Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

650 253-0000 main
Google.com

April 9, 20201

Österreichische Datenschutzbehörde
Barichgasse 40-42
1030 Wien

to: [redacted]

Dear [redacted]

I make reference to your email and letter dated February 26, 2021.

Please find the answers to your questions attached.

In your letter you make reference to a complaint by the complainant MB, who is represented by NOYB – European Center for Digital Rights, against the netdoktor.at GmbH and Google LLC. You also note that NOYB has lodged several similar complaints with other European Data Protection Authorities and that you therefore intend to communicate our responses to the other European Data Protection Authorities concerned with those complaints under Article 57 (1) (g) GDPR.

We did an analysis of the 50 redacted complaints published by NOYB. These complaints were filed with 13 European Data Protection Authorities and are directed against 50 entities (49 companies in 24 EU member states and in the UK and one university in Ireland) using Google Analytics on their websites in their capacity as controllers. Each complaint is also directed against Google LLC as processor. We found that the complaints are largely identical in their content. All complaints focus on a transfer of personal data to the United States and ask for a ban or suspension of relevant data flows to Google LLC in the United States.

Against this backdrop, we welcome your efforts to cooperate among the European Data Protection Authorities concerned to ensure the consistency of application of the GDPR. In accordance with that, your questions (as well as very similar questions we have received from the French CNIL and the Belgian GBA) are not limited to specific complaints but relate to how Google Analytics generally works and operates. We have therefore focussed our responses to your questions to information that we believe to be relevant for all of the complaints including the one that you refer to in your letter.

Regarding the table that was attached to your letter, we would like to note that the website owners who use Google Analytics, including the entities subject to the complaints, cover a wide range of industries and fields. As set out in our responses, Google Analytics is highly customizable and can therefore be implemented in many different ways, which leads to a wide spectrum of data that individual website owners can choose to collect. Additionally, as explained in our responses, it is the website owners that determine the purposes for

which they collect the data, the recipients of the data, its retention and other details mentioned in the table. As a consequence, we are unable to fill out the information requested in the table in a way that would be relevant for how Google Analytics generally works and operates. However, we believe that our answers to your questions as well as the resources we have linked to throughout our responses provide such information.

We hope that the responses we provide in the attached are helpful and we would be happy to provide any additional information that may be required.

Best regards,

Google Legal
Google LLC

Questions and answers

We would like to provide the following context to support the responses we have given to the below questions.

Throughout the document, we have referred to the applicable Google Analytics[1] customer (such as the netdoktor.at GmbH) as the "website owner" and visitors to the websites (such as the complainant) as the "user".

Website owners can choose between a free and a payable version of Google Analytics. Up until end of April 2021 Google offers Google Analytics under either (a) the Google Analytics Terms of Service with Google LLC, for customers of the free version (which, according to our records, is used by netdoktor.at GmbH) or (b) a Google Analytics 360 Order Form with Google Ireland Limited, for customers of the enterprise-level, paid version (both, as applicable, the "GA Terms"). In either case, the GA Terms incorporate the Google Ads Data Processing Terms ("DPTs"). From the end of April 2021 the GA Terms for both the free and the payable version are offered by the Google Ireland Limited and website owners who had previously contracted with Google LLC migrate to the Google Ireland Limited. See here a list of all language versions of both: (a) the Google Analytics Terms of Service with Google LLC, and (b) the Google Analytics Terms of Service with Google Ireland Limited.

In all cases, website owners contract with the Google LLC under the Standard Contractual Clauses pursuant to Commission Decision 2010/87/EU ("SCCs") (see our response to question #22 below).

We have attempted in our responses below to cover scenarios where either Google LLC or Google Ireland Limited provide the Google Analytics service, and we refer to Google LLC and Google Ireland Limited collectively as "Google" unless the distinction between the entities is relevant.

We should also point out that Google recently released the next generation of Google Analytics, known as Google Analytics 4, which offers a new kind of property with somewhat different reports than are available under the historical Universal Analytics version of the product. For the purposes of the responses below, the distinction between the various kinds of Google Analytics properties is largely irrelevant. We have therefore referred to all types generically as "Google Analytics", unless the distinction is clearly relevant. Additionally, website owners have the ability to use Google Analytics in combination with other products and services. We have focussed our responses on the features of a Google Analytics standard implementation without such combinations.

[1] Our responses are for the service Google Analytics. Should information on other Google services be required, we would like to ask for a specification of those additional services.

1. Please describe why you have decided to develop Google Services tools (including Google Analytics) and provide owners of the website with the possibility to implement Google Services tools (including Google Analytics tool) in a specific website.

Google Analytics is a measurement service that allows customers to measure traffic to their properties, including website owners who wish to measure traffic to their websites. Web analytics services are a popular category of service offered by multiple providers and are considered an essential tool for operating a website.

Website owners depend on web analytics services such as Google Analytics to help them understand how their users interact with their site and services. Google Analytics helps them create more engaging content and to monitor and maintain the stability of their websites. Without Google Analytics, website owners may be unaware of major issues with their website that could severely impact their services. For example, Google Analytics enables website owners to create custom alerts that notify them when certain trigger events take place (e.g. a spike in traffic or when there is no traffic at all). As another example, website owners can set up dashboards that give overviews of reports and metrics that customers most care about, such as monitoring in real-time the number of visitors on a site. Google Analytics may also help website owners measure and optimise the effectiveness of the ad campaigns they run on Google ads services.

2. Please describe how owners of a website can implement the Google Services (including Google Analytics tool) in a specific website.

How Does Google Analytics Collect Data?

Before describing how website owners can implement Google Analytics into their websites, we think it would be helpful to explain how Google Analytics collects data:

Similar to many other web analytics services, Google Analytics works by the inclusion of a block of JavaScript code on pages in a website. When users of a website view a page, this JavaScript code references a JavaScript file that was previously downloaded to the user's device, which then executes the tracking operation for Google Analytics. The tracking operation retrieves data about the page request through various means and sends this information to the Analytics server via a list of parameters attached to a single-pixel GIF image request.

The data that Google Analytics collects on behalf of the website owner comes from these sources:

- The HTTP request of the user
- Browser/system information
- First-party cookies

A HTTP request for any webpage contains details about the browser and the computer making the request, such as the hostname, the browser type, referrer, and language. In addition, the DOM of most browsers provides access to more detailed browser and system information, such as Java and Flash support and screen resolution. Google Analytics leverages this information. Analytics also sets and reads first-party

cookies on a users' browsers enabling the measurement of user session and other information from the page request (the usage of Google Analytics cookies is described here).

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

> https://www.google-analytics.com/__utm.gif?utmwv=4&utmn=769876874&utmhn=example.com&utmcs=ISO-8859-1&utmsr=1280x1024&utmsc=32-bit&utmul=en-us&utmje=1&utmfl=9.0%20%20r115&utmcn=1&utmdt=GATC012%20setting%20variables&utmhid=2059107202&utmr=0&utmp=/auto/GATC012.html?utm_source=www.gatc012.org&utm_campaign=campaign+gatc012&utm_term=keywords+gatc012&utm_content=content+gatc012&utm_medium=medium+gatc012&utmac=UA-30138-1&utmcc=__utma%3D97315849.1774621898.1207701397.1207701397.1207701397.1%3B...

Additional information on how data is collected with Google Analytics can be found here.

How to implement Google Analytics into a website

At a high level, website owners need to complete the following basic steps in order to implement Google Analytics on a website:

1. **Create or sign in to a Google Analytics account at google.com/analytics**
2. **Set up a property in their Analytics account.** - A property is the collection point in Google Analytics for the data. For example, a website owner might create a property to collect data about a particular site.
3. **Set up a reporting view in the property.** - Reporting views let the website owner create filtered perspectives of the collected data; for example, creating a report view filter that excludes all internal traffic (such as traffic from the website owner's intranet).
4. **Add the tracking code to the website** so that data can be collected into the Analytics property, by embedding a global site tag right after the opening <head> tag on each webpage that the website owner wants to measure.

The global site tag is the above mentioned block of JavaScript code that allows website owners to have event data sent to Google Analytics. That tag can look as follows:

```
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async
src="https://www.googletagmanager.com/gtag/js?id=GA_MEASUREMENT_ID"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag( js , new Date());
```

```
    gtag( config ,  GA_MEASUREMENT_ID );
  </script>
```

In the above snippet, a website owner would replace **GA_MEASUREMENT_ID** with the ID of the Google Analytics property they set up in step 2 above.

Implementation and exact composition of the global site tag can vary significantly depending on the type of website and the needs and choices of the website owner.

3. Has the website owner concluded a contract with Google LLC and/or Google Ireland Ltd when embedding the Google Services (including Google Analytics) tool on its website? If so, please specify whether the website owner could negotiate the terms of the contract. Also, please indicate whether this or other contracts determines the responsibilities of the parties for compliance with the GDPR.

Yes, the ability to use Google Analytics is subject to contract.

Google offers Google Analytics under the GA Terms which incorporate the DPTs. Google Analytics is listed at https://privacy.google.com/businesses/adsservices/ as a Processor Service pursuant to the definition of "Processor Services" in section 2.1 of the DPTs. Pursuant to section 5.1.1 (b) Google acts as a processor on behalf of the website owner and as such, as well as set out in section 5.3, only processes Google Analytics Data under the instructions of the website owner when providing Google Analytics services.

As with many one-to-many, Software-as-a-Service products, the contract terms for the Google Analytics free version are available online and website owners agree to them on a click-to-accept basis. The contract terms for Google Analytics 360 are under the Google Analytics 360 Order Form. Some website owners who are interested in the payable service Google Analytics 360 choose to negotiate these terms.

In addition to implementing Google Analytics, a website owner may choose to share their analytics data with Google by activating the Google products & services data sharing setting, and separately accepting the Google Measurement Controller-Controller Data Protection Terms, which govern the use of that setting. When this data sharing is enabled, the relevant Google entity (see our response to question #25) will act as a controller. In these circumstances: (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. The Google Measurement Controller-Controller Data Protection Terms makes that clear (see clause 4.4).

Whether or not the data sharing setting is activated, this does not impact Google's role as a processor under the DPTs when providing the Google Analytics free service, since data collected under the data sharing setting is kept and handled separately from data collected in the processor capacity. Google always acts as a processor when delivering Google Analytics services to its customers as is also made clear by section 8.2 of the Google Measurement Controller-Controller Data Protection Terms.

4. What are the unalterable settings when implementing the code for Google Services (including Google Analytics) in a website and which settings are left in the hands of the owner of that website?

Website owners are in full control of whether, to what extent and how they implement Google Analytics on their website.

They have the overarching control whether to implement Google Analytics on a website at all as well as which individual pages of a website to implement it in (e.g. by either not embedding the global site tag in a page or by disabling pageview measurement for that page). Additionally, website owners have control over all settings made available in Google Analytics, thereby giving them a lot of additional granular control. The website owners choose how to configure their tags and can enable and disable various Google Analytics features via the user interface. Once website owners choose to implement Google Analytics or certain configurations of Google Analytics, some elements of data collection are happening for Google Analytics or a given configuration to function properly, while others can be configured further (e.g. see here and here).

In this context, please specify which entity determines

(i) what data are processed for which purposes,

The website owner determines the purposes for the processing of the data collected.

A purpose that all website owners are likely to have determined before choosing to implement a web analytics service like Google Analytics on their website is to measure the interactions of users with their website. Other purposes that website owners may determine can vary greatly. For example, a website owner may have determined the purpose of simply measuring the performance of their website or specific portions thereof for reporting purposes, another may have determined the purpose of gaining insights into the composition of the audience the website attracts with the aim to better serve that audience going forward, and another website owner may have determined the purpose of finding out which marketing channels drive traffic to which offerings on the website in order to improve those marketing channels etc.

In accordance with the purposes that the website owners have determined, they will determine the means by which to pursue those purposes including which web analytics tool to use and which data to collect through the chosen tool as well as retention periods for such data. Website owners who choose Google Analytics, can determine the data that is being collected by configuring their tags and enabling and disabling various Google Analytics features via the user interface (such as the Google Analytics Retention controls described below).

Where the website owner chooses to turn on the products & services data sharing setting, Google can separately access and analyse data to better understand online behavior and trends, and use this data to improve Google products and services. As described in our response to question #3, Google acts as a controller when it uses data for these purposes.

(ii) their retention period and when it begins,

The Website owner determines the retention periods for data.

The Google Analytics Data Retention controls give website owners the ability to set the amount of time before user-level and event-level data stored with Google Analytics is automatically deleted from Analytics servers. Depending on the type of Analytics property, the website owner can choose between multiple retention periods which range from 2 months to 50 months from when the data was collected. Website owners can also decide that certain event-level or user-level data does not expire. In certain circumstances, data will be retained for shorter periods than those selected. For example, the maximum amount of time that

Analytics will retain Google signals' data is 26 months, regardless of the settings (also see our response to question #6 (ii)).

Customers using Google Analytics can also use IP-Anonymization to instruct Google to anonymize all IP-addresses immediately after they are collected. If turned on, at no time is the full IP-address written to disk as all anonymization happens in memory nearly instantaneously after the request has been received.

(iii) their recipients, and

The website owner determines the recipients of the data in multiple ways.

Website owners choose Google and Google's subprocessors as recipients of data when they elect to use Google Analytics and implement it on their website. Information about our subprocessors is set out in the DPTs: https://privacy.google.com/businesses/subprocessors/

Since Google Analytics customers own and control the data processed by Google on their behalf, website owners have multiple ways of sharing their analytics data with additional recipients. The type of data shared with other recipients will depend on the way in which the website owner uses the product functionality. Inter alia, they can use functions via the user interface to share reports, they can use reporting APIs to enable more direct, programmatic access to data and they can export and download data and then share it with any recipient they choose.

Where the website owner chooses to turn on the products & services data sharing setting, Google becomes a recipient of the data shared through that setting as it can then separately access and analyse that data.

(iv) the categories of data subjects.

By implementing a web analytics tool such as Google Analytics, which collects information about users' activity on a website, the website owner determines the category of data subjects as "users of my website". Website owners may choose to determine the categories of data subjects more narrowly by restricting access to a website or parts thereof to a category of users (e.g. "customers" who need to login to access the website). In addition, website owners may choose to import data about other categories of data subjects (who may or may not have visited the website) using the data import functionality.

Please also describe if the owner of the website has the possibility (for example, in the setting section of the tool) to decide

(v) which particular data Google receives because of the fact that he implements Google Services (including Google Analytics) in the website and

As said above in our response to question #4, website owners are in full control of how they implement Google Analytics on their website. This gives them the overarching control whether to collect any data through Google Analytics at all, as well as which portions of their website they want to collect data from. And website owners have control over all settings made available in Google Analytics, thereby giving them a lot of additional granular control. Website owners exercise this control by choosing how to configure their tags and enabling or disabling various Google Analytics features via the user interface.

Google Analytics contains a number of controls within the user interface, including controls that enable website owners to programmatically disable data collection from Google Analytics web properties, automatically anonymize IP addresses that are sent to Google and many more. See this help center article for more information.

(vi) whether or not any kind of data is transferred to the USA when implementing Google Services (including Google Analytics) in a website.

Google Analytics does not offer settings that enable data to be localised to any particular geographic location (also see our response to questions #7 and #8 below).

5. According to the Google Ads Data Processing Terms (section 5.2 and 5.3), Google would comply with the instructions given by the website owner. Please explain how Google LLC and Google Ireland Ltd would receive instructions from the website owner, with supporting examples.

The website owner instructs Google in multiple ways.

The website owner instructs Google to process data to provide the Google Analytics service and as documented in the form of the GA Terms and the DPTs by entering into the agreement with Google that incorporates the DPTs. Google receives these instructions by entering into that agreement with the website owner.

As set forth in section 5.2 (b) of the DPTs the website owners can further specify instructions by how they use the Google Analytics service. There are many ways that a website owner can issue instructions in this way, for example:

- The website owner could provide instructions via the settings in the Google Analytics user interface, such as instructions as to the retention period for data (see our response to question #4(ii)). Google directly receives these instructions via the settings (learn more here). If a website owner wanted to create and manage custom reports, they would open the user interface and follow the steps specified in this help centre article, and Google Analytics will create the reports as instructed.
- Website owners also issue instructions through the global site tag they embed in their websites. One such instruction can be made by setting the value of the anonymize_ip parameter in the global site tag to "true". This adds an additional parameter (&aip=1) to the pixel request that sends data to google-analytics.com (see our response to question #2 above). Google receives this instruction via the pixel request (learn more here).
- Examples of instructions to delete data are set out in our response to question #6(i) below.

6. Please prove and explain the following assertions that stem from the Analytics Help page entitled « Safeguarding your data » and the one entitled « Data retention »:

(i) « Safeguarding your data » - User Deletion : « Customers may delete a single user's data from Google Analytics by passing a single user identifier to the Google Analytics User Deletion API or via our User Explorer report ».

Deletion by passing a single user identifier to the User Deletion API. The Google Analytics User Deletion API allows website owners to process deletions of data associated with a given user identifier with the upsert method. This method for data deletion takes a User Deletion Request Resource as its only parameter. A user whose data will be deleted can be specified by setting one of the identifiers inside *id.userId* field. The type of the identifier must be specified inside the *id.type* field.

Deletion via our User Explorer report. The User Explorer report lets website owners isolate and examine individual rather than aggregate user behavior. The User Explorer functionality is enabled on the website owner's instruction. The website owner can choose to delete data for an individual user from a User Explorer report and from the Google Analytics system by clicking "Delete User" at the bottom of the report.

Once deletion is requested through either one of these methods, data associated with the user identifier will be removed from the report within 72 hours, and then deleted from Analytics servers during the next deletion process. Deletion processes are scheduled to occur approximately every two months.

(ii) « Data retention » - User and event data retention : « The maximum amount of time that Analytics will retain Google-signals data is 26 months, regardless of your settings. »

Google signals is an optional feature in Google Analytics that, when activated, supplements reports that are based on data from Google users who have turned on Ads Personalization in their Google account. For example, if a website owner has chosen to create remarketing audiences (more information here) and share those audiences with their own linked advertising accounts, the website owner will be able to use their advertising product accounts (e.g. Google Ads or Search Ads 360) to serve ads in cross device-eligible remarketing campaigns to the Google signed-in users that have turned on Ads Personalization.

Where we say in our data retention help centre article that the "maximum amount of time that Analytics will retain Google signals data is 26 months, regardless of your settings", this means that Google signals data will be subject to a maximum 26 months retention period, even if Analytics customers have set longer retention periods for data through the methods described in our response to question #4(ii) above. This serves the purpose of making website owners aware that choosing a longer retention period does not prolong the retention for Google signals beyond 26 months.

(iii) « Google Measurement Controller-Controller Data Protection Terms – 4.4 End Controllers : for European Controller Personal Data processed by Google, Google Ireland Limited is the Google End Controller.

Website owners may choose to activate the Google products & services data sharing setting, and accept the Google Measurement Controller-Controller Data Protection Terms, which govern the use of that setting.

When this data sharing setting is enabled, a Google entity will process data shared through that setting as a controller by separately accessing and analysing that data to better understand online behavior and trends, and use this data to improve Google products and services. In these circumstances: (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. The Google Measurement Controller-Controller Data Protection Terms makes that clear (see clause 4.4).

7. Please indicate in which country/countries the data received from Google Services (including Google Analytics) are hosted.

8. Regardless of your classification as personal data or non-personal data, please describe in detail which data may be transferred to the USA because of the fact that Google Services (including Google Analytics) are implemented in a specific website (for example IP-address, information stored in cookies, browser information or other meta data)?

(In response to questions #7 and #8:)

The websites that use Google Analytics are generally available globally and often attract a global audience and will therefore be visited by users around the world. The technical infrastructure that supports the collection through Google Analytics of information about those users' interactions with a website is deployed globally to reduce latency and ensure redundancy of systems.

Information about the locations of Google data centers is available here. Google operates data centers globally and to maximize the speed and reliability of our services, our infrastructure is generally set up to serve traffic from the data center that is the closest to where the traffic originates. The Analytics Collection Network (the set of servers that provide two main services: the serving of the Analytics JavaScript and the collection of data sent via the GIF requests) is no different and is widely deployed in the EU and elsewhere in the world. The Google Analytics pixel-request (including all the information sent with that request, see our response to question #2) will be first routed to the closest collector in the system and may then be transferred onward for storage and processing. Therefore the precise location of information collected through Google Analytics will vary depending on where such traffic originates.

In accordance with section 10.1 of the DPTs, the Customer agrees and instructs Google to store and process Customer Personal Data (as defined in section 2.1 of the DPTs), which includes Google Analytics Data, in any country in which Google or any of its Subprocessors maintain facilities.

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

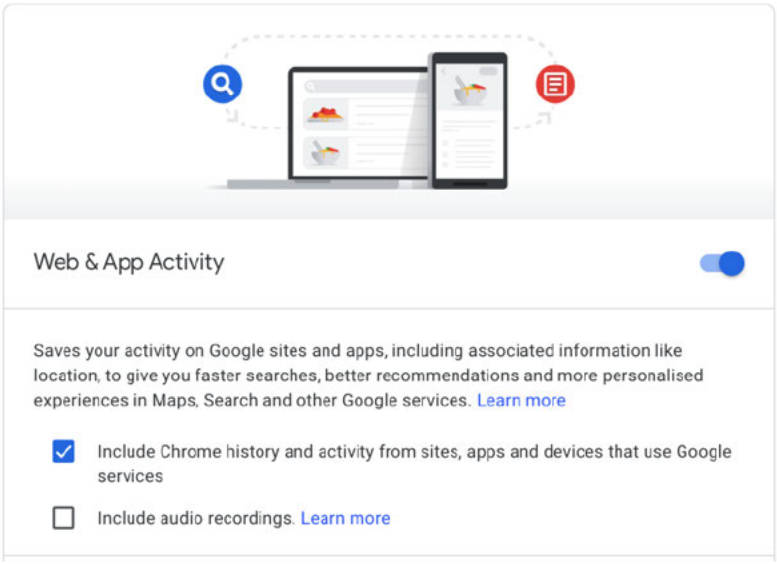
9. In the present complaint, the complainant was logged in his Google Account when visiting the specific website of the website owner. Does the implementation of Google Services (including Google Analytics) enable Google to receive the information that a specific Google Account user visited a specific website? If so, please describe how it is done and describe which information about the Google account user is collected.

No, the implementation of Google Analytics as such does not enable Google to receive the information that a specific Google Account user visited a specific website.

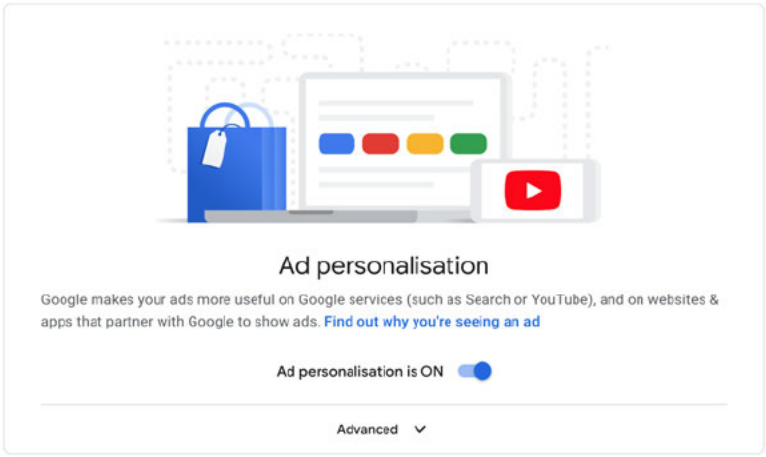
The implementation of Google Analytics on a website enables Google to receive the information that a specific Google Account user has visited that website, only if the following additional conditions are met:

(1) The user has activated the Web & App Activity setting in their Google Account and additionally;

(2) the user has chosen to include activity from sites that use Google services;



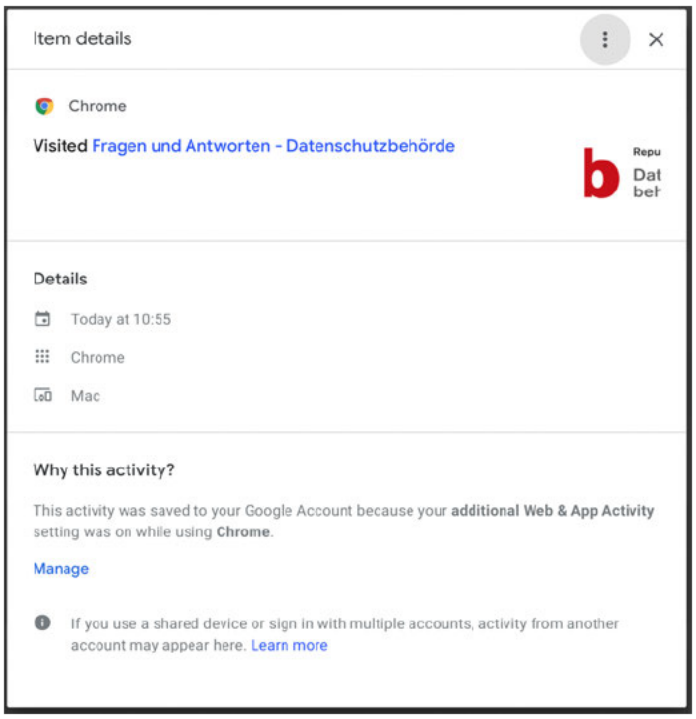
(3) the user has activated the Ads Personalisation setting;



(4) and the user is logged in to their Google account in the same browser, while visiting that website.

If Google Signals (see our response to question # 6(ii)) is activated on that website, Google is then able to log that user's visit to that website in the user's account Web & App Activity.

An entry in a user's Web & App Activity related to a visit to a website looks as follows (example is based on the use of the browser Chrome):



The user can deactivate or change Ads Personalisation (more information here) and/or Web & App Activity settings at any time and the user can delete individual entries or make bulk deletions in multiple ways any time (more information here).

10. If a website makes use of Google Services (including Google Analytics), does Google LLC and/or Google Ireland Ltd have the possibility to link data received from the browser of the user when visiting this website to a specific user even if that user is not logged into any Google Account at the time he/she accesses the website?

See our response at question #12 below.

11. If a website makes use of Google Services (including Google Analytics) and a Google user visits said website, does Google have the possibility to link the data received from this user's browser (that the user uses to visit the website) to that user, even if the browser used for visiting said website is a different browser than the one the user uses to log into his/her Google account?

See our response at question #12 below.

12. If a website makes use of Google Services (including Google Analytics) and a user who does not have a Google account visits said website, does Google have the possibility to link the data received from the browser of this user (that the user uses to visit the website) to that user?

Questions #10, #11 and #12 are asking whether Google, in the following three scenarios, has the possibility to link data, which it receives from the browser of a user who visits a website, to that user, because that website

uses Google Analytics:

> **Scenario 1** (question #10): The user visits the website. The user has a Google account but is not logged in to the Google account.
>
> **Scenario 2** (question #11): The user visits the website with one browser. The user is logged in to a Google account, but in another browser.
>
> **Scenario 3** (question #12): The user visits the website. The user does not have a Google account.

All three scenarios have in common that the user who visits the website is not logged in to any Google account in the browser that they use to visit that website. Accordingly, none of these scenarios meet condition (4) in our response to question #9 under which Google is enabled to collect the user's visit to the website in the user's account.

Please see our response to question #13 regarding the technical capabilities in Google Analytics that enable the linking of data, received from the browser of a user who visits a website, to a specific user.

13. From a technical point of view, please describe in detail what possible identifiers Google LLC and/or Google Ireland Ltd has available to link data received from the browser of a user when he visits a web page on which Google Services (including Google Analytics) are implemented to a specific user (for example but not limited to: UUID cookies or browser fingerprinting).

As mentioned in our response to question #2, Google Analytics uses first party cookies. Website owners use these cookies to enable Google Analytics to determine that two distinct hits to a website belong to the same user by sending a unique identifier, associated with that particular user, with each hit.

This is accomplished via the Client ID field, a unique, randomly generated string that gets stored in the cookies of the user's browser, so that subsequent visits to the same site can be associated with the same user.

Google Analytics enables the use of a single, first-party cookie named _ga to store the Client ID (more information here). The cookie's name, domain, and expiration time can all be customized by the website owner. Other cookies that can be created with Google Analytics and that are used to distinguish users include _gid, AMP_TOKEN, _gac_<property-id> and __utma. More information on the usage of Google Analytics cookies is available here.

Through these cookies Google Analytics enables the identification of unique users across browsing sessions, but it cannot identify unique users across different browsers or devices. If a website owner's website has its own authentication system, the website owner can use the User ID feature, in addition to the Client ID, to more accurately identify a user across all the devices and browsers they use to access the website.

Website owners are not allowed to use device fingerprinting or locally shared objects (e.g. Flash cookies, Browser Helper Objects, HTML5 local storage) other than HTTP cookies, or user-resettable device identifiers designed for use in measurement or advertising, in connection with Google Analytics. See this Analytics Policy for more information.

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.

14. Please describe the role of Google LLC and/or Google Ireland Ltd in the collection of raw data and their processing for statistic purposes.

Please see our response to question #3 regarding Google's role as a processor when collecting data on behalf of website owners who use Google Analytics.

15. Please describe in detail how Google LLC and/or Google Ireland Ltd can use the information they receive because of the fact that Google Services (including Google Analytics) are implemented in a specific website. For example, can they use this information to enrich the profile of a user for personalised ads or to improve the Google services? Please provide factual evidence for your answer.

Please see our response to question #3 regarding how Google uses data under the products & services data sharing setting.

Please also see our responses to questions #s 9 to 13.

As mentioned in those responses, website owners are the controllers of the data they collect on their sites via Google Analytics, and Google is a processor of that data, meaning Google would only use the data under the instructions of the website owners.

16. Considering the Article 29 Working Party Opinion 9/2014 on the application of Directive 2002/58/EC, how do Google Tools assess the HTTP Do Not Track (DNT) header requests (also available on Google Chrome web browser)? How does it affect cookies stored by Google Tools on the user's device and data collected from the user's web browser?

Enabling "Do Not Track" on a browser like Chrome means that a corresponding request will be included with a user's browsing traffic. As emphasized in the mentioned Opinion, any effect depends on whether a website responds to the request, and how the request is interpreted by that website.

For example, some websites may respond to this request by showing ads that aren't based on other websites a user has visited. Many websites will still collect and use browsing data - for example to improve security, to provide content, services, ads and recommendations on their websites, and to generate reporting statistics.

Website owners have multiple options how to enable their visitors to express their preferences with regard to data collection through the website and how to honour those preferences as encouraged in the Opinion. The use of these solutions is very widespread and they can be used to control collection through web analytics services including Google Analytics.

Google, too, offers support to website owners with the following options:

- Website owners can notify their users of the availability of the Google Analytics opt-out browser add-on. Once installed, the add-on prevents the Google Analytics JavaScript that is running on any website from sharing information with Google Analytics (learn more here).

- If a website owner wants to disable the Google Analytics tag on a page without having to remove the Google Analytics tag itself, e.g. to support a user to opt-out or opt-in of Google Analytics measurement, the analytics.js library includes a window property that, when set to true, disables analytics.js from sending data to Google Analytics. When Google Analytics attempts to set a cookie or send data back to the Google Analytics servers, it will check whether this property is set to true. If it is, no action will be taken (learn more here).

17. When a website implements Google Tools, if one user visiting that page does not consent to other cookies than the strictly necessary ones and not allowing those for statistical purposes, how can this information be passed to the implemented Google Tools by the website owner? What will be the behaviour of each tool based on this user's preference?

As said above, website owners have multiple options how to enable their visitors to express their preferences with regard to data collection through the website and how to honour those preferences.

Google Analytics will behave differently depending on what the website owner chooses to implement. At a high level, the website owner has the following options, which have the following impacts on the behaviour of Google Analytics:

- *Prevent the inclusion of the global site tag* - A website owner can make the inclusion of the global site tag into the webpage loaded by the user subject to certain conditions, such as a user's choice expressed in a consent notice. As explained in our response to question #2 above, the Analytics tracking operation would only start retrieving data from a user's browser when the Analytics JavaScript code on the customer's website references the JavaScript file that collects and attaches the data parameters to a single-pixel image request.
- *Disable the global site tag* - A website owner can include the global site tag loaded but disable it (by setting the `send_page_view` parameter to `false`) subject to certain conditions, such as a user's choice expressed in a consent notice. This is an instruction to the Google Analytics JavaScript file not to execute the tracking operation that retrieves and attaches the parameters to the pixel request (see example here).
- *Prevent sending of data by Google Analytics JavaScript* - Both the abovementioned Google Analytics opt-out browser add-on and window property essentially prevent the Google Analytics JavaScript from executing the tracking operation, thereby preventing data from being sent to Google Analytics.
- *Implement Consent Mode (beta) in Google Analytics* - Website owners can implement Consent Mode (beta), which allows them to adjust how Google tags behave based on the cookie consent status of a user. When consent for ad storage or analytics storage is denied, the associated Google measurement functions deployed via global site tags (gtag.js) or Google Tag Manager will adjust their behavior accordingly (see here).

18. Pursuant to the Analytics Help page entitled « Data sharing settings », regardless of the data sharing settings, the Analytics data may also be used by Google only insofar as necessary to maintain and protect the Analytics service. Please specify this processing, and notably

It is important to consider this quote in its immediate context:

> "These settings [i.e. the data sharing settings] only let you customize how you share the data you collect from websites, mobile apps, and other digital devices using Analytics. They do not apply to data about your Analytics account or how your account is used, like the number of properties and which additional features are set up. Regardless of your data sharing settings, your Analytics data may also be used only insofar as necessary to maintain and protect the Analytics service."

Data related to users' activity on the Google Analytics customer's site belongs to that website owner, and, per its role as a processor, Google would only use this data as instructed and necessary to provide and maintain the service, which may include checking the data for spam and fraud detection purposes.

If the website owner chooses to enable the Google products & services data sharing setting (and accept additional terms governing the use of that setting), then Google becomes a controller of that data, and may use it more broadly to improve its products and services.

Separately, Google is the controller of any personal data related to how website owners use Google Analytics (for example, the number of properties their account has, and which additional features are set up in their account), and use of that data is not impacted by the customer's data sharing settings. This data is not not related to users' visits to the website owner's site that is described in our response to question #2.

The processing conducted for maintaining and protecting the Analytics service includes detection and prevention of misuse, abuse, spam, malware and other harmful activity that endangers the service or its users.

(i) which data are "necessary", and which is the legal basis for such a processing,

See our answer immediately above.

The data related to how website owners use Google Analytics that may be used, is data like the number of properties and which additional features are set up in a given Google Analytics account. Insofar as such data constitutes personal data, the legal basis for the processing by Google will be that the processing is necessary for the performance of a contract to which the website owner - as the data subject - is party and Google's legitimate interest to protect the Analytics service against misuse, abuse, spam, malware and other harmful activity that endangers the service or its users.

(ii) if such use can be made by both Google LLC and Google Ireland Ltd and

To the extent such data is personal data, it will be used for these purposes by the Google entity that is the controller of such data. In relation to website owners as data subjects in the EEA and Switzerland this is the Google Ireland Limited.

(iii) if this applies regardless of the offer (Google Analytics 360 and the free version of Google Analytics).

Data will be used to protect and maintain both the Google Analytics and Google Analytics 360 services.

19. Does Google Ireland Ltd send data received through Google Services (including Google Analytics) to Google LLC? If yes, please describe which ones and for which purposes.

As described in our response to question #3 above, the embedded global site tag leverages functionality of the devices and software that users use to interact with a website that has implemented Google Analytics, so that these devices send Google Analytics Data to the domain google-analytics.com by making the single-pixel GIF image request mentioned in our response to question #2.

As mentioned in our response to question #7, the Google Analytics pixel-request will be first routed to the closest collector in the system and may then be transferred onward for storage and processing. Therefore the precise location of information collected through Google Analytics will vary depending on where such traffic originates.

In accordance with section 10.1 of the DPTs, the website owner agrees and instructs Google to store and process Customer Personal Data (as defined in section 2.1 of the DPTs), which includes Google Analytics Data, in any country in which Google or any of its Subprocessors maintain facilities. Where Google Ireland Limited is the website owner's processor, Google LLC is a Subprocessor to Google Ireland Limited under the DPTs and the data importer under the SCCs.

20. Does Google Ireland Ltd disclose any kind of data received through Google Services (including Google Analytics) to any entities other than Google LLC (all designated hereafter as the Recipients)?

If yes, please describe in detail

i) which data Google Ireland Ltd discloses to any kind of entities other than Google LLC and

ii) to whom Google Ireland Ltd discloses the data (specifying in which countries they are settled and where they process the data) and for which purposes.

Please see our response to question #4 (iii) with regard to recipients of data.

Because Google Ireland Limited is responsible for providing the majority of Google services in the European Economic Area and Switzerland, it also receives requests for user information from governments.

Requests from Irish government agencies

Google Ireland considers Irish law when evaluating requests for user information by an Irish agency. Irish law requires that Irish law enforcement authorities obtain a judicially-authorized order to compel Google Ireland to provide user information.

Requests from government authorities outside Ireland

Google Ireland offers services to users located throughout the European Economic Area and Switzerland, and we sometimes receive data disclosure requests from government authorities outside of Ireland. In this case, we may provide user data if doing so is consistent with all of the following:

- **Irish law**, which means that the access and disclosure is permitted under applicable Irish law, such as the Irish Criminal Justice Act
- **European Union (EU) law applicable in Ireland**, which means any EU laws applicable in Ireland including the General Data Protection Regulation (GDPR)
- **Law of the requesting country** which means that we require the authority to follow the same due process and legal requirements that would apply if the request were made to a local provider of a similar service
- **International norms** which means we only provide data in response to requests that satisfy the Global Network Initiative's Principles on Freedom of Expression and Privacy and its associated implementation guidelines
- **Google's policies** which include any applicable terms of service and privacy policies, as well as policies related to the protection of freedom of expression

21. Please describe whether Google LLC and/or Google Ireland determines the purposes and means of the processing of the data Google receives through Google Services (including Google Analytics).

As said above, website owners determine the purposes and the means of the processing of any personal data they collect through Google Analytics. Google acts as a processor on behalf of its customers when providing Google Analytics.

Customers may choose to activate the Google products & services data sharing setting (and accept additional terms governing the use of that setting). When this data sharing setting is enabled, Google can separately access and analyse data to better understand online behavior and trends, and use this data to improve Google products and services. Google acts as a controller when it uses data for these purposes (and the additional terms governing the use of this setting makes that clear). However, this does not impact Google's role as a processor under the GA DPT since data collected under the data sharing setting is kept and handled separately from data collected in the processor capacity. Google always acts as a processor when delivering Google Analytics services to the Customer.

22. In its ruling from 16 July 2020, case C-311/18, the European Court of Justice held that the Privacy Shield Decision (Commission Implementing Decision (EU) 2016/1250 of 12 July 2016) was invalid. Please describe if and when you checked whether or not this court ruling applies to the possible international data transfers resulting from the tool Google Services (including Google Analytics)?

The applicability of the decision to website owners' use of Google Analytics was self-evident immediately, given that until that decision Google and website owners relied on the EU-US Privacy Shield and Google LLC's certification with the US Department of Commerce under the EU-US Privacy Shield Framework as a transfer mechanism.

Following the CJEU's decision, Google immediately started work to amend the DPTs to make SCCs applicable to all impacted contracts. This involved updating a large number of contracts, sending notifications to

website owners on August 3, 2020, translations and publication of the relevant contract terms. These changes to the DPTs became effective on August 12, 2020. Google LLC continues to be certified under the EU-US Privacy Shield Framework and continued to apply the protections of that framework to any Google Analytics Data that had been transferred during the time it took to update the DPTs.

The updated DPTs set forth in section 10 that to the extent the storage and/or processing of Customer Personal Data, including personal data in Google Analytics Data, involves transfers of Customer Personal Data from the EEA to any third country that is not subject to an adequacy decision under the GDPR, the website owner (as data exporter) will be deemed to have entered into the SCCs with Google LLC (as data importer)[2] for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. The SCCs are made available at https://privacy.google.com/businesses/processorterms/mccs. These SCCs correspond to the clauses published by the European Commission in its decision 2010/87/EU.

23. If you concluded that this court ruling does not apply to your use of the tool, please describe the reasons for this conclusion in detail.

Please see answer to question #22 above.

24. If you concluded that this court ruling does apply to your use of the tool, please describe on which transfer tool pursuant to Chapter 5 of the GDPR you base the data transfers to third countries, particularly to the USA.

Please see answer to question #22 above. The SCCs used correspond to the clauses published by the European Commission in its decision 2010/87/EU.

25. If you base the data transfers to the USA on standard data protection clauses (SCCs) adopted by the Commission pursuant to Article 46 (2) (c) GDPR, please inform us with whom you have signed such SSCs, specify which template from the Commission was used for concluding SCCs (SCCs for transfers between two data controllers or SCCs for the transfer of personal data to processors established in third countries) and provide a signed copy of them.

The website owners enter into the SCCs with Google LLC. The SCCs are made available at https://privacy.google.com/businesses/processorterms/mccs. These SCCs correspond to the clauses published by the European Commission in its decision 2010/87/EU.

Website owners were notified in accordance with Section 16.3 of the Google Ads Data Processing Terms on August 3rd, 2020 that these SCCs were to be incorporated into the DPTs. The incorporation of the SCCs

[2] For the avoidance of doubt, this is also the case for website owners having contracted with the Google Ireland Limited under the Google Analytics 360 Order Form.

became binding between Google and website owners on 12 August 2020.

If website owners choose (at their option) to turn on the products & services data sharing setting, (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. The Google Measurement Controller-Controller Data Protection Terms makes that clear (see clause 4.4). Where Google Ireland Limited acts as the independent controller, SCCs are not required because Google Ireland Limited is established in Ireland and such transfers are therefore permitted under the EU GDPR. However, the parties do enter into the Google Measurement Controller-Controller Terms.

26. If you have concluded such SCCs, have you ensured that there is no agreement, arrangement or similar that contradicts, directly or indirectly, any clause of the SCCs or prejudices the fundamental rights or freedoms of the data subjects (for example: any clause that provides conditions for audits or other rights and obligations set forth in the SCCs)?

Under Clause 10 of the SCCs both the website owner and Google LLC undertake not to vary or modify the SCCs. According to Clause 10 of the SCCs, this does not preclude the parties from adding clauses on business related issues where required, as long as they do not contradict the SCCs. The Google Ads Data Processing Terms include clauses on business related issues, including business related processes and procedures regarding how audits should be conducted. The clauses do not vary or modify the SCCs and for the avoidance of doubt, section 7.5.4 of the Google Ads Data Processing Terms makes it clear that nothing in the audits clause varies or modifies any rights or obligations of the data exporter or data importer under the SCCs.

27. If you have concluded such SCCs, have you checked that there is nothing in the third country's legislation that prohibits the Recipients (in particular Google LLC) from complying with their contractual obligations as laid out in the SCCs in order to ensure that the level of data protection of natural persons guaranteed in the EEA is not undermined?

Yes.

28. If you concluded that the Recipients (in particular Google LLC) can in fact guarantee the fulfilment of the contractual obligations as laid out in the SCCs, please describe your reasons for this conclusion in detail and provide evidence of these facts to the Austrian Data Protection Authority.

In its ruling from 16 July 2020, case C-311/18, the CJEU states that it has to be verified if the law or practice of the third country to which personal data is exported impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools such as the SCCs. In that case, the Court still leaves open the possibility for exporters to implement supplementary measures that bring the effectiveness of the appropriate safeguards up to the level required by EU law.

U.S. Laws mentioned in the complaints

All complaints including the one against netdoktor.at GmbH focus on the impact of U.S. law on data transfers to the U.S. In particular the complaint focuses on US Executive Order 12333 (EO 12333) and Title 50 United States Code (U.S.C.) § 1881a (FISA 702), both of which were also considered by the CJEU in its ruling. Without going into all the relevant details, we have set out specific information about those laws below.

EO 12333 is a charter document that organizes and assigns roles and responsibilities to the U.S. intelligence community and articulates high-level principles with which all intelligence activity must comply. Specific intelligence activities conducted under EO 12333 are subject to more specific implementing procedures (which may be classified) that include safeguards and protections appropriate to that type of intelligence activity. EO 12333 primarily governs intelligence activities that occur outside the US. EO 12333 is understood to permit the US to conduct electronic surveillance *outside* the US consistent with US legal requirements; it does *not* authorise electronic surveillance *within* the US nor does it impose requirements on service providers inside or outside the US.

Section 702 of the FISA Amendments Act (FAA), which also requires the US government to minimize its use and dissemination of data, has two components: Upstream and Downstream.

- Section 702 Upstream authorizes U.S. authorities to collect data travelling over internet "backbone" infrastructure controlled by electronic communication service providers in the U.S. (e.g. U.S. telecom providers). To the extent any user or customer data traverses networks subject to Upstream 702 collection, that data is encrypted in transit as described below.
- Section 702 Downstream authorizes U.S. authorities to obtain targeted data directly from electronic communication service providers. To the extent Google LLC may be subject to targeted requests under Downstream 702, Google carefully reviews each request it receives under FISA in accordance with the guidelines described below to make sure it satisfies all applicable legal requirements and Google's policies.

In the ruling, the CJEU has expressed its views on these laws. In response to the Judgement, the U.S. Government has published a whitepaper providing information on privacy protections in U.S. law concerning government access to data for national security purposes. This whitepaper covers material reviewed by the CJEU and some material the US Government considers additional.

In its FAQ document on the ruling[3], the EDPB has summarized the CJEU's finding by saying that the CJEU found that U.S. law (i.e., Section 702 FISA and EO 12333) does not ensure an essentially equivalent level of protection. The EPDB goes on to say that whether or not transfers of personal data on the basis of SCCs can continue will depend on the result of an assessment, taking into account the circumstances of the transfers, and supplementary measures that are put in place.

Supplementary Measures

When launching the SCCs for Google Analytics, Google relied on measures - legal, technical, and operational - that were put in place to protect Google Analytics Data, including the following:

[3] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems.

Legal and Organizational Measures

- Google evaluates each and every request it receives from governmental authorities for user data. A dedicated team of Google lawyers and specially trained personnel will always **carefully review each request** to make sure it satisfies applicable laws and Google's policies. We also review whether a request is proportional and we attempt to have it narrowed if this is not the case. In some cases we object to producing any information at all.
- We will **notify the customer** before any of their information is disclosed unless such notification is prohibited by law or the request involves an emergency, such as an imminent threat to life. We will provide delayed notice to the customer if a legal prohibition on prior notification is lifted, such as when a statutory or court ordered disclosure prohibition period has expired.
- Google **publishes a** Transparency Report. Specifically, Google provides as much information as legally permissible on the US national security requests it receives in its Transparency Report.
- Google also publishes its policy on handling government requests for information for more information about how we handle government requests for user data, and for a more detailed explanation about our policies and procedures.

Technical Measures

- Protection of data in transit

  Google utilizes **robust technical measures** to safeguard personal data, and to protect against interception in transit.
  - Google Analytics by default uses **HTTP Strict Transport Security** (HSTS), which instructs browsers that support HTTP over SSL (HTTPS) to use that encryption protocol for all communication between end users, websites, and Google Analytics' servers. Such encryption prevents intruders from being able to passively listen to communications between websites and users. More information on Google's use of HTTPS is available here.
  - Google also **encrypts data** at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google (see below for specific technologies that are used). For example, **when data is transferred between Google's data centers.** Even if any data were intercepted during these transfers, it would be unreadable. For more information:
    - **Protecting communication between Google services.**
      Google protects service-to-service communications at the application layer using a mutual authentication and transport encryption system developed by Google called Application Layer Transport Security (ALTS). ALTS is similar in concept to mutually authenticated TLS but has been designed and optimized to meet the needs of Google's data center environments. ALTS authenticates the communication between Google services and helps protect data in transit. ALTS is a highly reliable, trusted system that provides authentication and security for Google's Remote Procedure Call (RPC) communications. ALTS requires minimal involvement from Google services themselves. When Google services communicate with each other they do not need to explicitly configure anything to ensure data transmission is protected; this is protection of user data by design and by default.
    - **Protecting data in transit between data centers.**

ALTS ensures the integrity of Google traffic is protected, and encrypted as needed. After a handshake protocol between the client and the server is complete and the client and the server negotiate the necessary shared cryptographic secrets for encrypting and authenticating network traffic, ALTS secures RPC (Remote Procedure Call) traffic by forcing integrity, and optional encryption, using the negotiated shared secrets. Google supports multiple protocols for integrity guarantees, e.g., AES-GMAC (Advanced Encryption Standard) with 128 bit keys. Whenever traffic leaves a physical boundary controlled by or on behalf of Google, e.g., in transit over WAN (Wide Area Network) between data centers, all protocols are upgraded automatically to provide encryption as well as integrity guarantees.

- **Protecting communication between users and websites.**
  HTTPS encryption helps keep users' browsing safe by securely connecting their browser or app with the websites they visit. HTTPS relies on encryption technology—SSL or TLS—to secure these connections. Such encryption prevents intruders from being able to passively listen to communications between websites and users. In 2015 Google announced a set of initiatives to bring this "HTTPS Everywhere" mission to our advertising products as well, to support our advertiser and publisher customers and partners. We have been publishing a report that provides data on the status of HTTPS adoption and usage at Google and across the web, including for our advertising products, as well as additional information about Google's use of encryption.

- Protection of data at rest

Google utilizes **robust technical measures** to safeguard personal data, and to protect against it against unauthorized access at rest. Encryption "at rest" in this section means encryption used to protect user data that is stored on a disk (including solid-state drives) or backup media.

- Google **encrypts Google Analytics Data** that is stored **at rest** in its data centers using the Advanced Encryption Standard. Each data center is protected with **six layers of physical security** designed to thwart unauthorized access.
  - All user data is encrypted at the storage level, generally using AES256 (Advanced Encryption Standard). Data is often encrypted at multiple levels in Google's production storage stack in data centers, including at the hardware level, without requiring any action by Google customers. Using multiple layers of encryption adds redundant data protection and allows Google to select the optimal approach based on application requirements.
  - Google uses common cryptographic libraries which incorporate Google's FIPS 140-2 validated module, to implement encryption consistently across products. Consistent use of common libraries means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code.
  - Google provides public-facing information about our data protection and security measures here.

- Google **custom-builds servers exclusively for its data centers** and maintains an industry-leading security team to ensure that Google's data centers are among the safest in the world. Google's production data centers are protected by several layers of security to prevent any unauthorised access to data, including specifically:

- **Layer 1 - Boundary security**: Data center site boundaries are physically secured with fencing, signage and other measures.
- **Layer 2 - Secure perimeter**: Secure perimeter defence systems include full thermal and standard camera coverage, smart fencing, visitor movement analysis, crash barriers and 24/7 guard patrols.
- **Layer 3 - Building access**: Visitors are authenticated using badge readers together with biometrics, including iris scans before access through secure doors is permitted.
- **Layer 4 - SOC**: Google's security operations center (SOC) monitors the data center 24/7.
- **Layer 5 - Data center floor**: Access to the data center floor is strictly "as needed". All data is encrypted at rest. Rather than storing each user's data on a single machine or group of machines, Google distributes all data - including Google's own corporate data - across many computers in different locations Data is chunked and replicated across multiple systems to avoid any single point of failure. Google names these data chunks randomly for additional security, making them unreadable to the human eye.
- **Layer 6 - Secure disposal of data storage devices**: Google rigorously tracks the location and status of each hard drive in its data centers. Hard drives that have reached the end of their lives are destroyed in a thorough, multi-step process to prevent access to data.

More information about security of Google's data centers can be found here.

- We **limit access** to Google Analytics Data containing any personal data to Google personnel who need it to do their jobs:
  - **Infrastructure Security Personnel.** Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Processor Services, and responding to security incidents.
  - **Access Control and Privilege Management.** Administrators and users of Google's advertising and analytics products must authenticate themselves via a central authentication system or via a single sign on system in order to use the products.
  - **Internal Data Access Processes and Policies – Access Policy**. Google's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorised persons to access data they are authorised to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording. The systems are designed to detect any inappropriate access. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimise the potential for unauthorised account use.

- Google has also earned **ISO 27001 certification** for the systems, applications, people, technology, processes and data centers serving Google Analytics, as demonstrated in the published certificate available here.

Pseudonymity of Google Analytics Data

To the extent Google Analytics Data for measurement transferred by website owners is personal data, it would have to be regarded as **pseudonymous**. The Google Analytics Terms of Service (and the GA Terms for the premium version, Google Analytics 360) mandate that no data be passed to Google that Google could use or recognize as personally identifiable information, i.e. information that could be used on its own to directly identify, contact, or precisely locate an individual (see here). Access of any third party to the Google Analytics Data will therefore generally not put that party in a position to identify the data subject based on that data. The existence of any additional information held by website owners or third parties that could enable attribution to a specific data subject as well as how and where such additional information is stored and the technical and organisational measures to which it is subject may vary greatly among website owners.

Specifically:

- Google Analytics customers have full rights over their Google Analytics Data and moreover, the cookies set by Google Analytics for measurement are **first party cookies**, which means that data subjects' cookie values will be different for each Customer (i.e. there is not a single Google Analytics cookie ID per user that is used on all sites using Google Analytics). Google Analytics customers have control over whether they collect any additional information, where they store it, how they protect it and whether it is shared with or made available to Google.
- To the extent the IP-addresses contained in Google Analytics Data constitute personal data, any additional information held by internet access service providers in the EU that could enable attribution of these IP-addresses to a natural person are protected by technical and organisational safeguards, upheld by these providers, which will differ from provider to provider.

Optional Technical Measure

In addition to the above measures, website owners can use **IP-Anonymization** to instruct Google to anonymize all IP-addresses immediately after they are collected, thereby contributing to **data minimisation**. If used, at no time is the full IP-address written to disk as all anonymization happens in memory nearly instantaneously after the request has been received.

All of the above mentioned measures were in place prior to the ruling and therefore also existed during the time it took to update the terms.

Conclusion

We believe, taking into account the circumstances of the transfers the type and format of the data and the above described measures that are put in place, that U.S. law does not impinge on the adequate level of protection guaranteed by the SCCs that Google LLC enters into with the website owners.

Upon their publication, we have also reviewed the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and we were encouraged by the fact that measures outlined above are explicitly recommended as supplementary measures in Annex 2 of the Recommendations, inter alia:

- Legal review of data requests, point 112
- Notification of customers before disclosure, point 99
- Transparency Report on data requests, point 129

- Policy on handling data requests, point 122
- Encryption, points 79, 84
- Strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, point 131
- Adoption of strict data security and data privacy policies based on ISO norms, point 135
- Pseudonymity, point 80
- Data minimisation, point 131

29. If you concluded that the Recipients (in particular Google LLC) cannot guarantee the fulfilment of the contractual obligations as laid out in the SCC, have you considered the implementation of supplementary measures and if yes, which one(s)? Have you checked that these supplementary measures can be implemented in practice and that there is nothing in the third country legislation that prevents the Recipients from doing so in order to ensure that the level of data protection of natural persons guaranteed in the EEA is not undermined? Please describe the result of this assessment and the reasons for your conclusion in detail.

Please see our response to question #28.

30. If you base the international data transfers on a derogation pursuant to Article 49 (1) GDPR, please explain which derogation it is based on and how the use of this derogation is in compliance with the right to data protection pursuant to Article 8 of the Charter of Fundamental Rights.

As far as we are aware, website owners do not base any international data transfers on a derogation pursuant to Article 49(1) GDPR.

31. If you keep transferring data despite the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, have you notified your competent supervisory authority? To our knowledge, we have not received such a notification.

Please see our response to question #28.