noyb - European Centre for Digital Rights
Goldschlagstrasse 172/4/3/2
1140 Vienna
AUSTRIA

To the:
Austrian Data Protection Authority
Barichgasse 40-42
1030 Vienna

By e-mail: dsb@dsb.gv.at

Vienna, 05.05.2021

Ref. no. of the DSB:	**D155.027**
Ref. no. of *noyb*:	**C-029-44**
Complainant:	[redacted]
Represented pursuant to Article 80(1) of the GDPR by:	***noyb* - European Centre for Digital Rights** Goldschlagstr. 172/4/3/2, 1140 Vienna
Respondent to the first complaint	**netdoktor.at GmbH** Heiligenstädter Lände 29 / Top 5 1190 Vienna
Represented by:	**DORDA Lawyers Ltd.** University Ring 10 1010 Vienna
Second respondent:	**Google LLC** 1600 Amphitheatre Parkway Mountain View, CA 94043, United States of America
Regarding:	Transfers of personal data to third countries (Article 44 et seq. GDPR)

SUBMISSION

Table of contents

A. General remarks

The questions raised by the DSB and the EDPB seem to go beyond the scope of complaint D155.027. We have therefore decided to highlight in **Part B** the relevant elements for the complaints procedure and penal proceedings.

In **Part C** we comment on all elements raised by Google LLC.

In general, it should be noted that Google LLC answered the DSB's questions only inadequately or evasively and made irrelevant or even misleading submissions in some places. This should probably be taken into account within the penalty assessment (maximum penalty: € 6 billion).

B. On the infringement of Article 44 GDPR by Google LLC

1. Subject matter of the complaint with regard to Google LLC

The subject matter of the complaint procedure pursuant to Section 24 of the DSG is to be determined by the complaint itself. With regard to Google LLC, only the transmission and receipt of the data ("processing" within the meaning of Article 4(2) of the GDPR) contrary to Article 44 et seq. of the GDPR or the subsequent unlawful further processing in the USA (for example, further storage) is relevant.

It is undeniable that Google LLC's responses alone would give rise to further proceedings (such as on transfers to countless other countries, onward processing as a controller, or on the changing and unclear role of Google Ireland Ltd). Of course, it is up to the other supervisory authorities in the EEA to check these elements officially.

However, the complainant considers this to be outside the scope of this complaint. These elements also seem irrelevant for the assessment of the breach of law by Google LLC in the context of the data transfer to the USA.

2. Applicability of the GDPR to data processing operations carried out by Google LLC

The material scope of application of the GDPR is satisfied pursuant to Article 2(1) of the GDPR, as personal data of the complainant were processed via Google Analytics when he visited the website of netdoktor.at GmbH on 14.08.2020. This resulted in particular in a transfer of personal data of the complainant from netdoktor.at GmbH to Google LLC (See in detail point B. 5.2).

The geographical scope of application is also satisfied with regard to the processing operations at issue, since Google LLC monitors the "*behaviour*" of data subjects in the EEA via Google Analytics pursuant to Article 3(2)(b) GDPR.

Pursuant to Article 3(2) of the GDPR, the personal scope of application of the GDPR applies irrespective of whether Google LLC has carried out the processing operations in question as a (sub-)processor of netdoktor.at GmbH or as a controller, as the GDPR explicitly applies to a "*controller or processor not established in the Union*", provided that the circumstances set out in Article 3(2)(a) or (b) of the GDPR are fulfilled.

3. Google Ireland Ltd. is not a party to the proceedings and is otherwise irrelevant

The complaint is directed against netdoktor.at GmbH (first respondent) as a data exporter located in the EEA and Google LLC (second respondent) as a data importer located in the USA.

Google Ireland Ltd. is not a party to the proceedings before the DSB, in particular because:

- At the time of the website visit (14.08.2020), only netdoktor.at GmbH and Google LLC were contracting parties (see Attachments 1 and 3).
- Subsequent changes to the contractual structure with regard to Google Analytics (contract takeover by Google Ireland Ltd., as stated under "Questions and Answers" in the statement by Google LLC) are therefore irrelevant.
- The mere adoption of contracts by Google Ireland Ltd. would also not establish an objectively assessable role as "controller" or "processor" under Article 4(7) or (8) GDPR - the GDPR excludes a mere declaration of roles ("*forum shopping*").
- Crucially, nothing changes even after the current situation described: Even after 30 April 2021, data transfers in connection with Google Analytics are to be based on standard contractual clauses between the website owner as data exporter and Google LLC as data importer (see "Questions and Answers" as well as answer 22 and footnote 3 in the statement by Google LLC).
- It would also be irrelevant whether personal data of the complainant were transferred to Google LLC via an "intermediate stop" at Google Ireland Ltd. or directly by netdoktor.at GmbH. Even an "intermediate stop" does not change the relevant processing activities (transmission by netdoktor.at GmbH or receipt of the personal data by Google LLC). Google LLC alone names 105 sub-processors (see point C. 4.3.) whose data processing activities are not the subject of the complaint. In addition, from network providers to hosting providers, countless other controllers and processors ("intermediate stops") are presumably involved in the processing anyway, whose data processing activities are also not the subject of the complaint.

- In any case, it is decisive that Google LLC as the data importer collected and processed personal data of the complainant in violation of Articles 44 et seq. of the GDPR at the relevant time (see below).

4. The DSB is directly responsible for Google LLC

According to Article 55 of the GDPR, each supervisory authority is globally competent for complaints and processing operations. The exception contanied in Article 56 of the GDPR is not applicable in the present case, as Google LLC - as a controller or processor - does not maintain its "main establishment" in the EEA.

In particular, Google Ireland Ltd. is, according to Google LLC, an independent controller or processor and therefore not an "establishment" of Google LLC in the EEA. In other words, a company cannot at the same time be an independent controller or processor within the meaning of Article 4(7) and (8) GDPR respectively, and also be the "establishment" of another controller or processor. Google Ireland Ltd. cannot therefore be considered the "main establishment" of Google LLC within the meaning of Article 4(16) of the GDPR with regard to data processing in connection with Google Analytics. Article 56 GDPR is therefore not applicable, which Google LLC also seems to acknowledge.

We assume that the DSB under the EDPB has the relevant communications from Google LLC with other regulators on this issue, but we are also happy to provide them to the extent that they are available to us.

5. Google LLC has demonstrably violated Article 44 *et seq.* GDPR

5.1. Chapter V of the GDPR directly applies to Google LLC as a processor

Article 44 of the GDPR explicitly requires the "controller and processor" to comply with Chapter V of the GDPR.[1] This not only applies to the receipt of personal data in the third country (relevant here for Google LLC) but would even apply to onward transfers (emphasis added):

> "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions of this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

[1] See *Schröder* in Kühling/Buchner (eds.), GDPR BDSG3(2020), Article 44 GDPR, para 5.

5.2. Data transfer to Google LLC in the USA is undisputed

It is clear from the available technical documentation and Google LLC's responses that (personal) data belonging to the complainant was transferred to the USA (or that the use of Google Analytics generally leads to a transfer of website visitors' data to the USA):

The fact that all data processed in connection with Google Analytics are ultimately (also) processed on servers located in the USA is openly admitted by Google LLC itself in its answer to questions 7 and 8 and is therefore undisputed:

> "*All data collected through Google Analytics (see our response to question #2) is hosted (i.e. stored and processed) in the USA.*"

5.3. Personal nature of the transmitted data is undisputed and proven

5.3.1. Google LLC's own information confirms transmission of personal data

It is further undisputed that the data transmitted are "personal data" within the meaning of Article 4(1) of the GDPR:

- netdoktor.at GmbH and Google LLC themselves clearly assume that there will be processing of personal data including their transfer to a third country - otherwise the conclusion of a contract processing agreement pursuant to Article 28 of the GDPR including standard contractual clauses pursuant to Article 46(2)(c) of the GDPR (see Attachment 3; in particular point 10.2) would be completely pointless.
- In its answer to question 6, Google LLC clearly states that a data subject can be identified by means of a "user identifier" for the purpose of deletion. This means that there is the possibility of identifiability within the meaning of Article 4(1) of the GDPR (see in detail point C. 6.).
- Similarly, Google LLC explicitly states in response to question 13 that Google Analytics uses a "*unique identifier, associated with that particular user*".
- In its answer to question 28 under "Pseudonymity of Google Analytics data", Google LLC states that the data transmitted to Google LLC would sometimes only be "pseudonymous data". Apart from the fact that this is factually incorrect - see point C. 22.9. for details - Google LLC once again admits to processing personal data in any case, since pseudonymised data (Article 4(5) of the GDPR) also fall under the concept of personal data within the meaning of Article 4(1) of the GDPR, and are thus fully subject to the provisions of Chapter V of the GDPR.

5.3.2. Deliberately set cookie data and user identification numbers (UIDs)

The evidence presented also makes it indisputable that netdoktor.at and Google LLC process and transfer personal data to the USA:

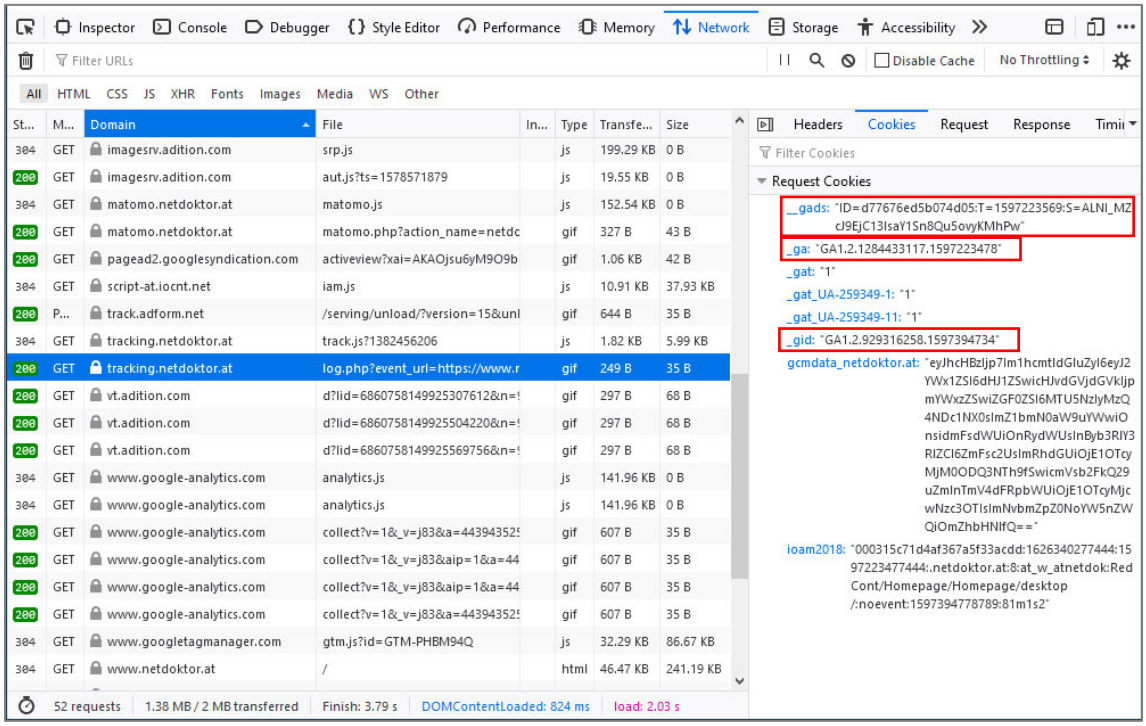
(1) At least some of the cookies set on the occasion of the website visit on 14.08.2020 contain unique user identification numbers (see HAR file, Attachment 4), in particular the cookies "_ga" and "_gid" which, according to Google documentation (Attachment 7), contain a user identification number and are "*used to distinguish users*" and the cookie "_gads" which, according to Google's privacy statement (Attachment 8), "*enables websites* to *display advertising from Google, including personalised advertising*". Also the value "cid" in URLs, which according to Google (Attachment 9) is supposed to identify users and corresponds to the value in the "_ga" cookie.

(2) For example, the following personal data (in particular cookies or identifiers) were demonstrably created or processed by Google LLC in the specific case (see HAR file, Attachment 4):

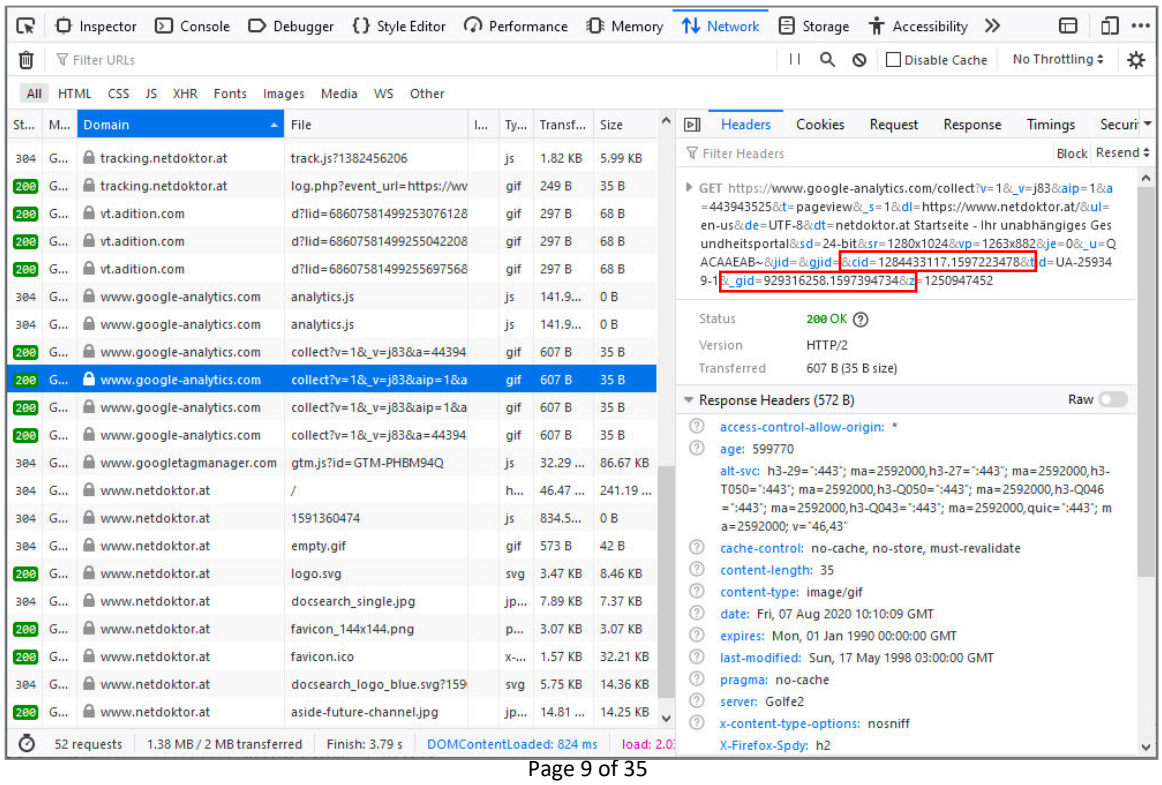
Domain	Name	Value	Purpose
https://tracking.netdoktor.at/	_ga	GA1.2.1284433117.1597223478	Google Analytics
https://tracking.netdoktor.at/	_gid	GA1.2.929316258.1597394734	Google Analytics
https://tracking.netdoktor.at/	_gads	ID=d77676ed5b074d05:T=1597223569:S=ALNI_MZcJ9EjC13lsaY1Sn8Qu5ovyKMhPw	Google Advertising
https://www.google-analytics.com/	_gid	929316258.1597394734	Google Analytics
https://www.google-analytics.com/	cid	1284433117.1597223478	Google Analytics

Identical values that occurred in different transactions were colour-coded (orange and green).

(3) For example, in the transaction between the complainant's browser and https://tracking.netdoktor.at/, which was started on 14/08/2020 at 12:46:19.344 CET, the user identification numbers were set in the cookies "__gads", "_ga" and "_gid":



(4) Similarly, these user identification numbers "_gid" and "cid" were transmitted to https://www.google-analytics.com/ on 14/08/2020 at 12:46:19.948 CET (i.e. 604 mos. later):



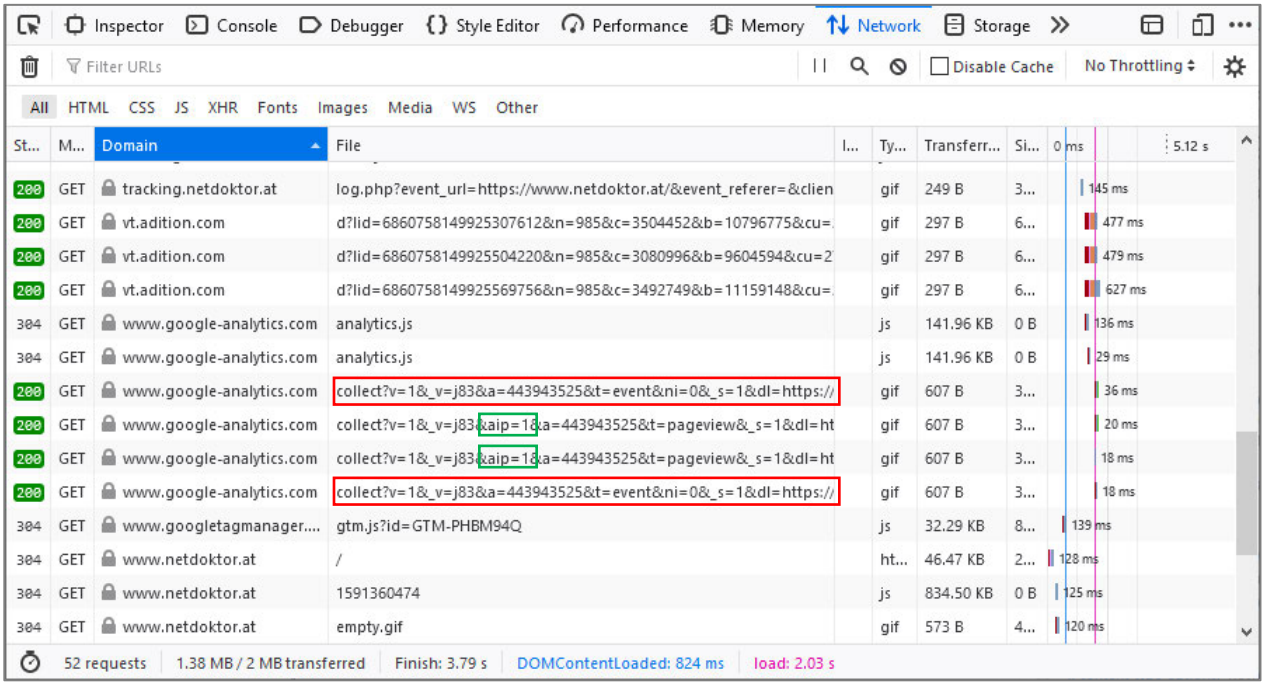
These user identification numbers are each an "online identifier" within the meaning of Article 4(1) of the GDPR, which serves to identify natural persons and is specifically assigned to a user. These user identification numbers - or the information linked to them - are therefore to be treated as "personal data" without any doubt.

5.3.3. Technically unavoidable transmission of IP addresses

- In any case, the IP address of the complainant was also transmitted. This is a personal data and was transmitted to Google LLC. Even a possible anonymisation of the IP address put forward by Google does not change this, as it only takes place after Google has collected the IP address (see point C. 4.2).

  Chapter V of the GDPR also does not provide for any exceptions for "subsequently anonymised data", which is why this line of argument by Google LLC is legally irrelevant anyway.

- Furthermore, a closer examination of the HAR file (Attachment 4) revealed that only two (green) of four transactions with https://www.google-analytics.com/ contained the necessary "*api=1*" parameter for the anonymisation of IP addresses:



It must therefore be assumed (in the absence of other evidence) that the complainant's IP address was not even anonymised in all transactions. The relevant parameters are missing in at least two transactions (red mark).

However, this circumstance does not seem to be legally relevant, as the anonymisations are only carried out after transmission anyway (see above), which is why we refrain from further explanations on this.

5.3.4. Use of Google DoubleClick, Google Tag Manager, a Google account and option of data sharing by netdoktor.at GmbH

The available data in the HAR file (Attachment 4) also indicate other forms of data sharing, in particular data exchange with the Google Syndication service (ade.googlesyndication.com), which also enables connections to Google LLC advertising (doubleclick.net). Likewise, netdoktor.at GmbH uses Google Tag Manager, which can be seen, for example, in the transactions to https://www.google-analytics.com/ (with the value "gtm=2wg871PHBM94Q"). Here, too, there is at least the question of the exchange of IP addresses and other identification numbers.

The complainant was also logged into his private Google account at the time of the website visit, which is likely to lead to additional identifiability for Google LLC (see point C. 8.).

Finally, Google itself describes in questions/answers 3, 4, and 13 that depending on the settings of netdoktor. at GmbH (which are naturally unknown to the complainant), the complainant's data could be synchronised with other Google services. For this, too, these personal data must at least already be available to Google LLC.

In summary, it is undisputed and apparent that Google LLC received and processed various types of personal data of the complainant.

A concrete argument to the contrary also does not exist because Google LLC does not address the individual case in the current complaint with a single word.

5.4. Data transfer based on Article 46(2)(c) of the GDPR is unlawful

5.4.1. Google LLC uses standard contractual clauses pursuant to Article 46(1)(c) GDPR

Google LLC's response to question 22 indicates that Google LLC has based data transfers from the EU since 12.08.2020 solely on standard contractual clauses under Article 46(2)(c) of the GDPR (specifically, those under Commission Decision 2010/87/EU).

As the CJEU held in C-311/18, this is not sufficient if the law of the third country makes compliance with the standard contractual clauses impossible (see paragraphs 134, 135 of the judgment and already paragraph 6 of the complaint).

5.4.2. Google LLC falls under FISA 702 and provides data to the USA

Google LLC, as an "*electronic communication service provider*" under 50 USC § 1881 (4), was and is required to provide personal data under 50 USC § 1881a and even publicly admits to doing so - see the transparency report linked in the answer to question 28. [2]

Google LLC is therefore categorically unable to comply with the appropriate safeguards required by the CJEU in C-311/18 to ensure compliance with the level of data protection required by EU law (see in this respect paragraph 180 *et seq.* of the judgment).

Furthermore, by disclosing personal data to administrative authorities attributable to the US government (such as US intelligence agencies), Google LLC continuously violates Article 48 of the GDPR, which was included in the current version of the GDPR as the "anti-NSA article" in response to the Snowden revelations.

5.4.3. The "additional measures" put forward are irrelevant

The "additional measures" described by Google LLC in its response to question 28 (in paragraph 133 of judgment C-311/18), while occupying five pages, are all completely ineffective or completely irrelevant in light of 50 USC § 1881a.

➔ **We refer to the details in the answer to question/answer 28 below.**

In summary, the inadequacies can be simply stated as follows:

50 USC § 1881a (i) requires general and common support to disclose all data requested by the US government ("acquisition") without any case-by-case decision under a "directive"). In the original text:

> *"...the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition".*

The technical implementation of direct data interception from hosting providers (known as "Upstream" or formerly "PRISM") is likely to involve an automated exchange of selectors (e.g. an email address, telephone number or user identifiers) using the FBI's "Direct Interception Unit" (FBI-DIU) and a subsequent transmission of relevant data.

In this context, the legal framework under 50 USC § 1881a does not provide for or allow for a case-by-case review or even a case-by-case decision. Google LLC only receives an annual "directive" to tolerate or support such a system, but is never put in the position of actually making "case-by-case

[2] https://transparencyreport.google.com/user-data/overview?hl=en (accessed 04.05.2021).

decisions", which would be impossible even with over 210,000 requests in 2019. Google LLC's suggested (but not actually advanced) case-by-case review is inconsistent with the US legal framework.

50 USC § 1881a(i)(4) accordingly also only allows a "directive" (i.e. an order to condone/support an entire surveillance programme) to be challenged in court. Since the grounds for such a remedy are extremely limited, no relevant protection would be expected even if Google LLC were to exhaust all remedies in the interest of its customers.

Google LLC's remaining submissions in its response to Question 28 are either:

(1) a description of the minimum level of data security required by Article 32 GDPR (access restrictions in data centres, encryption using HTTPS/TSL or AES-256, as with any normal website and smartphone) and therefore not an "additional measure",

(2) impossible simply because of the legal obligation of secrecy under US law (for example, informing the data subjects about a data query by the NSA) and/or

(3) technically irrelevant (for example, encryption if Google LLC itself holds the keys and therefore has to decrypt the data anyway in case of US government requests).

The "additional measures" put forward by Google LLC are therefore useless at best with regard to 50 USC § 1881a and EO 12.333, but are probably in reality an attempt to deliberately and brazenly deceive customers and authorities in the EEA in order not to have to change their systems (e.g. separating EU data from data centres that are under NSA access).

This deliberate deception in the interest of undisturbed profit maximisation is not only a violation of clause 5(b) of the Annex to Decision 2010/87, but must also be assessed in the context of the penalty assessment under Article 83(2) of the GDPR.

5.5. Infringement of Article 44 of the GDPR

In the absence of any other legal basis under Chapter V of the GDPR, the data transfer was in any case unlawful. Future comparable data transfers are to be prohibited pursuant to Article 58(2)(f) and (j) of the GDPR (see point B. 6.2).

6. On the DSB's powers and duty of enforcement under Articles 58(2) and 83 of the GDPR

6.1. Remedy of a completed breach of law is excluded

The visit to the website of netdoktor.at GmbH by the complainant on 14 August 2020 and the associated data transfers to the USA constitute a past, self-contained fact and constitute a breach of the GDPR that cannot be remedied. A subsequent elimination of the legal violation within the meaning of Section 24(6) of the DSG is therefore excluded.

6.2. Obligation to prohibit processing

The CJEU explicitly stated in paragraphs 113, 135 and 146 of judgment C-311/18 that "*the competent supervisory authority, [is] obliged to suspend or terminate the transfer of personal data to the third country concerned*".

In this respect, the DSB has no discretionary power: The further processing of personal data in connection with Google Analytics by netdoktor.at GmbH and Google LLC must be prohibited pursuant to Article 58(2)(f) and (j) of the GDPR or, in the case of Google LLC, the deletion of data already transmitted must also be ordered.

6.3. Obligation to penalise and exercise discretion under Articles 83(1) and (2) GDPR

The GDPR provides for an obligation of each supervisory authority to impose effective, proportionate and dissuasive penalties - see the wording "*shall ensure*" in Article 83(1) GDPR. Each supervisory authority is obliged to exercise its discretion as to the specific penalty on the basis of the criteria of Article 83(2) of the GDPR ("circumscribed discretion").

According to Article 83(5)(c) of the GDPR, the infringements committed by Google LLC are to be punished with 4% of the annual turnover achieved worldwide. The penalty range is thus - according to the last annual report[3] and the current conversion rate - approximately € 6.07 billion.

When exercising the obligated discretion in the context of the assessment of the penalty, it must be noted in particular as aggravating:

- that the transfer of the complainant's personal data is only one of millions of cases. Google LLC is taking personal data from thousands of websites and millions of data subjects in the EEA in connection with Google Analytics in breach of Article 44 *et seq.* of the GDPR (Article 83(2)(a) GDPR);
- that Google LLC was aware of the facts and of the law (see in particular judgment in C-311/18) and intentionally continues to transfer personal data to the US (Article 83(2)(b) GDPR);
- that Google LLC has made no attempt at serious harm reduction (see in particular point C. 22.) (Article 83(2)(c) GDPR);
- that Google LLC, as a processor under Article 38(3)(c) of the GDPR, bears sole responsibility for the transfers of the data to third parties and the lack of any technically reasonable measure (such as the separation of data from the EEA and storage outside the de facto access of US companies and US authorities) (Article 83(2)(d) of the GDPR);

[3] https://www.sec.gov/Archives/edgar/data/1652044/000165204421000006/googexhibit991q420.htm (aufgerufen am 03.05.2021).

- that Google LLC has now already been repeatedly penalized by European authorities (e.g. on 21.1.2019 and on 10.12.2020 by the French CNIL) for violations of the GDPR and so far - probably also because of the comparatively low penalties for Google - no change in behavior has occurred (Article 83(2)(e) GDPR);
- that Google LLC, by using deliberately ambiguous and vague wording in its statement, is working against clarification of the facts (Article 83(2)(f) GDPR; see for example point C. 2. and point C. 22.);
- that Google LLC broadly transfers extremely sensitive information about data subjects' website visits (in the event sometimes health information) to the US and therefore potentially has to make it available to the US government (Article 83(2)(g) GDPR);
- that Google LLC continues to deny committing a breach in the first place and that the breach only became known to the supervisory authority through a complaint under Article 77 GDPR (Article 83(2)(h) GDPR); and
- that Google LLC is attempting to cover up the evident breach of the law (Article 83(2)(k) GDPR) by means of misinformation about alleged "additional measures" vis-à-vis the public, customers and the authorities.

6.4. On the enforceability of a penalty notice against Google LLC

Finally, we would like to point out the assets of the Google Group that can be seized, as well as the option of third-party debtor execution in Austria and in the EU.

For example, the shares of Google Austria GmbH (FN 265694b) as well as any claims of the Google group against third-party debtors in Austria are attachable under the EO.

Likewise, pursuant to Article 9 of the Treaty between the Republic of Austria and the Federal Republic of Germany on Administrative and Legal Assistance in Administrative Matters (Federal Law Gazette No. 526/1990), Austrian administrative penalties are enforceable in Germany, which is highly relevant not only with regard to the shares in Google Germany GmbH (HRB 86891), but also with regard to third-party debtors in Germany (in particular the banking location in Frankfurt and any existing credit balances of the Google group with international financial institutions). Penalties are to be remitted to the requesting authority (i.e. the DSB) in this regard.

Finally, reference should be made to the possibilities of the EU-VStVG (BGBI. I Nr. 3/2008) and the Council Framework Decision 2005/214/JHA, which could enable enforcement of DSB penalties throughout the EU, although according to Section 9 EU-VStVG the proceeds of the penalty accrue to the legal entity in the requested EU Member State.

In our view, there is therefore nothing to prevent the corresponding enforceability of a decision issued by the DSB against Google LLC in terms of substantive law and procedural law.

C. Google LLC's responses in detail

In the following, we would like to address Google LLC's responses in detail. To the extent that we do not comment on individual statements or allegations made by Google LLC, this does not mean that the complainant acknowledges the legal opinion of the respondent or that the these elements are undisputed.

1. Re. "Questions and Answers"

Google LLC states that it refers to Google LLC and Google Ireland Ltd. together as "Google" in its responses, unless the distinction between the companies is relevant. Similarly, Google always answers the DSB's questions about "Google Services Tools" with an answer about Google Analytics only (see for instance answer 3 in Google LLC's statement).

Since these distinctions are in any case irrelevant for the purposes of this complaint, we subsequently assume that all statements made by Google LLC in any case (also) apply to data processing by Google LCC and always also refer to Google Analytics.

The obviously evasive and imprecise answer must arguably be taken into account in the context of the assessment of penalties (Article 83(2)(f) GDPR).

2. Question 1 and 2 - Questions about the Google Analytics product

noyb has nothing to add to this. Google LLC's statements are generic, do not relate to the specific case and are therefore undisputed.

3. Question 3 - Contract between netdoktor.at GmbH and Google LLC

3.1. General remark

Google LLC's answer to this question is conditional and not conclusive. Google LLC describes possible scenarios but does not answer

- whether netdoktor.at GmbH uses the free Google Analytics version or the paid version "Google Analytics 360";
- whether netdoktor.at GmbH has negotiated or attempted to negotiate the terms of the contract in relation to Google LLC;
- whether netdoktor.at GmbH has activated the "data sharing setting" and thus, in the opinion of Google LLC, there is (also) a data protection responsibility of Google LLC and/or Google Ireland Ltd.

If, in the opinion of the DSB, these questions are relevant to the decision, Google LLC and/or netdoktor.at GmbH should be ordered to answer them conclusively.

In particular, the question would arise as to how a controller using Google services can "consent" to the processing of data of data subjects merely by "activating data sharing". According to Article 6(1)(a) of the GDPR, the decision on the disclosure of user data (new processing purpose!) would probably primarily have to be obtained from the data subject - not from netdoktor.at GmbH. The fact that such consent would be required also follows from Article 6(4) GDPR due to the lack of purpose compatibility.

3.2. On the liability of Google companies in the event of a "data release"

Although this should not be relevant in any case, we would like to express our doubts about the responsibility model outlined by Google LLC when "data sharing" is activated. The statement "*(i) Google Ireland Limited is the controller for personal data relating to a data subject located in the European Economic Area or Switzerland, and (ii) Google LLC is the data controller for personal data relating to a data subject located in the UK*" is illogical and incomprehensible and raises a multitude of questions:

(1) To what extent should Google Ireland Ltd. determine the purposes and means of data processing (Article 4(7) GDPR) only because a user is located within the EEA/Switzerland? Google LLC describes the data collection itself as a global network which, purely from a technical point of view, addresses the geographically closest server and involves global downstream processing.

(2) What criteria does Google LLC or Google Ireland Ltd. use to determine the location of the data subjects - what does "*in the European Economic Area*" mean, for example? The IP address, for example, or the top-level domain of the website come into question. At the same time, Google LLC claims to anonymise the IP address immediately and not to use any other data itself.

(3) How do Google LLC or Google Ireland Ltd. recognise a change in the localisation of a data subject? How is a distinction made, for example, between the use of a VPN tunnel, a stopover on an international journey and a move? How does walking through St. Peter's Square in Rome, for example, which - as part of the Vatican - is not part of the EEA, affect the responsibility of the Google companies?

(4) In the event of such a change of location, on what legal basis is data transferred from Google LLC to Google Ireland Ltd. or in the other direction, and how is information provided in this case pursuant to Article 14 of the GDPR?

We would like to note that even a reliable localisation of a data subject should mostly require his or her identification and thus the processing of personal data.

As we understand it, Google LLC is always responsible for data processing in connection with globally offered Google services within the meaning of Article 4(7) of the GDPR, unless there is a delegated processing pursuant to Article 4(8) of the GDPR.

4. Question 4 - Settings of the website owner

4.1. General remark

noyb has no position on the design options in general, as this is also irrelevant for the decision on the complaint from our point of view. The DSB's questions seem to focus on a lack of responsibility of the website owner.

However, since Chapter V of the GDPR applies equally to controllers and processors and makes no distinction between these roles, the exact determination of the role in the context of the complaint seems irrelevant.

However, to the extent that this is helpful to the DSB, we would like to note the following:

4.2. Re. ii) - Anonymisation of IP addresses

With regard to the IP anonymisation option cited by Google LLC, we would like to note that, according to Google LLC's own information in the linked document "IP Anonymization (or IP masking) in Google Analytics", this only takes place after data transmission to and data collection by Google LLC:

> *"The IP anonymization/masking takes place as soon as data is received by Google Analytics, before any storage or processing takes place."*

Whether personal data is processed or permanently stored on a hard disk, an SSD, a RAM or any other storage medium is completely irrelevant for the applicability of the GDPR and in particular Article 44 *et seq.* of the GDPR. Other forms of communication (such as telephone calls, messaging or streams) are also technically "volatile" and do not lead to permanent storage. However, they still fall under the concept of processing according to Article 4(2) GDPR and thus all provisions of the GDPR.

Furthermore, it should be emphasised that Google LLC only talks about anonymisation in the "Analytics Collection Network". However, as is well known, Google operates countless services with countless purposes. Thus, even according to Google LLC, the anonymisation of the IP address does not affect the use of advertising services, cookies or processing within the framework of the Google Tag Manager for security purposes, but only the "Analytics Collection Network".

4.3. Re. iii) - The 105 sub-processors

Many of the 105 sub-processors listed by Google LLC via hyperlink are themselves likely to be considered "*electronic communication service providers*" or these sub-processors are based in third countries for which no adequacy decision of the European Commission exists (e.g. Brazil, Philippines, India).

As Article 44 GDPR clearly states, onward transfers by a third country to another third country must also comply with the conditions of Chapter V GDPR. Point 11.3(a)(i) of Attachment 3 (referred to by us as *New Contractual Data Processing Terms for Google Advertising Products*) only mentions standard contractual clauses according to point 10.2. of Attachment 3 in this context - i.e. standard contractual clauses between the website owner (netdoktor.at GmbH) as data exporter and Google LLC as data importer.

However, on which transfer mechanism according to Chapter V GDPR are data transfers to the mentioned sub-processors based if they are located in a third country?

4.4. Re. v) - Concrete data transfer

We want to note that Google LLC also completely ignores the question here and does not provide any concrete information whatsoever as to what specific data goes to Google LLC when using Google Services.

4.5. Re. vi) - Worldwide processing of all data

We note that Google LLC indisputably processes all the data subject to the complaint in any region of the world.

5. Question 5 - Instructions by the website owner

As already stated, a violation of the instructions to Google LLC as a processor seems irrelevant for the handling of the complaint, and is primarily a question concerning the internal relationship between netdoktor.at GmbH and Google LLC. At most, an additional illegality results.

Even if Google LLC does not receive or follow instructions and therefore becomes a controller itself under Article 28(10) GDPR, this has no relevance with regard to Chapter V GDPR - in any case, Google LLC qualifies as a US-based data importer.

However, if the DSB considers this to be relevant to the decision (in particular also with regard to the assessment of penalties), we suggest asking Google LLC how Google LLC would deal with the following instructions from a website owner (if necessary via instructions to Google Ireland Ltd.):

- Instruction to process personal data only in the EEA
- Instruction not to transfer personal data to (certain) sub-processors.

6. Question 6 - Targeted deletion of individual users possible

6.1. General remark

We welcome this very targeted question by the DSB, which in particular makes the personal nature of the relevant data indisputable.

6.2. Re. i) Cancellation by "segregation" possible

Google LLC clearly indicates that a data subject can be identified by a "user identifier" for the purpose of deletion. These are probably user identifier numbers such as those created in the current case in the "_ga", "_gid", "__gads" or "cid" cookies or values (see above, point B. 5.3). Thus, in any case, the possibility of identifiability within the meaning of Article 4(1) of the GDPR indisputably exists.

The same applies to the aforementioned deletion via the "User Explorer report"; it talks about the potential to "*isolate [...] individual user behaviour*" - it is therefore precisely the "singling out" of a natural person referred to in recital 26 of the GDPR, which leads to his or her identifiability within the meaning of Article 4(1) of the GDPR.

It should also be borne in mind that such a deletion request to Google LLC also inevitably results in a transfer of personal data that is subject to Chapter V of the GDPR.

Irrelevant to the complaint, but also disconcerting, is that the deletion of a website visitor's data from "Google Analytics servers" may only take place 2 months after the actual deletion request by the website owner - which in our view is not compatible with Article 28(3)(a) of the GDPR in conjunction with Article 5(1)(e) of the GDPR.

6.3. Re. ii) Use of "Google signals" left open

Google LLC leaves open whether netdoktor.at GmbH uses "Google signals" or not. However, since there are references to the use of Google DoubleClick (advertising) in the data of the specific website visit (see HAR file, Attachment 4) and the "__gads" cookie (Google Ads) was also set, a connection with the advertising products is at least probable.

6.4. Re. iii) Responsibility for measurement services

Google LLC leaves open whether netdoktor.at GmbH has activated "data sharing" (see above point C. 3.1.).

The information on further processing for own purposes conflicts with the information provided by Google LLC, according to which data is anonymised or pseudonymised, or cannot be assigned to a user by Google LLC. The following questions arise in this context:

- Why does Google LLC assume that Google Ireland Ltd. is responsible for "personal data" if this data cannot be attributed?
- How will Google LLC and Google Ireland Ltd. determine whether a data subject is present in the EEA if they are supposedly unable to identify him or her?

Regarding the alleged responsibility of Google Ireland, which we doubt in any case, we refer to our comments at point C. 3.2.

7. Question 7 and 8 - Transfer of data to the USA

We would like to note that Google LLC itself clearly states that all data processed in connection with Google Analytics is always also transmitted to the USA:

> *"All data collected through Google Analytics (see our response to question #2) is hosted (i.e. stored and further processed) in the USA."*

The transfer of data to the USA is thus undisputed in any case.

The extent to which data has passed through a specific "collector" in an individual case and whether the complainant's data is also stored in the countries in which Google LLC or its 105 subcontracted data processors maintain a data centre is therefore ultimately irrelevant. Onward transfers to other third countries can at best increase the extent of the violations of Articles 44 *et seq.* of the GDPR attributable to Google LLC, but not reduce them (see already above, point C. 4.3).

8. Question 9 - Linking to the complainant's Google account

8.1. General remark

Google LLC again answered the DSB's question evasively and incorrectly by first stating that "*as such*" the use of Google Analytics does not require disclosure, but then admitting that the data can be transferred.

However, once again, the personal nature of the data is in any case undisputed and conclusively proven (see above, point B. 5.3) and thus an additional link to a data subject via the Google account is irrelevant for the complaint proceedings in the complainant's view. However, out of procedural caution, we take the following position:

8.2. On the dissemination of data

Google LLC obviously uses the word "*receive*" here with the intention of gross deception. Google LLC states that it would only "receive" information about the specific Google user if -the person concerned had made certain settings.

Rather, Google LLC seems to "receive" the data (and thus "process" it according to Article 4(2) of the GDPR), but states that it will not further use it for certain purposes if certain settings have been made. However, Google LLC does not provide any proof or technical details on the alleged limited use, it only provides a screenshot of the setting.

In any event, the complainant therefore **disputes** that Google LLC does not "receive" and thus "process" these personal data within the meaning of Article 4(2) of the GDPR.

8.3. On the settings in the complainant's Google Account

Google LLC does not explain in any way why the four conditions should be essential for Google LLC to receive the information that a certain user has visited a certain website. Unless the DSB already assumes that the transferred data is personally identifiable in light of the explanations under point B. 5.3, we suggest that Google LLC be asked to explain and demonstrate the actual relevance of these conditions.

Specifically, it is no longer possible for the complainant to reconstruct which data protection settings he had selected in his Google account on the day of the website visit (14.08.2020). Since then, the complainant has repeatedly deleted his history in the browser "Firefox" and has consequently been confronted again and again with the consent banner used by Google LLC. It is likely that the complainant has repeatedly consented to this procedure (exasperated).

It should also be noted that Google LLC is to be considered the accountable controller with regard to the settings in the complainant's Google Account.

Despite the accountability obligation pursuant to Articles 5(2) and 7(1) of the GDPR, Google LLC does not claim that the data subject had activated or deactivated certain settings at the relevant time. Until proven otherwise, it must therefore be assumed that the Google account data was transferred and processed, which results in additional processing of personal data within the meaning of Article 4(1) and (2) of the GDPR.

9. Question 10 to 12 - Different website visit scenarios

In our view, Google LLC's responses are in principle irrelevant to the present complaint, as the complainant was logged into his Google account in the same browser (Firefox) at the relevant time.

However, if this is helpful for the DSB, we would like to point out the following: Here, too, Google LLC (likely knowingly) confuses the question, which asks about the pure abstract possibility (!) of linking, with the, according to Google LLC non-existence of, internal linking. Google LLC fails to provide any proof of the alleged non-existence of linking.

10. Question 13 - User identification numbers used and linkage

In its answer to question 13, Google LLC openly admits that the user identification numbers listed above under point B0(in particular also "_ga", "_gid") contain a unique user ID. This is thus undisputed in any case.

Even if this is irrelevant for the assessment of the complaint, the following sentence in the English original of Google LLC's statement is worth highlighting in a whole series of points:

> *"As a general matter, unless instructed to do so, Google does not attempt to link data it collects as a processor on behalf of website owners using Google Analytics with data it collects as a controller in relation to its users and the relevant policies and systems are designed to avoid such linking."*

This simply means that Google LLC, at the instruction (presumably of the website owner), also links this personal data with other data that Google LLC (or another Google company) obtains from other products, in particular this appears to apply to advertising products.

Even if there is no such instruction, the phrases "*as a general matter*", "*does not attempt*" and "*designed to avoid*" allow a virtually limitless scope:

- Firstly, Google LLC implicitly describes itself as being able and willing to link the data anyway, contrary to the general rule.
- Secondly, Google LLC acknowledges that the attempt to avoid linkage may fail.
- Thirdly, Google LLC suggests that there are cases where, in Google LLC's view, it is unavoidable to establish such a link.

11. Question 14 - Raw data collection

Again, Google LLC seems to simply ignore the DSB's question. However, a response to the question does not seem necessary with regard to the complaint.

12. Question 15 - Data use

Once again, Google LLC seems to ignore the DSB's question. However, a response to the question does not seem necessary in view of the complaint.

13. Question 16 - Do not Track (DNT)

The answer seems irrelevant for the decision on the complaint.

However, if this is helpful for the DSB, we would like to clarify that Google LLC does not inherently support the "DNT" standard in the context of Google Analytics. In a roundabout way (e.g. a "Consent Management Platform"), a website owner can set its systems in such a way that the Google Analytics code on its website is not included if the website receives a "DNT" signal from a user. However, this requires additional software that "builds in" or "builds out" Google Analytics on the website depending on the DNT status.

14. Question 17 - Consent to cookies

Again, Google LLC seems to be evasive in answering the DSB's question.

However, it does not seem necessary to answer the question with regard to the complaint, as the transfer to the USA according to Chapter V of the GDPR is independent of the question of consent according to Article 5(3) of the ePrivacy Directive, Section 96(3) of the TKG and Article 6(1) of the GDPR, respectively.

If this is nevertheless considered relevant by the DSB, we would like to point out that, to our knowledge, consent is regularly obtained via a "cookie banner" in accordance with Article 5(3) of the ePrivacy Directive and Section 96(3) of the TKG 2003, which then controls the integration of the Google Analytics code.

In the case of netdoktor.at GmbH, OneTrust LLC is used (as a "consent management platform"), which itself sets cookies and processes personal data partly under access pursuant to 50 USC §1881a. However, this is not the subject of the complaint.

15. Question 18 - "Necessary" use by Google LLC

The answer to this question also does not seem relevant for the decision on the complaint, since the complainant primarily objected to the transfer of his personal data to the US.

Whether Google LLC may also process personal data already unlawfully transferred as a controller for the purpose of "protecting the Analytics service" will in all likelihood boil down to the question of whether there is effective consent of data subjects or a legitimate interest of Google LLC. To the extent that additional data is transferred out of the EEA to Google LLC in the US for the purpose of "protecting the Analytics service", an effective "controller to controller" transfer mechanism would again be required.

In any case, it should be noted again that Google LLC leaves it open (i) whether netdoktor.at GmbH has activated "data sharing" for other purposes, (ii) to what extent personal data (such as the IP address) are still used before anonymisation, for example for security purposes, and (iii) how a division of responsibility under data protection law between Google LLC and Google Ireland Ltd. is objectively justified depending on the location of the data subjects.

16. Question 19 - Transfer from Google Ireland Ltd. to Google LLC

The response of Google LLC is relevant insofar as it clarifies that Google LLC is always the final (sub)processor, even if the Google group now argues that Google Ireland Ltd. will be "inserted" as a contractual partner of the website owner and processor as of May 2021. Since Chapter V of the GDPR does not distinguish between controllers and various processors, it is thus undisputed that Google LLC processes the complainant's personal data at all times and in all cases, contrary to the provisions of Chapter V of the GDPR.

17. Question 20 - Disclosure to authorities

In essence, Google LLC admits that Google Ireland Ltd. also complies with third country data requests - which are sometimes not enforceable in the EEA - contrary to Article 48 GDPR. In particular, it is worth highlighting that Google Ireland Ltd does not highlight the need for a mutual legal assistance agreement, which could arguably be sanctioned by the Irish DPC.

However, since the complaint relates to access via Google LLC, and data processing by Google Ireland Ltd. is not the subject of the complaint, this answer seems irrelevant for the decision on the complaint.

18. Question 21 – Purposes and means

noyb has nothing to contribute on this. The DSB's question seems to be aimed at the roles of Google LLC and Google Ireland Ltd. in determining purposes and means.

Since Chapter V of the GDPR applies equally to controllers and processors and makes no distinction between these roles, the exact determination of the roles in the context of the complaint seems irrelevant.

19. Question 22 - Applicability of Privacy Shield

Google LLC's response disputes the following:

- In any case, between 16.7.2020 and 12.8.2020, the data transfer to the USA takes place without an effective transfer mechanism, as the Privacy Shield decision had been revoked and Google LLC had not yet concluded standard contractual clauses with customers of Google Analytics (or other Google services).

  Google LLC hereby admitted that it had openly ignored the provisions of Chapter V of the GDPR for a good month before the complainant's visit and irrespective of legal violations after 12.8.2020 - despite the knowledge of the impending judgement. This is also punishable by a fine under Article 83 of the GDPR.

- Google LLC now uses the standard contractual clauses in the Annex to Decision 2010/87/EU.
- The standard contractual clauses have been concluded between netdoktor.at GmbH and Google LLC, making processing by various "intermediaries" irrelevant.

We have nothing to add to the statements of Google LLC in this respect.

20. Question 23 to 26 - Effect of standard contractual clauses

From the standard contractual clauses used by Google LLC and netdoktor.at GmbH it follows in particular that:

- Google LLC had a duty under clause 5(b) to notify netdoktor.at GmbH of US surveillance practices, in particular under 50 USC § 1881a, but apparently failed to do so.
- Google LLC has accepted the jurisdiction of the DSB in clause 8, in particular the right of the DSB to apply its powers under Article 58 GDPR also to Google LLC in the US.
- That Austrian law is applicable to the standard contractual clauses between Google LLC and netdoktor.at GmbH.

21. Question 27 - Review of US legislation

The length of Google LLC's response to this question is likely to correlate with the length of Google LLC's review. The audacity of this one-word answer should probably also be considered in the context of the penalty assessment.

22. Question 28 - Additional measures

22.1. General remark

In its opinion, Google LLC essentially relies on a five-page undifferentiated list of alleged "additional measures" within the meaning of paragraph 133 of the judgment C311/18 to "immunise" data transfers based on standard contractual clauses pursuant to Article 46(2)(c) of the GDPR against 50 USC § 1881a (also known as "FISA 702") - i.e. to ensure compliance with the level of data protection required under EU law. Unfortunately, this is structurally impossible.

On the points criticised by the CJEU (in particular, no specific legal basis for the monitoring and lack of legal protection), the "measures" put forward by Google LLC are completely irrelevant. Many are purely standard procedures that are obligatory under the GDPR anyway. If the US government's intelligence services were to be thwarted by a few legal or technical tricks, they would hardly be able to fulfil their surveillance mandate.

In addition, Google LLC, in its role as data importer, has the burden of proving the actual application and effectiveness of these "additional measures" with respect to requests under 50 USC § 1881a. Google LLC would have to explain specifically how certain measures can actually remedy the deficiencies identified by the CJEU, but leaves this completely open, listing only generic "measures". Moreover, some measures are obviously relevant for completely different scenarios (e.g. intrusion into data centres), which is why it cannot generally be assumed that Google LLC has actually specified concrete measures to thwart surveillance under 50 USC § 1881a here.

We would also like to point out that the CJEU has now already -confirmed the violation of EU fundamental rights (in particular Articles 7, 8 and 47 of the EU Charter of Fundamental Rights) by 50 USC § 1881a in two judgments (C362/14 -and C311/18) and that there is thus a supreme court clarification on the -relevant points which makes a decision simply possible. Even if Google LLC

speaks (in a way that in the end must unfortunately be described as arrogant) of a "*view on these laws*" of the highest European court, Google LLC will ultimately have to submit to this view.

The fact that Google LLC, in the face of this clear case law, is presenting a sham solution to the authorities and European customers is outrageous and must be taken into account as intentional deception in the context of the assessment of penalties under Article 83(2) of the GDPR.

22.2. Relevant CJEU case law

In particular, the CJEU found the following elements of the US legislation in C311/18 to be incompatible with European fundamental rights under Articles 7, 8 and 47 of the EU Charter of Fundamental Rights (CFR) (paragraphs 184 and 198):

- The lack of any legal protection before US courts under Article 47 of the Charter (see in particular paragraphs 183 and 197).
- The lack of any precise legal basis for supervision, which defines the scope and extent of the interference with fundamental rights itself and satisfies the requirement of proportionality (see paragraphs 175, 176, 180 and 183).
- The lack of any individual *ex ante* decision by a court, but the sole review of a monitoring system as a whole (paragraph 179) and the lack of any redress mechanism (paragraphs 187, 191 and 192).
- The lack of any legal protection for "non-US persons" (paragraph 180).

Since "additional measures" would have to overcome these problems, it is completely incomprehensible (or at most explainable with a denial of reality) how Google LLC can use "fences" or "signs" around its data centers as a reasonable argument in view of this situation. 50 USC § 1881a will hardly be impressed by a sign.

22.3. Relevant US law

In order to ensure that the DSB has all the necessary information at their disposal, we have tried to summarise the sometimes very complex US law in a concise manner. We are always available for further questions, but we believe that all relevant information is available and even undisputed in the context of the complaint.

22.4. EO 12.333 - Decree of the US President

Google LLC states that the data subject's data is processed on servers all over the world. It is correct that EO 12.333 is thus also[4] applicable for servers outside the USA.

[4] https://www.archives.gov/federal-register/codification/executive-order/12333.html (accessed 04.05.2021).

Sometimes unimaginable for European lawyers, this is a possibility for the US president to direct the activities of the US authorities by means of informal "decrees" (similar to an instruction), which arises directly from Article 2 of the US Constitution. Insofar as no law contradicts this, the president has a free hand. To put it simply, one can speak of a kind of "reverse legality principle": Provided there is no specific legal prohibition, the US president is free to issue these "decrees" - he does not need any specific legal authorisation.

Accordingly, Section 2.3 of EO 12.333 contains a restriction on the processing of information on US citizens (to comply with the 4th Amendment). However, EO 12.333 does not provide for any restriction on the "*collection, retention and dissemination*" of data on foreign nationals, which is thus allowed *e contrario* in any case.

Finally, Section 3.5 of EO 12.333 states that the Executive Order does not grant any rights to third parties. At the same time, an EO cannot be used to impose coercive measures on third parties (such as Google LLC), which is undisputed ("*nor does it impose requriements on service providers*").

With regard to the complaint, the following applies:

(1) Since Google LLC states that the data of data subjects are also stored and transmitted on servers outside the USA, EO 12.333 contains here in principle the possibility of extra-legal access to servers outside the USA.
(2) The tapping of data in the context of international data transfers to Google LLC (e.g. via "submarine cables", "internet nodes" other providers of the "backbone") also falls within the scope of EO 12.333.
(3) However, because EO 12.333 does not require Google LLC to comply directly, Google LLC may also refuse requests from US authorities under EO 12.333.

It should be emphasised that Google LCC does not explicitly exclude the transfer of data in accordance with EO 12.333, although this would be easy to clarify.

22.5. 50 USC § 1881a (also "Section 702" or "FISA 702")

Unlike EO 12.333, 50 USC § 1881a[5] is a statute that imposes a duty to cooperate directly and extensively in the large-scale surveillance of persons outside the United States by "electronic communication service providers" in the United States.

The law is characterised by a number of elements that are rather unimaginable in European law, all of which are designed for a completely generic authorisation of surveillance systems such as "PRISM" or "Upstream", as well as for a generic assistance of companies in these surveillance systems. As the CJEU stated in paragraph 179 of the judgment C-311/18, there is no authorisation of an individual surveillance measure and no verification of the selection of a target.

[5] https://www.law.cornell.edu/uscode/text/50/1881a (accessed 04.05.2021).

In detail:

- The target of surveillance is solely information ("*foreign intelligence information*"), i.e. not a specific person or entity. This information is defined very broadly in 50 USC § 1881(a), which makes it very difficult to combat a surveillance measure.
- Under 50 USC § 1881a, any "electronic communication provider" can potentially be required to assist in the acquisition of such information under 50 USC § 1881(b)(4). It is undisputed that Google LLC will be required to do so - Google LLC's own transparency report for 2019 mentions a full 202,500 user accounts affected by data requests under FISA 702. [6]
- 50 USC § 1881a (i) only recognises a general notice ("*Directive*") that requires
  (A) "*provide all information, facilities, or assistance*" - in other words, a very broad action,
  (B) in order to "*accomplish the acquisition*" of data rather than specific data.
  This already structurally excludes a case-by-case examination of the surveillance of the complainant or any other person concerned.
- Google LLC could challenge the entire "Directive" (see 50 USC § 1881a (i)(4)). However, there is no evident legal basis for a successful challenge, since 50 USC § 1881a legalises exactly the said surveillance under US law, which is classified by the CJEU as contrary to fundamental rights. Accordingly, Google LLC cannot take any successful legal action.
- If the entire challenge does not succeed, Google LLC must, in order to comply with US law, adapt all data, keys or technical precautions in such a way that the US government can obtain the data. In the context of "PRISM" (or now "Upstream"), this is probably done via an automatic interface set up by the FBI's "Direct Interception Unit" (FBI-DIU).
- The only limit to this assistance under US law is of a factual nature and lies with the information that Google LLC does not have in available, i.e. is not under the control of Google LLC ("*possession, custody or control*").

As a concrete example, one can vividly imagine "Room 641A"[7], where (before 50 USC § 1881a was codified) AT&T was extralegally required to install a secret "listening room" where the international data transfer was copied, scanned and processed in its entirety. The programme now continues as "Upstream" under 50 USC § 1881a and EO 12.333.

It is evident that no legally and technically knowledgeable employee of AT&T was allowed to sit in that room and review individual US government requirements, and no physical safeguards of the building helped against US government surveillance, as it was a legal coercive measure under US law.

[6] https://transparencyreport.google.com/user-data/us-national-security?hl=de; the number of 202,500 total user accounts concerned is obtained by adding the minimum values indicated in the column "Number of accounts" concerning the year 2019, both under "Requests for metadata [...] " and "Requests for content data [...]" (30,000+28,500+74,500+69,500=202,500) (accessed 04.05.2021).
[7] https://en.wikipedia.org/wiki/Room_641A (accessed 04.05.2021).

22.6. Legal measures by Google LLC

Specifically, Google LLC mentions practically only organisational measures; with good will, the following measures can be interpreted as legal measures:

- **Review of requests** ("*review each request*")

  The verification of requests by authorities is not an "additional measure" but an absolute minimum standard. Disclosure without a specific legal basis would at least violate Articles 5, 6(1) and 48 of the GDPR. The existence of valid requests under US law is also undisputed.

- **Attempt to limit requests** ("*attempt to have [requests] narrowed*")

  The mere attempt is of course laudable, but cannot stop structural mass surveillance, as the request (i.e. the "Directive") is already unlimited under 50 USC § 1881a(i) and covers any kind of information.

- **Objection in some cases** ("*in some cases we object to producing any information*")

  Google LLC does not indicate whether these cases relate to 50 USC § 1881a and EO 12.333. If this is the case, these appeals were unsuccessful, as Google LLC itself claims to have complied with queries under 50 USC § 1881a concerning at least 202,500 user accounts in 2019 alone.

In sum, Google LLC has not put forward any relevant measures at all with respect to 50 USC § 1881a.

With regard to EO 12.333, it is worth noting that Google LLC does not mention the most obvious legal "measure": non-compliance with unenforceable requests (such as those under EO 12.333). Instead, Google LLC speaks of "some cases" in which no data is disclosed. It can thus be assumed that Google LLC even discloses data pursuant to EO 12.333 and that there is no relevant measure here either.

22.7. Organisational measures of Google LLC

As "organisational measures" Google LLC primarily mentions information:

- **Inform the customer** *("notify the customer")*

  In principle, informing the customer (i.e. netdoktor.at GmbH) is irrelevant if the data of a data subject (such as the complainant) are processed. Furthermore, informing the data subject is in principle already explicitly and without time limit prohibited under 50 USC § 1881a(i)(1)(B) or by relevant laws under EO 12.333 ("*gag order*"). Google LLC does present the case of a prohibition as an exception, but since it is the statutory rule in the USA, this measure is also irrelevant.

- **Transparency report and policy** ("*policy on handling government requests"*)

  The fact that Google LLC also calls the information about the disclosure of customer data concerning at least 202,500 user accounts an "additional measure" has a certain audacity. Just because a breach of the law is loudly announced does not make it more legal.

It should also be pointed out that Google LLC itself admits that it does not release all information ("*as much information as legally permissible*"). What information is missing is unknown. In any case, Google LLC has not yet made any data available at all for 2020, although the official evaluation period of six months for the first half of 2020 has now been over five months. The latest data is 17 months old. [8]

For 2018 to 2019, the report shows an increase in data searches under 50 USC § 1881a ("FISA") of almost 25% which also argues against the existence of effective "additional measures".

Neither "measure" can limit the access of US authorities and the applicability of 50 USC § 1881a and EO 12.333 to the slightest extent and are therefore irrelevant.

22.8. Technical measures by Google LLC

More relevant under US law are technical measures, as external monitoring by the US government in the context of monitoring the internet backbone can thus be ruled out or at least made more complicated.

- "*protection of data in transit*"

  Technical measures (especially encryption) can sometimes provide a remedy against monitoring by third parties during transmission ("in transit").

  However, not transmitting data in plain text is not an "additional measure" but an absolute minimum standard that the controller and the data subject must ensure under Article 32(1)(a) GDPR.

  It should be noted here that Google LLC specifies conventional encryption methods (HTTPS and TLS), which are considered secure but can very likely be overcome by services such as the NSA. The protection here is limited and does not go beyond the security of a normal visit to https://news.ORF.at/, for example.

  It should also be noted that technically only a certain part of the data ("payload") can be encrypted. However, the address data on the "envelope" of a data packet (e.g. the IP address of the sender and recipient of a data packet) are necessarily openly visible - otherwise the data packet could often not find its destination. Open metadata can still be used to identify communication patterns (see CJEU in C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* on data retention) and to intercept relevant data packets despite encryption of the content.

  In addition, these measures are only relevant if the access by the US authorities takes place outside Google LLC (e.g. at an international network node). The measures are completely

[8] See https://transparencyreport.google.com/user-data/us-national-security?hl=de (accessed 04.05.2021).

irrelevant in the case of direct access (admitted by Google LLC itself) by US authorities. Here, Google LLC must make data or the relevant keys available to the NSA at any time in accordance with 50 USC § 1881a; encryption is thus immediately circumvented.

- "*protection of data at rest*"

  The protections to stored data put forward by Google LLC completely miss the point: CJEU jurisprudence and the complainant are not concerned that the US government secretly or with a sledgehammer enters data centres against the physical resistance of Google LLC and snatches a hard drive from the server, but that (legally under US law) US government notices force Google LLC to provide data.

  In this respect, neither the normal AES encryption of hard disks (which, incidentally, is also used on every Android smartphone) nor six security zones around the data centre are relevant. The US government is known to walk in through the front entrance at Google LLC with a notice - which legally binds Google LLC to allow access to data despite all these precautions.

Encryption during transmission using standard procedures (HTTPS and TSL) can at least make work more difficult for the US government in the case of external monitoring (for example at the internet backbone under EO 12.333 or 50 USC § 1881a). However, the security measures put forward are all irrelevant in the case of direct access via a "directive" under 50 USC § 1881a(i), which is relevant to the complaint and which the CJEU ruled to be contrary to fundamental rights, or in the case of cooperation between Google LLC and the US government under EO 12.333.

Google LLC does not mention a single measure that would lead to the end of *de facto* access by Google LLC to data and/or keys (termination of "*possession, custody or control*"), which is currently the only known case in which Google LLC does not have to answer a request by the US government. Concepts for this (e.g. outsourcing of processing to third parties who are not subject to instructions and who are *de facto* deprived of access by US authorities) exist, but are neither applied nor even argued by Google LLC.

In summary, Google LLC's submission on technical measures is at best an argumentative "smoke grenade", but more likely an attempt to deliberately deceive the DSB.

22.9. Alleged pseudonymity and optional technical measures

Finally, Google LLC argues that the data in Google Analytics are "pseudonymous". Even if this argument were correct, it would have no relevance under Chapter V of the GDPR, as pseudonyms are also personal data in any case. However, for the avoidance of doubt, in detail:

- **Google Analytics Terms of Service**

  The alleged contractual provision prohibiting the transfer of personal data to Google LLC was, as explained under point B5.2. and B. 5.3arguably not complied with by netdoktor.at GmbH and Google LLC and is therefore also irrelevant in the context of the present complaint.

  Google LLC itself admits in the small print[9] that it uses a different definition ("*personally identifiable information*"), which is not in line with "personal data" according to Article 4(1) of the GDPR. So here too, Google LLC is obviously engaging in a brazen deception of the DSB.

- **First Party Cookies**

  As already explained above, the "_ga", "_gat", "cis" and "__gads" values are obviously personal and even represent a standard case of an "online identifier" in the sense of Recital 30. Here, too, there is probably no "additional measure" - otherwise the entire online advertising system, which is based on massive surveillance of all internet users, would probably qualify as an "additional measure".

- **IP addresses**

  The fact that IP addresses are personal data has already been dealt with by the CJEU (see C-582/14) and is indisputable, in particular due to the clarification in Article 4(1) of the GDPR and Recital 30 of the GDPR. Google LLC's arguments to the contrary once again demonstrate its ignorance of European law.

  Google LCC's argument, however, becomes definitively grotesque when one notes that on the relevant page of the Transparency Report, Google LLC itself cites IP addresses as a typical identifier used by the US government for data requests ("*FISA requests may involve metadata such as the 'From' and 'To' fields in email headers, or the IP addresses associated with a particular account*"). / "*A FISA request can include non-content metadata - for example, ... the IP addresses associated with a particular account.* ”). [10]

  Google LLC also has records of almost every IP address in the world through its almost unavoidable presence on the Internet (from search to YouTube to various services that are built into third-party sites). The claim that such information is only available from the respective internet service providers (ISPs) is, especially in the case of players like Google LLC and the US government, completely unworldly and probably deliberately incorrect.

  For the optional anonymisation of IP addresses in the present case and its irrelevance with regard to the applicability of Articles 44 *et seq.* of the GDPR, see above under point C. 4.2.

  IP addresses are the "telephone numbers of the internet". Their supposed pseudonymity is therefore in no way a type of "additional measure" that would make the transfer of data to the

[9] https://support.google.com/analytics/answer/7686480?hl=de (accessed 04.05.2021).
[10] https://transparencyreport.google.com/user-data/us-national-security?hl=de (accessed 04.05.2021).

US legal despite the applicability of 50 USC § 1881a and EO 12.333. If one followed the logic of Google LLC, any online data transfer using IP addresses would be considered an "additional measure".

22.10. Summary

In summary, Google LLC is deliberately trying to deceive the DSB with five pages of attempts to sidetrack it and irrelevant argumentative "smoke grenades".

None of the alleged "additional measures" go beyond the normal standard of data processing under Article 32 GDPR or have relevance with regard to US government data access under 50 USC § 1881a and/or EO 12.333.

The processing by Google LLC falls precisely under **use case 6** "*Transfer to cloud service providers or other processors requiring access to unencrypted data*" in paragraph 88 of the EDPB's **Recommendations 01/2020,**[11] where the EDPB notes that

> *"the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.*"

The other measures (Google LLC cites 112, 99, 129, 122, 79, 84, 131, 135, and 80, for example) may have some relevance in the case of certain foreign laws, but in the case of 50 USC § 1881a and EO 12.333, they are not even a blunt sword, but mostly taken completely out of context of the recommendation.

That the alleged "additional measures" are of little use can also be easily seen from the fact that even according to the figures published by Google LLC itself. From 2018 to 2019 alone, data queries increased by almost 25% from 162,500 to 202,500.

This may be inconvenient for Google LLC, but in light of two CJEU rulings (C362/14 -and C-311/18) on US law, the clear rule in Chapter V and Article 48 of the GDPR, Articles 7, 8 and 47 of the Charter and the EDPB Recommendation, it is the inevitable outcome.

23. Question 29 - Actual protection of the "additional measures"

As the comments to question 28 show, Google LLC has probably at no point seriously attempted to evaluate the actual protective effect of the "additional measures".

---

11 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 04.05.2021).

24. Question 30 - Use of Article 49(1) GDPR

As Google LLC correctly states, the complainant is also not aware of any use of Article 49(1) GDPR by netdoktor.at GmbH. Much more, all possibilities under Article 49(1) GDPR are obviously not applicable in this case.

25. Question 31 - Notification of the supervisory authority

The apparent lack of exchange with the supervisory authorities must also be taken into account in the context of the assessment of penalties under Article 83(2) of the GDPR.