (such as the IP address or unique identification numbers) as starting point for monitoring individuals. In particular, it cannot be ruled out that these intelligence servicesalready Have collected information with the help of which the data transferred here can be traced back to the person of the complainant.

The fact that this is not just a "theoretical danger" is shown by the judgment of the ECJ of July 16, 2020, C 311/18, which was based on the incompatibility such methods and access options of the US authorities with the fundamental right to data protection according to Art. 8 EU-GRC has ultimately also declared the EU-US adequacy decision ("Privacy Shield") to be invalid.

This is particularly evident from the - mentioned in the factual findings - Transparency report of the second respondent who proves that there are data requests from US authorities to the second respondent. Metadata and content data can be requested from the second respondent.

It is true that it is not overlooked that it is of course not possible for the Respondent to check whether such accesses by US authorities occur in individual cases - i.e. per website visitor - and what information US authorities already have; conversely, this circumstance cannot be charged with affected persons, such as the complainant. So it was ultimately the first respondent as (then)Website operator , which - despite the publication of the aforementioned judgment of the European Court of Justice of July 16, 2020 - the tool Google Analytics Farther has used.

As a further interim result, it should be noted that the factual findings under C.9. The information listed (in any case in combination) is personal data in accordance with Art. 4 No. 1 GDPR.

e) Distribution of roles

As already stated, the First Respondent, as the website operator, has the decision met the tool "Google Analytics" on the website www.

[redacted] at to implement. Specifically, she has oneJavaScript code ("day of made available by the second respondent, inserted in the source text of their website, whereby this JavaScript code was executed in the complainant's browser when the website was visited. In this regard, the Respondent stated that the tool mentioned was used for the purpose ofstatistical evaluations is used on the behavior of website visitors (see statement of December 16, 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 (at least) as responsible is to be considered within the meaning of Art. 4 Z 7 GDPR.

What the Second Respondent It should be noted that the subject of the complaint relevant here (only) relates to the transfer of data to the second respondent in the USA. A possible further data processing of the factual determinations under C.9. The information cited (by Google Ireland Limited or the second respondent) is not the subject of the complaint and was therefore not determined in more detail in this direction.

With regard to the data processing in connection with the Google Analytics tool, it should be noted that the second respondent only makes this available and also has no influence on whether and to what extent the first respondent makes use of the tool functions and which specific settings she chooses.

As far as the Second Respondent therefore only provides Google Analytics (as a service), it has no influence on the "purposes and means" of data processing and is therefore case-related within the meaning of Art. 4 Z 8 GDPR Processor to qualify.

These considerations are made without prejudice to a further official review procedure in accordance with Article 58 (1) (b) GDPR and without prejudice to the second respondent's role in data protection law with regard to possible further data processing.

D.3. Ruling point 2. b)

a) Scope of Chapter V GDPR

The first thing to check is whether the First Respondent is subject to the obligations set out in Chapter V of the Ordinance.

According to Art. 44 GDPR, any *"[...] Transmission of personal data that is already being processed or after it Transmission to a third country or an international organization are to be processed, [...] only permitted if the controller and the processor comply with the conditions set out in this chapter and the other provisions of this ordinance are also complied with; this also applies to any further transfer of personal data from the third country or international organization concerned to another third country or international organization.All provisions of this chapter are to be applied to ensure that this is supported by this Ordinance guaranteed level of protection for natural persons is not undermined . "*

In the "Guidelines 5/2021 on the relationship between the scope of Art. 3 and the requirements for international data traffic in accordance with Chapter V GDPR" (currently still in public consultation), the EDPS has three cumulative Requirements identified when a "transfer to a third country or an international organization" within the meaning of Art. 44 GDPR is present (ibid. Rz 7):

- the person responsible for the processing or a processor is subject to the GDPR for the processing concerned;
- this person responsible for the processing or processor ("data exporter") lays by transmission or in some other way personal data that is the subject of this processing to another controller, a joint controller or a processor, open minded ("Data Importer");

- the data importer is located in a third country or is an international organization, regardless of whether this data importer is subject to the processing in question in accordance with Art. 3 of the GDPR or not.

The First Respondent has her own Based in Austria and at the time of the complaint was responsible for the operation of the website www. [redacted] at data protection officer.
In addition, the first respondent (as the data exporter) disclosed the complainant's personal data by proactively using the Google Analytics tool on its website www.
[redacted] at implemented has and as a direct consequence of this implementation, among other things Data was transferred to the second respondent (to the USA). After all, the second respondent in his capacity as a processor (and data importer) has his Based in the USA .

Since all the requirements set out in the EDPB guidelines are met, the First Respondent as data exporter complies with the provisions of Chapter V of the Ordinance.

b) Regulations of Chapter V GDPR

It is then necessary to check whether the data has been transferred to the USA in accordance with the provisions of Chapter V GDPR.

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

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

c) Adequacy decision

The ECJ has ruled that the EU-US adequacy decision ("Privacy Shield") - without maintaining its effect - is invalid (see the judgment of July 16, 2020, C 311/18 margin no. 201 f).

The present data transfer is therefore not covered by Art. 45 GDPR.

d) Appropriate guarantees

As can be seen from the factual findings, the respondents on August 12, 2020 Standard data protection clauses (hereinafter: SDK) according to Art. 46 Para. 2 lit. c GDPR for the transmission of personal data to the USA ("Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors"). Specifically, it was about

complaint time around those Clauses in the Version of Implementing decision of the European Commission 2010/87 / EU of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors in third countries according to Directive 95/46 / EC of the European Parliament and of the Council, OJ L 2010/39, p. 5 .

In the above-mentioned judgment of July 16, 2020, the ECJ stated that SDKs as an instrument for international data traffic are basically not objectionable, but the ECJ also pointed out that SDKs are, and therefore, a contract by their nature Authorities from a third country cannot bind:

According to this, there are situations in which the recipient of such a transmission can guarantee the necessary data protection solely on the basis of the standard data protection clauses, given the legal situation and practice in the third country concerned, but there are also situations in which the provisions contained in these clauses may be insufficient funds in order to ensure the effective protection of the personal data transmitted to the third country concerned in practice. This is how it is when thatLaw of this third country whose Authorities Intervention in the rights of the data subjects with regard to this data is permitted ”(ibid. Margin no. 126).

A more detailed analysis of the legal situation in the USA (as a third country) can be omitted at this point, as the ECJ already dealt with this in the cited judgment of July 16, 2020. He came to the conclusion that the EU-US adequacy decision based on the relevant law of the USA and the implementation ofgovernment surveillance programs - based on Section 702 of FISA and EO 12333 in conjunction with PPD-28 - no adequate level of protection for natural persons guaranteed (ibid. Margin no. 180 ff).

These considerations can be transferred to the present case. It is evident that the second respondent is to be qualified as a provider of electronic communications services within the meaning of 50 US Code § 1881 (b) (4) and is therefore subject to surveillance by US intelligence services in accordance with 50 US Code § 1881a (“FISA 702”). Accordingly, the second respondent is obliged to provide the US authorities with personal data in accordance with 50 US Code § 1881a.

As can be seen from the Transparency report ("Transparency Report") of the second respondent, such inquiries are also regularly made to them by US authorities (see https:// transparencyreport.google.com/user-data/us-national-security?hl=en, queried at the December 22, 2021).

If, however, the EU-US adequacy decision has already been declared invalid due to the legal situation in the USA, it cannot be assumed on a case-by-case basis that the (mere) conclusion of SDK guarantees an appropriate level of protection according to Art. 44 GDPR for the data transfer in question.

Against this background, the ECJ also stated in the cited judgment of July 16, 2020 that *"[...] By their nature, standard data protection clauses cannot offer guarantees that go beyond the contractual obligation to ensure compliance with the level of protection required by Union law [...]"* and it "[...] *Depending on the situation in a particular third country, it may be necessary for the controller additional measures takes to ensure compliance with this level of protection "* (ibid. margin no.133).

The present data transmission can therefore not alone are based on the standard data protection clauses concluded between the respondents in accordance with Art. 46 Paragraph 2 lit. c GDPR.

e) General information on "additional measures"

In its "Recommendations 01/2020 on measures to supplement transmission tools to ensure the level of protection under Union law for personal data", the EDSA stated that in the event that the law of the third country affects the effectiveness of suitable guarantees (such as SDK) , the data exporter either suspends the data transfer or has to implement additional measures ("supplementary measures") (ibid. margin nos. 28 ff and margin nos. 52).

According to the recommendations of the EDPB, such "additional measures" within the meaning of the judgment of the ECJ of 16 July 2020 can be of a contractual, technical or organizational nature (ibid. Margin no. 47):

With regard contractual Measures it is stated that *these "[...] complement and reinforce the guarantees offered by the transmission instrument and the relevant legal provisions in the third country, insofar as the guarantees, taking into account all the circumstances of the transmission, do not meet all the requirements necessary to ensure a level of protection that which is essentially equivalent in the EU. Since the contractual measures according to their naturegenerally cannot bind the authorities of the third country If they are not themselves a party to the contract, they must be combined with other technical and organizational measures to ensure the required level of data protection. Just because one or more of these measures has been selected and applied does not necessarily mean that it is systematically ensured that the intended transmission meets the requirements of Union law (guarantee of an essentially equivalent level of protection) "* (ibid. Rz 93).

to organizational Action is carried out that it is itself *"[...] about internal strategies, organizational methods and standards that controllers and processors could apply 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, organizational measures are required complement the*

contractual and / or technical measures are required to ensure that the protection of personal data is essentially equivalent to the level of protection guaranteed in the EU (ibid. margin no. 122).

to technical Measures are carried out that are intended to ensure that *"[...] the access of the authorities in third countries to the transmitted data does not undermine the effectiveness of the appropriate guarantees listed in Article 46 GDPR. Even if government access is consistent with the law of the data importer's country, these measures should be considered when government access goes beyond what is necessary and proportionate in a democratic society. These measures aim to exclude potentially infringing access by using thePrevent authorities from doing so to identify data subjects, to develop information about them, to determine them in other contexts or to link the transmitted data with other data records held by the authorities which, among other things, data about Online identifiers Containing devices, applications, tools and protocols that the data subjects have used in other contexts* (ibid. margin no.74).

Finally, the EDPS has stated that such “additional measures” can only be considered as effectively are to be considered within the meaning of the judgment of July 16, 2020, *"[...] if and to what extent the measure precisely closes the legal protection gaps determined by the data exporter during his examination of the legal situation in the third country. If it is ultimately not possible for the data exporter to achieve an essentially equivalent level of protection, he may not transmit the personal data "*(ibid. 70).

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

f) "Additional Measures" by the Second Respondent

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

In relation to the set out contractual and organizational Action is not recognizable to what extent a notification of the data subject about data requests (should this be permissible in the individual case at all), the publication of a transparency report or a "guideline for handling government inquiries" effectively in the sense of the above considerations. It is also unclear to what extent the "careful examination of every data access request" is aeffective measure represents, since the ECJ ruled in the aforementioned judgment of June 20, 2020 that permissible (i.e. in accordance with

US law legal) requests from US intelligence services not are compatible with the fundamental right to data protection according to Art. 8 EU-GRC.

Unless the technical Measures are affected as well not recognizable - and was also not explained comprehensibly by the respondents - to what extent the protection of communication between Google services, the protection of data in transit between data centers, the protection of communication between users and websites or "on-site security" Actually prevent or restrict access by US intelligence services based on US law.

If the second respondent subsequently refers to encryption technologies - such as the encryption of "data at rest" in the data centers - he must again be countered with recommendations 01/2020 of the EDSA. Namely, it states that a data importer (such as the Second Respondent) who is subject to 50 US Code § 1881a ("FISA 702") has a direct obligation with regard to the imported data that is in his possession, custody or control to grant access to or release them. This obligation can expressly also apply to thecryptographic key without which the data cannot be read (ibid. margin no. 76).

As long as the second respondent has the opportunity to access data in the Plain text access, the technical measures taken cannot be regarded as effective in the sense of the above considerations.

As a further technical measure, the second respondent adds that so far *"[...] Google Analytics data are personal data for measurement by website owners, [...] they are regarded as pseudonymous "* (see his statement of April 9, 2021, p. 26).

However, this is countered by the convincing view of the German Data Protection Conference, according to which *"[...] the fact that the users can be identified using IDs or identifiers, none Pseudonymization measure i. S. d. GDPR represents. In addition, these are not suitable guarantees to comply with data protection principles or to safeguard the rights of data subjects if IP addresses, cookie IDs, advertising IDs, unique user IDs or other identifiers are used to (re) identify users Use. Because, unlike in cases in which data is pseudonymized in order to disguise or delete the identifying data so that the data subjects can no longer be addressed, IDs or identifiers are used used for this , the individual individuals to make distinguishable and addressable . As a result, there is no protective effect. It is therefore not a matter of pseudonymizations i. S. d. Recital 28, which reduce the risks for the persons concerned and support the responsible parties and the processors in complying with their data protection obligations "*(see the guidance of the supervisory authorities for providers of telemedia from March 2019, p. 15).

In addition, the submission of the second respondent cannot be followed because the Google Analytics identifier - as stated above - is in any case combined with other elements and even with one that is undisputedly attributable to the complainant Google Account can be associated.

The mentioned "anonymization function of the IP address" is not relevant on a case-by-case basis, since - as also stated above - not has been implemented correctly. Apart from that, the IP address is only one of many “puzzle pieces” of the complainant's digital footprint.

As a further interim result, it should be noted that the "additional measures" in question not are effective, as these do not close the legal protection gaps identified in the framework of the judgment of the ECJ of June 20, 2020 - i.e. the access and monitoring options of US intelligence services.

The data transfer in question is therefore not covered by Art. 46 GDPR.

D.4. Ruling point 2. c)

a) On Art. 49 GDPR

According to the Respondent's own statements, the exception regulation pursuant to Art. 49 GDPR was not relevant for the transfer of data in question (see the statement of December 16, 2020).

Consent in accordance with Article 49 (1) (a) GDPR was not obtained. The data protection authority is also unable to determine to what extent another offense of Art. 49 GDPR is to be fulfilled.

The present data transmission can therefore also not based on Art. 49 GDPR.

b) Result

There for the representational Data transfer the first Respondent on the Second respondent (in the USA) was not guaranteed an adequate level of protection by an instrument of Chapter V of the Regulation, there is a violation of Art. 44 GDPR.

The first Respondent was (at least) to time relevant to the complaint - i.e. August 14, 2020 - for the operation of the website www. [redacted] at responsible. The one relevant here Data protection violation of Art. 44 GDPR is therefore attributable to the first respondent.

It was therefore according to the ruling to decide.

D.5. To the remedial powers

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

Since the responsibility for the operation of the website www. Compla[redacted]int at during the procedure (but only after August 14, 2020) to the [redacted] GmbH with Seat in Munich and Google Analytics is still implemented at the time of the decision, the data protection authority will bring the case to the competent German supervisory authority with regard to the (possible) use of the remedial powers pursuant to Art. 58 (2) GDPR.

D.6. Ruling point 3

It should be checked whether the Second Respondent (as data importer) is subject to the obligations set out in Chapter V of the Ordinance.

Based on the above-mentioned guidelines 5/2021 of the EDPB, it should again be stated that a transfer to a third country or an international organization "within the meaning of Art. 44 GDPR only exists if, among other things, the person responsible for the processing or the processor (data exporter) by transfer or in any other way personal data that is the subject of this processing, another person responsible for the processing, a jointly responsible person or a processor (data importer), disclosed .

In the present case, this requirement does not apply to the second respondent, since he (as the data importer) has the personal data of the complainant not discloses, but (only) receives it. In other words: The requirements of Chapter V GDPR are from the dataexporter , but not to be observed by the data importer.

The complainant's argument that a data transfer necessarily requires a recipient and that the second respondent (at least from a technical point of view) is part of the data transfer is not overlooked. However, this can be countered by the fact that the data protection responsibility for a processing operation (from a legal point of view) can still be "shared", i.e. one depending on the phase of the processing operationdifferent degrees who can give responsibility (cf. EDSA guidelines 7/2020 on the concept of controllers and processors, margin no. 63 ff with further references).

A violation of Art. 44 GDPR by the Second In the opinion of the data protection authority, there are therefore no respondents.

So overall was according to the ruling to decide.

Finally, it should be pointed out that on the question of the (possible) violation of Art. 5 ff in conjunction with Art. 28 Para. 3 lit. a and Art. 29 GDPR, the second respondent will agree to a further decision.

Legal remedies

You can object to this decision within **four weeks** a complaint can be made in writing to the Federal Administrative Court after delivery. The complaint**must be submitted to the data protection authority** and have to

- the name of the contested decision (GZ, subject)
- the name of the authority concerned,
- the reasons on which the allegation of illegality is based,
- the desire as well
- the information required to assess whether the complaint has been submitted in good time,

contain.

The data protection authority has the option to either through within two months **Appeal preliminary decision** to change your decision or the complaint with the files of the proceedings **to be submitted to the Federal Administrative Court**.

The complaint against this decision is **charges apply.** The fixed fee for a corresponding entry including enclosures is **30 euro**. The fee is to be paid to the account of the Austrian tax office, stating the purpose.

The fee is generally to be transferred electronically using the “tax office payment” function. The Austrian Tax Office - Special Responsibilities Office must be specified or selected as the recipient (IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW). Furthermore, the tax number / tax account number 10 999/9102, the tax type “EEE complaint fee”, the date of the notification as the period and the amount must be specified.

If the e-banking system of your bank does not have the “tax office payment” function, the eps procedure can be used in FinanzOnline. An electronic transfer can only be dispensed with if no e-banking system has been used up to now (even if the taxpayer has an internet connection). The payment must then be made by means of a payment order, paying attention to the correct allocation. Further information is available from the tax office and in the manual "*Electronic payment and notification of payment of self-assessment taxes*".

The payment **the fee** is when the complaint is lodged **towards the data protection authority** by means of a payment receipt to be added to the input or a printout of the issue of a payment order **to prove**. If the fee is not paid or not paid in full, a**Report to the responsible tax office**.

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

December 22, 2021

For the head of the data protection authority:

[redacted]

REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR	Signatory	serialNumber = 1831845058, CN = Data Protection Authority, C = AT
	Date Time	2022-01-12T12: 14: 21 + 01: 00
	Test information	Information on checking the electronic seal or electronic signature can be found at: https://www.signaturpruefung.gv.at Information on checking the printout can be found at: https://www.dsb.gv.at/-/amtssignatur
	notice	This document was officially signed.