Datatilsynet

TELENOR ASA
Postboks 800
1331 FORNEBU

By email to
eirik.h.andersen@telenor.com
tonje.orseth@telenor.com

Your reference	Our reference	Date
	20/03771-17	26.07.2023

Decision – Google Analytics – Telenor ASA

1. Introduction

The Norwegian Data Protection Authority ("Datatilsynet, "Norwegian SA", "we", "us", "our") is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation ("GDPR")[1] in Norway.

We refer to our advance notification of a reprimand to Telenor ASA ("Telenor", "you", "your") for having breached Article 44 GDPR, dated 28 February 2023. We also refer to the response to our advance notification, submitted by Telenor on 28 March 2023.

The present decision has been taken in accordance with the cooperation mechanism set out in Article 60 GDPR, in cooperation with the concerned supervisory authorities.

2. Decision

Pursuant to Article 58(2)(b) GDPR, we issue a reprimand to Telenor for having transferred personal data to a third country without complying with the conditions laid down in Chapter V GDPR, in violation of Article 44 GDPR.

3. Facts and background of the case

3.1 101 complaints from noyb – European Center for Digital Rights

Following the Court of Justice in the European Union ("CJEU") ruling on 16 July 2020 in *C-311/18 – Facebook Ireland and Schrems* ("Schrems II judgment"), noyb – European Center for Digital Rights ("noyb") lodged 101 complaints to several data protection authorities in the European Economic Area ("EEA"). All complaints concerned different European websites' use of Google Analytics ("GA") or Facebook Connect.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2018] L 119/1.

Based on the Schrems II judgment, noyb's complaints claim that the European websites' integration of Google Analytics and Facebook Connect causes European citizens visiting the websites to have their personal data transferred to the U.S. without a valid basis for transfer pursuant to Chapter V GDPR.

To ensure cooperation between every complaint-receiving supervisory authority ("SA") in the handling and enforcement of the 101 complaints, the European Data Protection Board ("EDPB") established a task force. This task force held regular meetings to organise and coordinate the complaints-handling process, and it has functioned as a forum for relevant discussions related to the subject matter of the complaints. It has also produced written documents, such as the questions provided to you in the order to provide information. Additionally, the task force prepared an order to provide information to Google in relation to the processing of personal data in Google Analytics.

Please note that all SAs participating in the task force have done so on a voluntary basis, and that SAs in no way are bound by the work of, or conclusions reached by, the task force.

3.2 Google Analytics

According to Google, "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. The analytics services are a popular category of service offered by multiple providers and are considered by many as an essential tool for operating a website. Website owners may use web analytics services such as Google Analytics to help them understand how their users interact with their site and services."[2]

3.3 Complaint against Telenor

On 17 August 2020, noyb lodged a complaint against the website www.telenor.com ("the Website") with the Austrian Data Protection Authority ("DPA"). In accordance with Article 80(1) GDPR, noyb is representing the data subject in Austria ("the complainant").

Pursuant to Article 4(23)(b), the processing of personal data subject to the complaint was assumed to be cross-border in nature. As Norway is the place of Telenor's central administration in the EEA, its main establishment within the meaning of Article 4(16)(a) GDPR is in Norway. In accordance with Article 56(1) GDPR, The Austrian DPA therefore transferred the complaint to the Norwegian SA.

On 17 August 2020, the complainant visited the Website while being logged in to the Google account associated with their email address. As a controller, Telenor had embedded the HTML code for Google Services, including Google Analytics, on the Website. The use of Google Analytics is subject to the *Google Analytics Terms of Service* and the *Google Ads Data Processing Terms*. According to the terms, Google is the contractual partner of the controller, processes personal data on behalf of the controller, and qualifies as the controller's data processor under Article 4(8) GDPR.

[2] Statement by Google, 9 April 2021.

In the course of the complainant's visit on the Website, Telenor processed the complainant's personal data – at least the IP address and cookie data. The complainant alleges that according to the HTTP Archive format ("HAR")[3] data of the Website visit provided by them, some of this data was transferred to Google. Pursuant to point 10 of the *Google Ads Data Processing Terms*, Telenor has agreed that Google may store and process personal data

> *"in the USA or any other country in which Google or any of its Subprocessors maintain facilities."*

The complainant maintains that such a transfer of their personal data from Telenor in the EEA to Google or its sub-processors in the USA (or any other non-EEA country) requires a legal basis under Article 44 *et seqq.* GDPR.

As the CJEU invalidated the "EU-U.S. Privacy Shield" decision in the Schrems II judgment, Telenor can no longer base the data transfer to Google in the U.S. on an adequacy decision under Article 45 GDPR. Telenor may also not base the data transfer on standard data protection clauses under Article 46(2)(c) and (d) if the third country receiving the personal data does not ensure adequate protection, under EU law, of the personal data transferred pursuant to those clauses.

In the Schrems II judgment, the CJEU explicitly found that further transfers to companies that fall under 50 U.S. Code § 1881a ("FISA 702") violate the relevant Articles in Chapter V GDPR, Article 7 and 8 and the essence of Article 47 of the Charter of Fundamental Rights of the European Union. Any further transfer of personal data would therefore violate the fundamental right to privacy, data protection and the right to an effective remedy to a fair trial.

Google qualifies as an *electronic communication service provider* within the meaning of 50 U.S. Code § 1881(b)(4). As such, they are subject to U.S. intelligence surveillance under FISA 702. As apparent by the "Snowden Slides" and Google's own Transparency Report, Google is actively providing personal data to the U.S. government under 50 U.S. Code § 1881a.

Consequently, Telenor is unable to ensure an adequate protection of the complainant's personal data that is transferred to Google. Nevertheless, as of 12 August 2020, Telenor and Google have attempted to rely on standard data protection clauses for data transfers to the U.S., as evidenced by point 10.2 of the *New Google Ads Data Processing Terms*.

Such practice ignores the Schrems II judgment, which puts Telenor under a legal obligation to refrain from transferring the complainant's personal data – or any other personal data – to Google in the U.S. More than one month after the judgment, Telenor had still not refrained from this processing.

[3] HAR is a JSON-formatted archive file format for logging a web browser's interaction with a website.

In its complaint, noyb requests that the NO SA fully investigates the complaint under Article 58(1), immediately imposes a ban or suspension of any data flows from Telenor to Google in the U.S., and imposes an effective, proportionate and dissuasive fine against Telenor under Article 83(5)(c).

3.4 The Norwegian Supervisory Authority's investigation

Following noyb's complaint and the subsequent transferral of the complaint from the Austrian SA to the Norwegian SA, we sent Telenor an order to provide information on 18 December 2021. The questions in the order to provide information were prepared by the aforementioned EDPB task force. Telenor asked for an extension on the deadline to reply to the order to provide information, and as per Telenor's request, we extended the deadline from 25 January 2021 to 8 February 2021. Telenor submitted its response to the Norwegian SA on 8 February 2021.

3.4.1 Telenor's response to the order to provide information

Controllership, purpose and use of Google Analytics:
Telenor stated that the decision to embed Google Analytics on the Website was made by Telenor. As such, Telenor is the data controller. Google is a data processor in the use of Google Analytics on the Website, pursuant to the *Google Analytics Terms of Service* and *Data Processing Terms* applicable to Google Analytics.

Telenor also stated that the Website is aimed at website visitors internationally, and that therefore, data subjects from several EEA states may systematically have been subject to processing through Google Analytics on the Website.

Google Analytics was implemented before the Schrems II judgment and remained active on the Website up until 15 January 2021. On that date, Telenor completed a planned disabling of the tool as part of a revamp of the site and move to a new CMS system. At the time you responded to our order to provide information, the use of Google Analytics was decommissioned. Google Analytics was embedded on the Website to provide basic, aggregated website analytics data about the use of the site in order to optimise and improve the site layout and content. At the time Google Analytics was chosen, it was deemed a basic and easy-to-implement solution that provided the necessary analytics functionalities to cover Telenor's minimal needs.

Data localisation:
According to the information available to you, no data localisation options, including to the U.S., has been or is available when using Google Analytics. Based on information provided by Google, the data collected by Google Analytics is processed in the data center closest to the location of the user. As Google does not offer Google Analytics with region-based processing, it cannot, according to Google, be accurately determined in which country/countries Google processes such data. Google's data centers are located in several countries in North America, South America, Europe and Asia.[4]

[4] https://www.google.com/about/datacenters/locations/, last visited 5 June, 2023.

Data collection:
As regards data collection using Google Analytics, you state – referencing the *Google Ads Data Protection Terms: Service Information* – that the personal data elements collected by Google Analytics are limited to online identifiers, including cookie identifiers, internet protocol ("IP") addresses, device identifiers and client identifiers. To reduce the privacy implications of the Website's monitoring and IP address collection, you have enabled the IP anonymisation feature of Google Analytics. It is your understanding that the identifiers listed above cannot be regarded as personal data in the context of your use of Google Analytics, as the IP anonymisation process has severed any link to an individual.

You have stated that the IP anonymisation feature of Google Analytics ensures that IP addresses from website visitors are anonymised (by removing the last octet of IPv4 addresses or removing the last 80 bits of IPv6 addresses) at the earliest possible time after data has been received by Google Analytics (i.e., the Analytics Collection Network), and before any subsequent processing takes place, including access to the data by you.

According to information you have received from Google, the IP anonymisation process takes place in the memory of the recipient webservers of Google Analytics only (i.e., data is never written to disk) and is deleted from memory rapidly. Only an extremely limited number of Google Data Center personnel have access to the relevant server memories, and such access is to your understanding never utilised for any direct processing purposes, only for technical system maintenance by Data Center personnel. Google logs all such access. Google has informed you that it would not be possible to extract such data following a potential legally binding authority request.

You assert that the only personal data collected by Google Analytics on the Website and subsequently processed by you in the context of Google Analytics has been IP addresses.

Transfers of personal data to third countries:
In late August 2020, you initiated a review project to assess agreements entered into by Telenor in light of the Schrems II judgment. You considered the Schrems II judgment to apply to your use of Google Analytics, as the agreement is entered into with Google as a U.S. data processor of Telenor.

Any transfer of personal data to Google is carried out subject to the SCC's Module Two.

You have not carried out a thorough review of potential third country legislation, as it, according to information from Google, is not possible to determine the exact location of processing. This is due to Google applying the user's proximity to the data center as one of the primary deciding factors for the processing location. You are aware of the CJEU's interpretation of U.S. law, specifically FISA 702 and Executive Order 12333, and your focus has therefore been to ensure that appropriate technical and organisational measures are implemented to prevent unauthorised access to personal data. Moreover, Google has confirmed that it will not be possible for foreign authorities to gain access to the IP addresses collected prior to the anonymisation process.

You have summarised the supplementary measures implemented by you and Google as follows.

Firstly, Google has established policies and procedures for handling authority requests for user data from authorities across the world. According to Google, any request for customer data is handled by a team of qualified lawyers, and the requests are carefully reviewed to make sure they satisfy requirements in applicable laws.

Secondly, Google has, through their IP anonymisation feature, made available a technical measure preventing the full IP addresses from being processed in manner that allows access by public authorities. This process is coupled with strict controls regarding privileges for access to the production environment of the Analytics Collection Network.

In terms of supplementary measures implemented by you, you have applied a redaction script as an additional measure on the Website to prevent personal data unintentionally being shared with Google.

You are of the opinion that the SCC's, in addition to the supplementary measures adopted by Telenor and Google, would guarantee the contractual obligations as laid out in the SCCs.

Your website analytics at present:
According to your privacy policy, you now use Adobe Analytics as your web analytics vendor. Adobe Analytics processes IP addresses before deletion to allow geo-locating on municipality and city level, which allows you to filter your anonymous web visitors by municipality and city. IP addresses are not visible to you because they are automatically removed after processing.

Adobe Analytics is a Software-as-a-Service (SaaS) that leverages cloud hosting. They use Adobe-owned servers in a Data Processing Center (DPC) in London for processing and storage.[5]

3.4.2 Advance notification of a reprimand

The information provided by Telenor did not mitigate our concerns regarding the lawfulness of the use of Google Analytics. On 28 February 2023, we therefore sent you an advance notification of our *intent to issue a reprimand to Telenor for having transferred personal data to a third country without complying with the conditions laid down in Chapter V GDPR, in violation of Article 44 GDPR.*

3.4.3 Telenor's response to the advance notification

The Norwegian SA received Telenor's response to the advance notification on 28 March 2023. We will go through Telenor's arguments in more detail below, but the main legal arguments can be summarised as follows:

[5] https://www.telenor.com/privacy-policy/, last visited 5 June, 2023.

- The Norwegian SA has not sufficiently distinguished the different roles of the parties, i.e., when Google is a controller and when Google is a processor.
- The Schrems II judgment related to the transfer of all or part of the personal data in clear text, which is substantially different from the processing activities in the present case.
- The Norwegian SA has not documented a clear preponderance of probability relating to the findings of transfers to the U.S. and that FISA 702 applies in practice. When issuing a reprimand stating that provisions of the GDPR have been infringed, European Convention on Human Rights ("ECHR") Article 6 requires that there must be established a clear preponderance of probability.
- The processing of personal data in question does not constitute cross-border processing.
- For visitors within the EEA, the IP address is not transferred to the U.S., as the IP address of European visitors are pseudonymised through the IP anonymisation in the memory of Google servers located in Europe.
- Telenor had a valid legal basis for transfer. FISA 702 does not apply to Google Analytics in practice, and the transfer did not constitute an infringement of Chapter V GDPR.

3.5 Statement by Google

On behalf of the EDPB taskforce, the Austrian DPA sent a questionnaire to Google regarding Google Analytics and supplementary measures. In a letter dated 9 April 2021, Google responded to the questions. Google lists the legal, organisational and technical supplementary measures they adopted after the Schrems II judgment. According to their statement, Google has implemented a legal review of data requests, notification of customers before disclosure, and publishes a Transparency Report on data requests. Additionally, they have, inter alia, implemented measures in relation to encryption, data access, pseudonymity, data minimisation, and adopted strict data security and data privacy policies.[6]

4. Relevant GDPR requirements

4.1 Material and territorial scope

Article 2(1) GDPR provides that the Regulation applies to "the processing of personal data wholly or partly by automated means (…)".

What constitutes "personal data" is defined in Article 4(1) GDPR as:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier (...)".*

Article 4(2) GDPR defines "processing" as:

[6] Statement by Google, 9 April 2021.

"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

As regards the territorial scope of the GDPR, Article 3(1) establishes that the Regulation:

"applies to the processing of personal data in the context of the activities of an establishment of a controller (...) in the Union, regardless of whether the processing takes place in the Union or not."

4.2 Controller and processor

Pursuant to Article 4(7) GDPR, "controller" means:

"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (...)".

Pursuant to Article 4(8) GDPR, "processor" means:

"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

4.3 Cross-border processing

Article 4(23) stipulates that cross-border processing means either:

(a) *"Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member state; or*

(b) *Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."*

4.4 Transfers of personal data to third countries

Transfer of personal data from the EEA to third countries is regulated by Chapter V GDPR.

Pursuant to Article 44 GDPR, the general principle for transfers reads as follows:

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

Chapter V GDPR further foresees different tools for transfer to ensure an equivalent level of protection for natural persons as provided for in the EEA and required by Article 44 GDPR.

Relevant tools for transfers:

Adequacy decisions, Article 45(1) GDPR:

> *"A transfer of personal data to a third country (...) may take place where the Commission has decided that the third country (...) in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation."*

Appropriate safeguards, Article 46(1) GDPR:

> *"In the absence of an [adequacy decision] (…) a controller may transfer personal data to a third country (...) only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."*

Pursuant to Article 46(2)(c), the appropriate safeguard may be provided for, without requiring any specific authorisation from a supervisory authority, by

> *"Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)."* ("SCCs")

Schrems II judgment:

In the Schrems II judgment, the CJEU declared the "EU-U.S. Privacy Shield" decision pursuant to Article 45(1) GDPR invalid, as American intelligence and surveillance laws undermined the level of protection for data subjects in the EEA guaranteed by the GDPR. Equally, the CJEU stated that the use of SCCs may not in themselves be sufficient to ensure that level of protection, in which case the implementation of supplementary measures may be necessary. The purpose of such supplementary measures is to ensure that personal data is not processed beyond what is necessary in a democratic society. The EDPB has issued recommendations on supplementary measures[7] ("EDPB Recommendations").

[7] See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available on https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, last visited 5 June 2023.

5. Our assessment of the case

5.1 Main legal questions

There are three main legal questions arising from this case, namely;

i) Whether or not personal data was processed in the context of the Google Analytics tool,
ii) Provided that personal data was processed, whether or not this personal data was transferred to the U.S., and
iii) Provided that the personal data was processed and transferred to the U.S., whether or not this transfer infringed Chapter V GDPR, also considering the Schrems II judgment.

In the following, we will assess these three questions in addition to other relevant elements of the case.

5.2 Scope of the Norwegian SA's investigation

Our investigation into your use of Google Analytics is limited to the time period from the CJEU's Schrems II judgment to your discontinuation of Google Analytics, i.e. between 16 July 2020 and 15 January 2021 – a time period of six months.

We have not investigated Google's potential further processing of the personal data subject to the complaint, as this was not within the scope of the complaint.

Furthermore, we have not investigated your use of the new web analytics vendor implemented on the Website.

5.3 Whether the processing in question constitutes cross-border processing

In our order to provide information dated 18 December 2020, we laid down an assumption stating that the processing of personal data within the context of Google Analytics on the Website was cross-border in nature according to Article 4(23)(b) GDPR. This assumption was based on the fact that the Telenor Website has a global reach, attracting visitors from both the EEA and the rest of the world, and that the Website's default language is English. In line with Article 4(23)(b), we assumed that the processing of personal data through Google Analytics on the Website substantially affected or was likely to substantially affect data subjects in more than one Member state. As such, we considered the processing to be cross-border in nature.

In your response to our order to provide information dated 8 February 2021, you did not contradict this assumption. Furthermore, you also stated that:

> *"The telenor.com site is open and accessible to any website visitor from around the globe. Telenor.com is the main corporate website of the Telenor Group, the site is*

aimed at visitors from all around the globe. As such, data subjects from any European Members State may have been subject to the processing of the Tool.[8] *"*

Following this, we concluded that the processing constituted cross-border processing within the meaning of Article 4(23)(b) in our advance notification with the following statement:

"The processing of personal data on the Website substantially affects or is likely to substantially affect data subjects in more than one Member State, as the target audience of the site are customers and stakeholders of Telenor's subsidiaries internationally. Thus, the processing constitutes cross-border processing pursuant to Article 4(23)(b) GDPR.[9] *"*

In your response to our advance notification, you state that the we have not provided any grounds to substantiate why we have concluded that the processing through Google Analytics on the Website constitutes cross-border processing. You are of the opinion that there is no cross-border processing of personal data through Google Analytics on the Website within the meaning of Article 4(23)(b) GDPR.

You argue that there is a certain threshold for the processing to "substantially affect or is likely to substantially affect data subjects in more than one Member State, and that this threshold is not met in the present case. Furthermore, you state that the Website is aimed at corporations and companies and not at individual data subjects per se, and that it does not offer services or products to customers in Norway or any other country. You also state that your statistical overview shows that the number of individuals from other EEA countries who visit the website is low, and that, as per February 2023, the top three countries from which the Website was visited were Pakistan, Norway and India. In your view, this speaks to the fact that the processing does not substantially affect a significant number of data subjects in several Member States. Against this background, you are of the opinion that the processing does not constitute cross-border processing.

Article 4(23)(b) establishes two conditions that must be met in order for the processing to be considered cross-border; the processing must take place in the context of the activities of a single establishment of a controller or processor in the Union, and the processing must substantially affect or be likely to substantially affect data subjects in more than one Member State.

The starting point for the assessment of whether the processing is cross-border or not, is the processing operation itself. In this case, the processing in question is the alleged collection and subsequent transfer of personal data to a third country through Google Analytics, embedded on the Website by Telenor.

As this processing took place in the context of the activities of a single establishment of Telenor in the Union, the first condition of Article 4(23)(b) is satisfied.

[8] Response from Telenor ASA to the questions posed by Datatilsynet on 18 December 2021, p. 1, question 4.
[9] Advance notification, point 3.3.1

When it comes to the second condition, namely that the processing must substantially affect or be likely to substantially affect data subjects in more than one Member State, we agree with Telenor that not all cross-border processing activity falls within the definition of cross-border processing in Article 4(23)(b). As you state, this is also the position of the EDPB.[10] We also agree that the fact that a website is accessible to anyone in the EEA with an Internet connection does not automatically mean that cross-border processing is taking place.

However, the processing in question does meet the threshold that Article 4(23)(b) sets out for the following reasons. As also stated in the above-mentioned EDPB Guidelines, Supervisory Authorities will interpret "substantially affects" on a case-by-case basis, taking into account the context of the processing, the type of data, the purpose of the processing, as well as several listed factors.[11]

Going off the list of factors, the collection and subsequent transfer of personal data to a third country through Google Analytics on the Website can have "unlikely, unanticipated or unwanted consequences for individuals".[12] A person visiting the website might not be aware that their personal data is being collected and subsequently transferred to the U.S., where it can be subject to U.S. intelligence surveillance. This type of processing is intrusive, uncomfortable, and is likely to substantially affect the data subjects.

Furthermore, the processing in question does not happen in plain sight and is difficult to follow for an individual. Again, some visitors might not even be aware that their personal data were being collected through Google Analytics when visiting the Website.

Moreover, the processing clearly affects data subjects in more than one Member State. The Website is the main corporate website of the Telenor Group, which has owner interests and shareholders in several countries inside and outside the EEA. Accordingly, the website is aimed at visitors from all around the globe, including the EEA, and arguably especially at visitors from countries where the Telenor Group has subsidiaries, which includes EEA countries such as Sweden and Denmark. Your statistical overview also demonstrates that Norway, Sweden, Denmark and Germany are among the top ten countries from which the Website is visited as per February 2023.[13]

Taking this into account, we have found the processing in question to substantially affect, or to be likely to substantially affect, data subjects in more than one Member State. As such, the processing constitutes cross-border processing within the meaning of Article 4(23)(b).

5.4 Competence of the Norwegian Supervisory Authority

[10] Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority, Version 2.0, Adopted on 29 March 2023, para. 7.
[11] Ibid, para. 12.
[12] Ibid, bullet point eight.
[13] Annex 1from Telenor: «Telenor.com | Besøk topp 50 land | Februar 2023».

As per point 5.3, the processing of personal data constitutes cross-border processing within the meaning of Article 4(23)(b).

Norway is the place of Telenor's central administration in the EEA. As such, the main establishment of Telenor, within the meaning of Article 4(16)(a) GDPR, is in Norway. The Austrian SA therefore transferred the complaint to the Norwegian SA in accordance with Article 56(1) GDPR.

Therefore, the Norwegian SA is the competent SA and acts as the lead supervisory authority in this case.

5.5 Controller and processor

5.5.1 General overview

Controller:
The complainant has identified Telenor as the controller in its complaint. In your response to us, you stated that the decision to embed Google Analytics on the Website was made by Telenor.

Therefore, we find it to be undisputed and clear that you "determine(d) the purposes and means of the processing of personal data" subject to the complaint, and therefore acted as a controller pursuant to Article 4(7) GDPR.

Processor:
The complainant further identifies Google in the U.S. as Telenor's processor in relation to the personal data processed in Google Analytics. In your response to us, you state that Google is the data processor in the use of Google Analytics on the Website, as stated in the *Google Analytics Terms of Service* and *Data processing Terms* applicable to Google Analytics. Furthermore, you have entered into SCCs with Google, using Module Two of the SCCs.

Against this background, we find it to be undisputed and clear that Google "processe(d) personal data on behalf of" you within the context of Google Analytics, and therefore acted as a processor pursuant to Article 4(8) GDPR.

Seeing as neither the complainant nor you have addressed Google Ireland Limited in relation to the processing of personal data in question, we have not investigated if, and to what extent, they are involved in the processing. Thus, we are assessing the case on the premise that a data subject in Austria visited the Website, and whether or not the complainant's personal data subsequently was unlawfully transferred from the EEA to the U.S. through your use of Google Analytics.

5.5.2 The roles of Telenor and Google

In your response to our advance notification, you claim that the Norwegian SA does not distinguish between data elements collected by Google as a data processor for Telenor in its

provision of Google Analytics, and personal data collected by Google as a data controller with respect to its provisioning of services to data subjects.[14]

You state that you are responsible as a controller and data exporter for the data collected through the use of Google Analytics, namely:

- IP addresses;
- Unique identifier that identifies the browser/device used to visit the Website ("cookie ID");
- Unique identifier used to identify the Website operator (in this case the account ID of Telenor);
- Address and HTML title of the Website (i.e. Telenor.com + subdomains); and
- Information on browser, operating system, screen resolution, language settings as well as date and time of access to the Website.

Furthermore, you state that where Google acts as data controller, any transfer of personal data by Google falls outside the responsibility of Telenor. Google is the controller when it comes to the processing of personal data that happens when a visitor visits the Website while being logged into their account. Where a visitor is logged into their account in the browser, this is a processing activity that occurs in the relationship between Google as a data controller and the individual using Google services such as a Google account. These processing activities occur by virtue of a contract entered into between Google and that particular user, and falls outside the processing activities and responsibilities of Telenor.

The Norwegian SA agrees with Telenor that there likely exist situations where Google is an independent or joint controller in relation to analytics data. However, our proceedings only concern the processing carried out in Google Analytics by Google as a data processor for Telenor, i.e. the above list of data collected through your use of Google Analytics. The current case does not concern how Google processes Google account data.

Nonetheless, in assessing whether the data in scope constitutes personal data, it is necessary to assess whether the data subject is *identifiable*, and this includes looking at *all* possibilities Google may have for identification.

5.6 Whether personal data was processed in Google Analytics

In order for the GDPR to apply, "personal data" pursuant to Article 2(1) must be processed. Therefore, the complainant needs to be identified or identifiable, directly or indirectly, by the data processed in Google Analytics.

Online identifiers, such as IP addresses and information stored in cookies, can be used to identify a user, in particular when combined with similar types of information. This is illustrated by Recital 30 GDPR, whereby:

[14] Telenor's Response to Advance notification of a reprimand p. 5.

> *"Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers (…). This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."*

In order to assess whether the complainant is identifiable through the data processed in Google Analytics, thus making it personal data pursuant to Article 4(1) GDPR, it must be assessed how Google Analytics works, and whether the complainant is identifiable to Telenor or Google.

Telenor has implemented Google Analytics on the Website by inserting a JavaScript command (a tag), which was specified by Google, into the source code of the Website. While the page is loading in the browser of the visitor, the JavaScript code is now loaded from the servers of Google and executed locally in the visitor's browser. A cookie, under the domain of the website operator, is set by this JavaScript code. Among other elements, a permanent unique identifier is set in the cookie value. This unique identifier is generated and managed by Google. Telenor, however, can read the value.

On the basis of the HAR data, the following data was processed when the complainant visited the Website:

- Unique identifier(s) that identifies the browser/device used to visit the Website, as well as a unique identifier that identifies the Website operator, in other words the Google Analytics account ID of the Website operator,
- Address and HTML title of the Website,
- Information on browser, operating system, screen resolution, language settings, as well as the time and date the Website was accessed by the complainant,
- The complainant's IP address.

As regards IP addresses, it is worth noting that the anonymisation process is carried out on Google's servers. In other words, the IP address is sent to Google before it is anonymised.

The CJEU has already ruled that IP addresses in most circumstances are to be considered as personal data.[15] In our view, IP addresses still qualify as personal data even though the means of identifiability lie in third entities. Additionally, IP addresses can be combined with further elements in order to make the data subject identifiable.

As these unique identifiers are set with the specific purpose to differentiate individuals, where differentiation was not possible before, they contribute to making the individual identifiable. In this regard, we note the findings of the Austrian SA in a similar case, also referring to a decision by the European Data Protection Supervisor, that these Google Analytics identifiers in principle qualify as personal data.[16]

[15] See judgments C-597/19 and C-582/14.
[16] See page 27 of the decision in question, available on https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rzt.pdf, last accessed 13 June 2023.

Even if unique identifiers per se would not make individuals identifiable, they can also be combined with further elements.

In this case and as already mentioned, the IP address and cookie identifiers were combined with, *inter alia*, the address of the specific website the complainant visited, the time and date of the website visit, as well as metadata about the browser and operating system. While the latter may appear seemingly innocuous, the combination of settings and parameters of the browser and the operating system may sometimes be sufficiently unique to lead to so-called device fingerprinting.

Therefore, both you and Google have several elements that combined can enable you to single out visitors, including the complainant, on the Website where Google Analytics was implemented. The GDPR does not require the controller or processor to know the name or physical address of the visitor – it suffices that it would be possible to identify an individual, also relying on additional data from other sources. As illustrated by Recital 26, the *singling out* of individuals may be sufficient to make them identifiable.

Additionally, the complainant was logged into their Google account at the time the Website was visited. As shown by Google's statement, the implementation of Google Analytics on a website enables Google to receive information that a specific Google account has visited that website. Even though Google states that certain settings must be enabled in order for them to process such information, it must be noted that the definition of personal data is based on whether it is technically possible to identify an individual, not whether a party chooses to do so in practice. In our understanding, tweaking the relevant settings would affect the latter aspect, but not necessarily the former.

Furthermore, the fact that you consider Google your data processor and have entered into a data processing agreement with them in the context of your use of Google Analytics, would also seem to indicate that the contracting parties are of the opinion that personal data is being processed.

Taking all of this into account, as a result, we find that the data in question is to be regarded as personal data within the meaning of Article 4(1) GDPR.

5.7 Whether a transfer of personal data to the U.S. has taken place

In your response to our advance notification of a reprimand, you state that personal data in clear text was not transferred to the U.S. for processing in Google Analytics. You had implemented the IP anonymisation feature in Google Analytics. When applying this feature, the IP address will be transmitted to the Google server closest to the Website visitor for IP anonymisation and subsequent return of the cookie ID. The IP anonymisation process occurs in the memory of the server and results in an instantaneous deletion of the IP address. Google has confirmed that it is not possible for any public authority to gain access to the IP address prior to the IP anonymisation process.

You further state that for visitors within the EEA, the IP address is not transferred to the U.S., as the IP Addresses of European visitors are pseudonymised through the IP anonymisation in the memory of Google servers located in Europe. The IP address of EEA visitors is thus not exported out of the EEA, only the cookie ID. As regards Website visitors from outside the EEA, you state that you will be a data exporter under Chapter V GDPR in situations where the IP address is transferred for IP anonymisation to another third country, i.e. when the closest server location to the visitor is in a third country.

Furthermore, you state that, as a result of the Google Analytics network being hosted within the U.S., data elements such as cookie ID, website visited, operating system, device type and screen resolution will be exported to and processed within the U.S. You are responsible under Chapter V GDPR for the export of these data elements.

We find that there is no dispute surrounding the fact that all data processed in Google Analytics eventually ends up in the U.S. – some data in clear text, and other pseudonymised. We further agree that the IP addresses of EEA visitors are most likely truncated on a European server before the cookie ID is transferred to the U.S.

However, the Website has many visitors from different third countries.[17] When a visitor from a third country closer to a non-EEA data centre visited the Website, they are never connected to a European server, but are connected to a Google server in a third country instead.[18] As such, the IP address of the visitor is transferred to a third country before it can be anonymised. Pursuant to Article 3(1) GDPR, the Regulation "applies to the processing of personal data in the context of the activities of an establishment of a controller (…) in the Union, regardless of whether the processing takes place in the Union or not." This means that the GDPR applies regardless of where the data subject is located.[19]

In any case, as explained above, there are several data categories which in themselves or in combination constitute personal data, including the visitor's unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system. Even if IP addresses are disregarded, we find that the totality of the data transferred still constitute personal data.

Against this background, we find that personal data was transferred to the U.S. through the use of Google Analytics on the Website.

5.8 Whether the transfer of personal data infringed Article 44 et seqq. GDPR

In your response to our advance notification, you state that Telenor had a valid legal basis for transfer, that the data was not at risk for authority requests under FISA 702, that the transferred data were trivial in nature and would not have entailed an infringement of the

[17] Annex 1from Telenor: «Telenor.com | Besøk topp 50 land | Februar 2023».
[18] https://support.google.com/analytics/answer/11598602, last visited 14 June 2023.
[19] See also EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available on https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, which on p. 10 states the following: "However, geographical location is not important for the purposes of Article 3(1) with regard to the place in which processing is carried out, or with regard to the location of the data subjects in question."

fundamental rights of the individual if accessed by the authorities, but rather a mere interference.

As the processing activities took place within the U.S., Telenor and Google had entered into the SCCs for processors as the legal basis for transfer of personal data to the U.S. Under the SCC, Telenor acted as data exporter and Google acted as data importer. You disagree with our advance notification, where we held that the use of SCCs generally will not be sufficient for transfer of personal data to an organisation in the U.S. subject to FISA 702. You further maintain that Telenor and Google had implemented adequate supplementary measures to protect the data.

You state that although Google has been subject to access requests in general, this is not a relevant prior instance of requests for access. Furthermore, Google has confirmed publicly that during the 15-year period during which Google Analytics has been available, Google had, as of 19 January 2022, not received a single FISA request for such data. You therefore contend that FISA 702 did not apply to Google Analytics in practice.

Google LLC, as a data importer in the U.S., classifies as an electronic communications service provider within the meaning of 50 U.S. Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to FISA 702, and is therefore obliged to provide the U.S. government with personal data when FISA 702 is invoked.

In Schrems II, the CJEU held that the U.S. surveillance programs based on FISA 702, E.O. 12333 and Presidential Policy Directive 28 do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programs based on those provisions cannot be considered to be limited to what is strictly necessary.[20] In other words, the CJEU found that the level of protection of personal data when transferring personal data to the U.S. is not essentially equivalent to that guaranteed in the EU.

As pointed out by Telenor, it is important to distinguish between interferences with, and infringements of, fundamental rights. Laws on governmental access which do not meet the requirements of proportionality and necessity constitute infringements by definition, and the CJEU found that U.S. surveillance laws fall within this category.

As an exception from this, we have stated in our public-facing guidance that transferring personal data *that are publicly available* to third countries without supplementary measures may possibly not constitute an infringement. This is clearly not relevant in this case, as the personal data in question are not publicly available.

Worth noting is that neither the wording of Chapter V GDPR, the Schrems II judgment, nor the practice of other EEA data protection authorities permit a so-called 'risk-based approach' under which data can be transferred without supplementary measures if they are not likely to be intercepted (for example if the controller believes that the data are not 'interesting' to third

[20] Schrems II judgment, para. 184.

country authorities) or if the consequences of interception are perceived by the controller as being small (for example due to the perceived nature of the data).

Furthermore, the CJEU points out that when transferring personal data on the basis of SCCs, in order to ensure that the level of protection is not undermined, it is necessary to also examine the third country's legal system with regard to access by third country authorities.[21] Where problematic legislation on governmental access prevails, it is necessary to adopt supplementary measures in addition to the SCCs to uphold the level of protection.[22]

For transfers of personal data to the U.S., it is clear that problematic legislation prevails over the SCCs, and thus supplementary measures are required unless an exception applies.

However, the EDPB has since the Schrems II judgment stated that if there is no reason to believe that the problematic legislation in question applies in practice, adopting supplementary measures is not necessary. Though this 'permittance' was formulated by the EDPB after Telenor stopped using Google Analytics, Telenor should be able to benefit from it if the conditions are met.

Concomitantly, the EDPB has specified what is required in this situation and emphasised that controllers remain accountable for their assessments:

> *You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below.*[23]

Furthermore, the EDPB has stated as follows:

> *You must however note that the absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the Article 46 GDPR transfer tool that allows the transfer to proceed without supplementary measures.*[24]

It is important to note the fundamental difference between situations where there is no reason to believe that personal data are in practice covered by problematic legislation (in Norwegian: *ingen grunn til å tro at loven i praksis får anvendelse*), and situations where personal data are in fact within scope of the legislation, but there is no reason to believe that authorities will utilise the access they are granted under that legislation (in Norwegian: *ingen grunn til å tro*

[21] Ibid., para 104.
[22] Ibid., para. 133.
[23] EDPB recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, para 43.3, available on https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en,
[24] Ibid., para. 47.

at loven i praksis vil bli anvendt). Only the former fulfils the criteria set out in the EDPB guidelines, while Telenor's arguments appear to be tied to the latter.

To be clear, the wording of FISA 702 indicates that the personal data in this case are within scope of the problematic legislation. Telenor has failed to demonstrate and document that FISA 702 is not interpreted and/or applied in practice so as to *cover* that personal data, and Telenor has not documented that it has examined the experience of other actors operating within the same sector and/or consulted the sources of information described by the EDPB. Telenor's assertion that Google has not historically received access requests regarding Google Analytics data is in itself not sufficient.

Therefore, the question at hand is whether the SCCs were supplemented by appropriate measures to prevent U.S. intelligence services processing personal data of visitors to the Website beyond what is necessary in a democratic society.

The EDPB Recommendations explain and exemplify which supplementary measures are considered by EEA supervisory authorities to be appropriate in this regard. In general, technical measures that prevent personal data being made available to the data importer in clear text would be required here.

Though it has been argued that supplementary measures are in place, it is clear that those measures do not prevent Google from having clear text access to at least some of the personal data in question, such as the combination of the visitor's unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system, again noting that the scope of personal data in this case is wider than just the IP addresses.

On this background, we find that the transfer of personal data infringed Article 44 GDPR.

5.9 Conclusion

Based on the above, we find that personal data of visitors to the Website was processed in the context of Google Analytics, that those personal data were transferred to the U.S., and that this transfer infringed Chapter V GDPR.

6. Corrective measure

The complainant requests us to impose a ban or suspension of data flows from Telenor to Google in the U.S., as well as impose an effective, proportionate and dissuasive administrative fine against you.

Seeing as your use of Google Analytics was discontinued on 15 January 2021, there is no reason to impose a ban or suspension of data flows from Telenor to Google in the U.S.

We have, however, considered whether we should exercise any other corrective powers. Taking into account all elements of the case, we find a reprimand to be an adequate and proportionate corrective measure. Pursuant to Article 58(2)(b), a reprimand is a corrective measure that SAs can issue to a controller or processor where processing operations have

infringed the GDPR. The purpose of reprimands is to indicate criticism towards the identified infringements.

In your response to our advance notification, you claim that the issuance of a reprimand requires a clear preponderance of probability, as a reprimand is to be considered as punishment under the European Convention of Human Rights ("ECHR") Article 6. You base this on the assumption that a reprimand is a "final statement of guilt" for breaching Chapter V GDPR, similar to formal warnings[25] under the Norwegian Public Administration Act. You state that this threshold is not met in the present case.

As the case currently stands, also taking as a basis the additional information you provided in your response to our advance notification, we find that there is a clear preponderance of probability that personal data, including the Website visitor's unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system, was transferred to the U.S. without sufficient supplementary measures where such supplementary measures were required.

In any case, we reject that a reprimand pursuant to Article 58(2)(b) is to be considered as punishment under the ECHR Article 6.

The European Court of Human Rights ("ECtHR") has interpreted the notion of 'criminal charge' for the purposes of Article 6 ECHR in several of its judgments, most notably in the Engel Case.[26] In that judgment, the ECtHR set out three criteria for the determination of whether a charge is 'criminal', namely:

1. the classification of the charge in national law;
2. the nature of the offence; and
3. the degree of severity of the penalty.[27]

The ECtHR further elaborated on what constitutes a 'criminal charge' in the Öztürk Case,[28] where it concluded that a penalty was criminal *inter alia* because it was punitive and intended to be deterrent.[29]

Applied to the present case, it is clear that a reprimand is not classified as a criminal law penalty under Norwegian law.

As for the degree of severity of the reprimand, it has little impact on the controller and no tangible repercussions. A reprimand cannot be considered to be a measure of any considerable severity,[30] and it is not of a punitive nature.

[25] Norwegian: "Formelle advarsler".
[26] Case of Engel and Others v. the Netherlands (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72)
[27] Ibid., para. 82.
[28] Case of Öztürk v. Germany (Application no. 8544/79)
[29] Ibid., para. 53.
[30] In this regard, it is worth noting Recital 148 GDPR, which states that a reprimand may be issued in case of a minor infringement.

Also worth noting is that under the GDPR, only administrative fines are intended to be dissuasive, pursuant to Article 83(1), in contrast to reprimands and the other corrective measures listed in Article 58(2).

As for Telenor's representations regarding formal warnings, we note that formal warnings are not listed in the Norwegian Public Administration Act Chapter IX among the administrative sanctions that constitute a 'criminal charge' in the sense of the ECHR.

7. Right of appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.[31]

Yours sincerely

Jørgen Skorstad
Director, law

Trine Smedbold
Legal Adviser

This letter has electronic approval and is therefore not signed

Copy: noyb – European Center for Digital Rights

[31] Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).