Datatilsynet

Disqus Inc.
717 Market St
San Francisco CA 94103

Your reference	Our reference	Date
	20/01801-5	02.05.2021

Advance notification of an administrative fine – Disqus Inc.

Table of contents

Postal address:	Office address:	Phone:	Fax:	Ent.reg:	Home page:
P.O. Box 458 Sentrum N-0105 OSLO	Tollbugt 3	+47 22 39 69 00	+47 22 42 23 50	974 761 467	www.datatilsynet.no/en/

1. Background

On 8 May 2020, the Norwegian Data Protection Authority ("NO DPA", "we") ordered Disqus Inc. ("Disqus", "you") to provide information regarding the processing of personal data about data subjects in Norway through the Disqus Widget, a comment widget used on multiple websites of Norwegian companies (hereinafter "the widget").

Disqus replied to the order to provide information by e-mail on 10 July 2020.

Our order to provide information was sent after a series of news articles published by the NRK, the Norwegian Broadcasting Corporation, in which NRK described how Disqus processed personal data about Norwegian users, while, according to NRK, being unaware that the General Data Protection Regulation ("GDPR") was applicable.[1]

[1] See section 3.2 for more information.

The information Disqus has provided has not mitigated our concerns regarding the processing of personal data in question and its relation to the fundamental data protection principles of lawfulness and transparency. In light of the factual circumstances of the case, the pertinent processing of personal data appears to be in breach of several of the articles of the GDPR.

We are therefore notifying you of our intent to sanction the apparent breaches with an administrative fine – see our reasoning in the paragraphs below.

The purpose of an advance notification is to ensure that the case is clarified as thoroughly as possible before an administrative decision is made, and to allow for contradiction.[2]

In other words, this is a draft decision. Before making a final decision, we will take into account Disqus' comments to this draft, which must be submitted within the time limit specified below in section 7.

2. Advance notification

In line with the Norwegian Public Administration Act section 16, we hereby provide advance notification of our intent to make the following decision:

Pursuant to article 58(2)(i) GDPR, we impose an administrative fine against Disqus Inc. of 25 000 000 - twenty five million - NOK, for

a. *having processed the personal data of data subjects in Norway, collected from the websites NRK.no/ytring, P3.no, tv.2.no/broom, khrono.no, adressa.no, rights.no and document.no, through tracking, analysing and profiling, and disclosing personal data to third party advertisers, without a legal basis pursuant to Articles 5(1)(a) and 6(1) GDPR,*

b. *failure to provide the data subjects with information in accordance with Articles 5(1)(a), 12(1) and 13 GDPR, and*

c. *failure to identify GDPR as the applicable legal framework for processing the personal data of data subjects in Norway pursuant to Article 5(2) GDPR.*

The NO DPA is the supervisory authority established in line with Article 51(1) GDPR to monitor the application of the GDPR on the territory of the Kingdom of Norway. This follows from the Norwegian Personal Data Act Section 20.

We have the powers to impose an administrative fine pursuant to Article 58(2)(i).

In the present case, we have focused our investigation on Disqus' responsibility under the GDPR as a controller being present on the websites mentioned above for the pertinent data

[2] See section 17 first para. of Act relating to procedure in cases concerning the public administration (Public Administration Act) (LOV-1967-02-10).

processing operations. However, there might be additional issues regarding e.g. the website owners' responsibility under the GDPR for admitting Disqus to their websites. The fact that some issues have fallen outside the scope of our investigation does not preclude those issues from being addressed in the future. We may decide to investigate additional issues later on, following individual complaints or *ex officio*, see the tasks and powers of the supervisory authorities laid down in Articles 57 and 58 GDPR.

3. Facts of the case

3.1 Factual background

Disqus is an American company owned by Zeta Global, which offers an online public comment sharing platform, into which users may log in and create profiles in order to participate in conversations. Advertising is the predominant business model, according to the Disqus privacy policy.[3]

Through news articles published by the NRK, we were made aware that Disqus has collected and disclosed personal data to third party advertising partners about data subjects in Norway through the Disqus widget, a comment plug-in for websites.

The online newspaper Computerworld.no has also written about the Disqus widget and data collection.[4] According to these news articles, the data were first collected through cookies that Disqus placed upon the users visit to the website running the widget. Subsequently Disqus' cookies collected personal data about the users before disclosing this personal data to multiple third party advertising partners.

Based on this information, we sent Disqus an inquiry on 8 May 2020, in which we ordered Disqus to answer ten questions, and to provide further information on the processing of personal data in question.

In your reply, received on 10 July 2020, you stated the following:

> *Neither Disqus nor its parent Zeta Global have any business operations in Norway, and as such, do not believe that the Datatilsynet has established legal jurisdiction to conduct an investigation of or take adverse action against Disqus. But, because the processing in question was the result of a good-faith error by Disqus which was promptly corrected upon its discovery, in the interests of transparency we have elected to respond to this inquiry. We maintain, however, that Disqus is not subject to the jurisdiction of the Datatilsynet.*

[3] See pt. 4 of the policy: https://help.disqus.com/en/articles/1717103-disqus-privacy-policy (Last seen 26.04.21).
[4] https://www.cw.no/artikkel/gdpr/en-skjult-kommentar (Last seen 26.04.21).

You also informed us that Disqus, in the period between 25 May 2018 and 12 December 2019, placed cookies on the web browsers of all natural persons in Norway ("the data subjects") who visited Norwegian websites that were running the widget.

The data subjects include both registered users in Norway and anonymous users of the websites in Norway.

Further, you explained how information about Norwegian users was collected by the use of cookies:

> *Disqus cookies log visits to certain web pages (e.g., other pages where the Disqus widget is running), for the purpose of creating aggregated interest groups, which is then used for decisioning in online behavioral advertising.*

Furthermore, you explained that

> *The data collected consisted primarily of urls and time and date stamps for when those urls were accessed, but also included data automatically sent by browsers, including IP address.*

According to your response, you are unable to provide us with the exact number of Norwegian users that these cookies have logged, but you have informed us that 10 377 Norwegian users registered to use your service between 25 May 2018 and 12 December 2019.

You have informed us that you made the collected personal data available in real-time to Zeta Global, your parent company, and that the data was shared with Zeta Global for advertising purposes on a real-time basis. On the other hand, you have not confirmed that Disqus or Zeta Global have disclosed the collected personal data to any third party advertising partners of the companies. You have also explained "*Disqus did not intentionally target Norwegian data subjects for data collection and does not advertise in Norway*".

According to your statement

> *…any use by Zeta of data collected via cookies placed in error by Disqus would have been minimal, if it occurred at all. If there was any use, it would have been in the context of online display advertising (e.g. to a Norwegian visitor to a U.S. website) where data collected by Disqus would help inform which users were shown which online advertisements.*

Furthermore, you emphasize that

> *Disqus did not know it had the data, did not knowingly use it to advertise to Norwegian data subjects, did not otherwise profit from use of the data, did not sell or otherwise transfer the data to third parties (other than making it available to Zeta Global, Disqus' parent company), immediately changed Disqus' configuration for Norway upon being*

informed of the error, and promptly deleted the data that had been collected via inappropriately placed cookies.

As further explained in sections 3.2 and 3.3, tests conducted by NRK and Conzentio showed that the personal data Disqus collected through cookies were disclosed to third party advertising partners of Disqus and Zeta Global.

The Disqus Privacy Policy contains a list over external third party online advertising companies with which Disqus "*shares*" the personal data the company collects through cookies.[5]

You have provided the following information regarding "Data recipients" on your website:

> *We work with LiveRamp to help marketers connect browsers and devices with data from other sources that has been obfuscated to remove any directly identifying information. LiveRamp provides a privacy policy and opt-out options.*
>
> *We share [the data subjects'] web browsing activity with Viglink to allow advertisers to personalize ads based on the types of products and services in which [the data subjects] seem to be interested. You may read Viglink's privacy policy and opt-out.*
>
> *We share [the data subjects'] web browsing activity with Disqus' parent company, Zeta Global, to enable personalized marketing based on [the data subjects'] perceived interests. Please see Zeta's privacy policy.* [6]

Your website informs the following concerning Disqus' use of tracking cookies and ad service:

> *Disqus uses "authentication" cookies, e.g., `sessionid`, `disqusauth`, and `disqusauths`, to keep you logged in from your web browser and personalize your Disqus experience.*
>
> *Disqus uses "unique" cookies, e.g., `disqus_unique` and `_jid`, to associate web-based activities with a page load and with a web browser, including activities that violate our Terms of Service, and understand your interests and product usage.*
>
> *When Disqus loads ads, we use ad serving technologies from Google that may set cookies for the purposes of personalized marketing, associating ads with later activities, and limiting how you are shown specific ads.*

Despite not having a GDPR compliant solution in place for the widget on the websites, you argue that your processing of personal data about the data subjects can fulfil the criteria under Article 6(1)(f) GDPR.

---

[5] https://disqus.com/data-sharing-settings/ (Last seen 26.04.21)
[6] https://disqus.com/data-sharing-settings/ (Last seen 26.04.21)

To support this argument, you state that the data subjects who were registered users of Disqus "voluntarily registered themselves to use the service, had adequate notice of Disqus' data processing activities, and at all times had the ability to exercise their privacy rights."

As for the "anonymous site visitors", you argue that you had a legal basis for processing their personal data under Article 6(1)(f) because

> *"the identity of these users was never known to Disqus and it was able to recognize such users only by an anonymous cookie ID, not by name, email, or other directly identifying personal data. In addition, such data was not used for commercial purposes, sold to third parties, or used to harm data subjects in any way."*

You also argue that this processing "produced effectively no privacy risks to data subjects."

Furthermore you argue that "the data processed in that case was not personal data at all, because Disqus had no means of identifying individuals from their cookie IDs", but that you in an "abundance of caution deleted all such data in December 2019".

3.2 Press coverage by the NRK

The NRK news articles from November and December 2019[7] described how the privacy consulting company Conzentio has conducted tests of the Disqus widget and your data collection.

According to one of the articles, the tests showed that Disqus has placed third party cookies on the user equipment of visitors to the website running the widget. Conzentio stated in the articles that Disqus collected information about which other websites running the Disqus widget the user visited, in addition to their IP-address, technical browser data and a unique ID, through these cookies.[8]

The NRK further described how the tests showed that Disqus shared the personal data with third party advertising partners and its parent company Zeta Global. The articles state that Disqus' collection and disclosure or dissemination of personal data took place without a valid consent pursuant to the GDPR, and without the data subjects being informed by Disqus of this.

Anders Willstedt of Conzentio states that their tests showed that the Disqus widget sent user data to a large number of third parties without the webpage owner or the users' knowledge.

---

[7] https://nrkbeta.no/2019/11/18/nettstedet-deres-sendte-besoksdata-til-81-selskaper/ (Last seen 26.04.21)
https://nrkbeta.no/2019/12/18/disqus-delte-persondata-om-titalls-millioner-internettbrukere-uten-at-nettsidene-visste-om-det/ (Last seen 26.04.21)
https://nrkbeta.no/2019/12/20/nrk-fjerner-kommentarfelt-pa-p3-og-ytring-etter-avsloring/ (Last seen 26.04.21)

[8] https://nrkbeta.no/2019/11/18/nettstedet-deres-sendte-besoksdata-til-81-selskaper/ (Last seen 26.04.21)

According to the NRK, the number of affected website users in Norway amounts to several hundred thousand.

The articles list P3.no, tv.2.no/broom, khrono.no, adressa.no, rights.no and document.no as affected websites ("the websites") that were running the Disqus widget. In another article, NRK confirms that their debate website NRK.no/ytring was also among the affected websites.[9]

The websites are all various news sources and online newspapers. NRK.no/ytring is the debate section of the national broadcaster NRK's website, while P3.no is the website of the NRK radio channel P3. Tv2.no/broom is a section of the broadcaster TV2's website for automobile content, Khrono is an online newspaper for higher education and research, Adresseavisen is a large online newspaper, and rights.no and document.no are online newspapers as well.

Megan Rose of Zeta Global confirms that Norway was not included in the GDPR compliant version of the Disqus widget.[10] Rose explains that Disqus collected personal data about Norwegian residents by mistake, and that this happened because the company failed to identify the GDPR as applicable to Norway, as it is not an EU member state. Neither Zeta Global, nor Disqus comments the alleged sharing of personal data with third parties in the article.

3.3 Press coverage by Computerworld.no

Computerworld.no has written an article based on the articles by the NRK, where they explain how Disqus through third party cookies has collected personal data about their visitors without the visitors' knowledge.[11]

The article elaborates how the tests that revealed Disqus' cookie practice and disclosure of personal data were conducted. Computerworld explains that Conzentio has developed a scanner bot, which mimics a regular website user and navigates websites through clicks as a regular user would. According to Conzentio, the bot's behaviour triggers activity on the website, where some cookies are placed at the time of the first visit, while others are placed after the bot has visited several websites. The scan that the NRK and Computerworld's articles are based on was conducted in the summer of 2019.

4. Relevant GDPR requirements

4.1 Material scope

[9] https://nrkbeta.no/2019/12/20/nrk-fjerner-kommentarfelt-pa-p3-og-ytring-etter-avsloring/ (Last seen 26.04.21).
[10] https://nrkbeta.no/2019/12/18/disqus-delte-persondata-om-titalls-millioner-internettbrukere-uten-at-nettsidene-visste-om-det/ (Last seen 26.04.21)
[11] https://www.cw.no/artikkel/gdpr/en-skjult-kommentar (Last seen 26.04.21)

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

"Personal data" is defined by Article 4(1) 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.*

Pursuant to Article 4(2) "processing" means

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means […]*

4.2 Controller

Pursuant to Article 4(7), a "controller" is 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.*

4.3 Territorial scope

The Norwegian Personal Data Act[12] incorporates the GDPR into Norwegian law. The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

Pursuant to Section 4 of the Norwegian Personal Data Act, the Act applies to the processing of personal data of data subjects in Norway conducted by controllers that are not established in the EEA, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in Norway; or (b) the monitoring of their behaviour as far as their behaviour takes place within Norway.

Article 3(2) GDPR provides that

> *[t]his Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> *(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

[12] LOV-2018-06-15-38.

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

The GDPR is incorporated into the EEA Agreement, and is therefore applicable in the EEA/EFTA states (Norway, Liechtenstein and Iceland). Pursuant to Article 1(b) of the Decision of the EEA Joint Committee, the EEA/EFTA States are included where the GDPR refers to "member states":

> *Notwithstanding the provisions of Protocol 1 to this Agreement, and unless otherwise provided for in this Agreement, the terms "Member State(s)" and "supervisory authorities" shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.* [13]

4.4 The supervisory authority

Pursuant to Article 51(1) GDPR:

> *Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*

Datatilsynet is the national supervisory authority in Norway, pursuant to the Norwegian Personal Data Act Section 20.

The supervisory authority's competence is regulated by Article 55(1) GDPR:

> *Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*

Article 57(1)GDPR sets forth the tasks of the supervisory authority:

1. *Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:*

(a) monitor and enforce the application of this Regulation;

[…]

[13] See Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

Article 58(1) and (2) GDPR regulates the supervisory authority's investigative and corrective powers:

> *1. Each supervisory authority shall have all of the following investigative powers:*
>
> *(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;*
>
> *(b) to carry out investigations in the form of data protection audits;*
>
> *(c) to carry out a review on certifications issued pursuant to Article 42(7);*
>
> *(d) to notify the controller or the processor of an alleged infringement of this Regulation;*
>
> *(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;*
>
> *(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.*
>
> *2. Each supervisory authority shall have all of the following corrective powers:*
>
> *(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
>
> *(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;*
>
> *(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;*
>
> *(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*
>
> *(e) to order the controller to communicate a personal data breach to the data subject;*
>
> *(f) to impose a temporary or definitive limitation including a ban on processing;*

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

4.5 Principles relating to processing of personal data

According to Article 5(1)(a) GDPR:

[personal data shall be] processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Pursuant to Article 5(2):

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

4.6 Profiling

In accordance with Article 4(4), "profiling" is defined as:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

4.7 Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 12(1) GDPR stipulates how the controller shall provide information to the data subjects:

> *1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

4.8 Information to be provided where personal data are collected from the data subject

Articles 13(1) and (2) GDPR list the information the controller must provide to the data subjects when personal data is collected from the data subjects, as well as when it shall be provided:

> *1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
>
> *(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*
>
> *(b) the contact details of the data protection officer, where applicable;*
>
> *(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
>
> *(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
>
> *(e) the recipients or categories of recipients of the personal data, if any;*
>
> *(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*
>
> *2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following*

further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.9 **Lawfulness of processing**

Pursuant to Article 6(1) GDPR, processing shall be lawful only if and to the extent that at least one of the requirements in (a) to (f) applies.

Where the controller relies on Article 6(1)(f) for processing, the following conditions must be fulfilled by the controller:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
[...]
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5. Our assessment of the case

5.1 Material scope of the GDPR

You argue that the data Disqus collected from cookies was not personal data, as you had no means of identifying individuals from their cookie IDs.

Recital 26 GDPR states the following regarding the definition of "personal data":

> *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.*

Online identifiers are explicitly mentioned as an example of information relating to an identifiable natural person in Article 4 (1) GDPR.

Recital 30 GDPR further elaborates on online identifiers as a type of personal data:

> *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 such as radio frequency identification tags. 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 the present case, Disqus has placed cookies in the terminal equipment of all visitors to the Websites, and assigned each individual visitor with a unique cookie ID. Subsequently, you tracked the visitors across websites, collected data such as IP address, time of visit to websites, analysed this information, and placed the user in interest groups according to their online activity and inferred interests or other characteristics.

An IP address is a unique online identifier, explicitly defined as personal data pursuant to Recital 30 GDPR, which may reveal the location of a user. This suggests you have processed information related to identifiable natural persons, and thus "personal data" pursuant to Article 4(2).

A cookie ID is a unique online identifier assigned each individual user of e.g. a website. The ID is assigned when the website owner or a third party places a cookie in their terminal

equipment. The ID enables the controller to distinguish and recognize each unique user, as well as to track each users' online activity both on and across websites.

A cookie ID may not necessarily alone *identify* a natural person with e.g. name and address. Regardless of whether this constitutes *identifiable* information, each cookie ID is unique and placed in the browser of a natural person, enabling the controller to distinguish one website user from another, and to monitor how each user interacts with the website. The cookie ID therefore constitutes information concerning an *identifiable* natural person, as the controller is able to single out individual users and their activity based on the assigned ID. Hence, a cookie ID fulfils the criteria in Article 4(1) GDPR, and constitutes "personal data".

Assigning cookie IDs to users, tracking users' across websites, as well as subsequently analysing and sharing data about the online behaviour concerning each unique ID clearly constitutes "processing of personal data" pursuant to Article 4(2).

Based on this, we consider Disqus' processing of the personal data of data subjects in Norway to be within the material scope of the GDPR pursuant to Article 2.

5.2 Controller

As discussed in section 5.1, it is clear that Disqus has processed personal data in the present case.

For Disqus to be responsible for these processing activities under the GDPR, the company must fulfil the criteria of being a controller pursuant to Article 4(7) GDPR.

According to the ComputerWorld article[14], the website owners could have disabled «Tracking: Enable anonymous cookies targeting for your site's visitors. This helps to provide personalized content and ad-vertising for your site's visitors» and «Affiliate links: Automatically append merchant codes to product links on your site» in the settings for the Disqus widget.

Our understanding is that these data sharing settings were turned on by default, and that this was a consequence of Disqus not knowing the GDPR was applicable to data subjects in Norway. As Disqus did not know the GDPR was applicable, the company did not ran a version of the widget not intended for EEA countries. As Disqus informs us, data sharing settings are turned off and GDPR consent boxes are available to the data subject in the GDPR compliant widget version.

The website owners are as controllers of personal data processing on their website responsible for what third party tracking they allow to be present on the website.

[14] https://www.cw.no/artikkel/gdpr/en-skjult-kommentar (last seen 26.04.21).

In the present case, we have focused our investigation on Disqus' responsibility under the GDPR as a controller present on the websites.

Disqus may be a controller for certain processing activities that occurs through their presence on websites, when this processing fulfills the criteria for controllership in Article 4(7) GDPR, including processing personal data for their own purposes.

In the present case, it is clear that Disqus' tracking, analysing and profiling of the visitors to the websites happened in Disqus' own economical interest, namely data collection for the purpose of online behavioural advertising. Furthermore, it is clear that Disqus decided the means of processing, i.e. tracking, analysing, profiling and simultaneous disclosure to third parties.

Based on this, our assessment is that Disqus has determined the purposes and means of the tracking, analysing, and disclosure of personal data to Zeta Global and other third parties that has occurred in the present case.

Furthermore, Disqus has informed us that the company does not advertise in Norway, and that Disqus has allegedly not used personal data collected through the websites to serve ads in Norway. This strengthens our assessment that the data processing has happened solely in the interest of Disqus, and that Disqus is the controller under the GDPR for the processing activities subject to this investigation.

In conclusion, we consider Disqus to be the controller of the tracking, analysing, profiling and disclosing of personal data subject to this investigation pursuant to Article 4(7) GDPR.

5.3 Territorial scope of the GDPR

5.3.1 The applicable law

As listed in section 4.3, where a controller is not established in the EEA, Article 3(2)(a) and (b) GDPR prescribes two alternative criteria for the Regulation to apply to the controllers processing of personal data of data subjects who are in the EEA. We will examine these in the following.

5.3.2 "the offering of goods or services…"

Recital 23 GDPR prescribes the following factors as relevant when examining whether a controller is "offering goods or services", which is the first of the two criteria in Article 3(2), to data subjects in the EEA;

> *In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the*

Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

The European Data Protection Board[15] ("the EDPB") have adopted guidelines regarding the GDPRs territorial scope.[16] The EDPB states that relevant factors to take into account when considering whether a controller offers goods or services to data subjects in the union are;

When taking into account the specific facts of the case, the following factors could therefore inter alia be taken into consideration, possibly in combination with one another:

- The EU or at least one Member State is designated by name with reference to the good or service offered;

- The data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience

- The international nature of the activity at issue, such as certain tourist activities;

- The mention of dedicated addresses or phone numbers to be reached from an EU country;

- The use of a top-level domain name other than that of the third country in which the controller or processor is established, for example ".de", or the use of neutral top-level domain names such as ".eu";

[15] "The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities." (https://edpb.europa.eu/about-edpb/about-edpb_en).
[16] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

- The description of travel instructions from one or more other EU Member States to the place where the service is provided;

- The mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers;

- The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states;

- The data controller offers the delivery of goods in EU Member States.

In the present case, Disqus offers the Disqus Widget to the people visiting websites running the Widget. The Widget is a service offered to the users of a website, enabling them to post comments on the website. In our case, the Widget was offered on seven Norwegian news websites as a service for the users of the Websites and as means for them to express their views on the content of the Websites, e.g. news articles. This indicates that Disqus offers a service to data subjects in Norway.

Furthermore, the Disqus Widget was available in Norwegian to data subjects in Norway, visiting Norwegian news websites, available in the Norwegian language, with a Norwegian country code top-level domain.[17]

Based on this information, we find it clear that Disqus fulfils the criteria of "offering services" to data subjects in Norway, pursuant to The Norwegian Personal Data Act Section 4 (b), cf. Article 3(2)(b) GDPR.

5.3.3 "monitoring" the behaviour of data subjects in the EEA

The monitoring criteria is the second of the two alternative criteria in Article 3(2), to data subjects in the EEA.

Recital 24 GDPR states the following regarding the monitoring criteria:

> *The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or*

[17] https://www.norid.no/en/om-domenenavn/er-det-forskjell-pa-norske-domenenavn-og-andre/ (Last seen 26.04.21)

him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Online tracking using cookies and behavioural advertising are explicitly mentioned as activities which constitute monitoring of behaviour in the EDPB Guidelines on the territorial scope of the GDPR.[18]

In the present case, you admit that Disqus has placed cookies on the browsers of natural persons in Norway that visited the Websites. Furthermore, you admit that Disqus through these cookies have collected data on which other websites the data subjects visited, the time of visit, as well as information like their IP address. This information was then analysed and used to place the data subjects in interest groups based on their inferred interests or characteristics for the purposes of online behavioural marketing.

Our assessment is that Disqus' placing of cookies and subsequent tracking of data subjects in Norway, constitutes monitoring of data subject behaviour in the EEA, pursuant to Article 3(2)(b) GDPR.

Hence, our conclusion is that Disqus' abovementioned processing of personal data concerning data subjects in Norway falls within the territorial scope of the GDPR pursuant to Article 3(2)(a) and 3(2)(b) GDPR.

5.4 The NO DPAs competence

In your response to our order to provide information, you argue that Disqus is "not the subject of to the jurisdiction of Datatilsynet" and that we do not have legal jurisdiction "to conduct an investigation of or take adverse action against Disqus";

> *Neither Disqus nor its parent Zeta Global have any business operations in Norway, and as such, do not believe that the Datatilsynet has established legal jurisdiction to conduct an investigation of or take adverse action against Disqus. But, because the processing in question was the result of a good-faith error by Disqus which was promptly corrected upon its discovery, in the interests of transparency we have elected to respond to this inquiry. We maintain, however, that Disqus is not subject to the jurisdiction of the Datatilsynet.*

Pursuant to Article 51(1) GDPR:

> *Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*

[18] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), p. 20.

Datatilsynet is the national supervisory authority in Norway, pursuant to the Norwegian Personal Data Act Section 20.

The supervisory authority's competence is regulated by Article 55(1) GDPR:

> *Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*

Article 57(1)GDPR sets forth the tasks of the supervisory authority:

1. *Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:*

(a) monitor and enforce the application of this Regulation;

..

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

Article 58(1) and (2) GDPR regulates the supervisory authority's investigative and corrective powers, including the power to order the controller to provide any information it requires for the performance of its tasks pursuant to Article 58(1)(a), and the power to impose an administrative fine pursuant to Article 83 GDPR, see Article 58(2)(i).

According to Article 56(1) GDPR regulates the competence of the "lead supervisory authority" and the cooperation and consistency ("one stop shop") mechanism between the supervisory authorities:

> *1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*

Article 4(16) defines the concept of "main establishment":

> *'main establishment' means:*
>
> a) *as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;*

b) *as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;*

Pursuant to Article 4(23), "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.*

For the cooperation mechanism to be applicable, the first criterion is that the controller must have an establishment in the EEA.

As we have concluded in 4.2, Disqus, Inc. is the controller for the processing of personal data for marketing purposes in the context of the Disqus Widget. It also appears that you do not have an establishment in the EEA.

Because Disqus is not established in the EEA, pursuant to Article 56(1) GDPR, the cooperation mechanism set out in Chapter VII Section 1 GDPR does not apply, and as such, the Norwegian Data Protection Authority is competent to handle the matter pursuant to Article 55(1).

The Article 29 Working Party ("WP29"), the predecessor of the EDPB, have made guidelines for identifying a controller or processor's lead supervisory authority under the GDPR.[19] The EDPB have endorsed these guidelines, and they are therefore relevant when applying the GDPR. The guidelines also provide guidance on the supervisory authorities' competence in the case where a company is not established within the EU:

> *The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a Member State does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every Member State they are active in, through their local representative.*[20]

[19] Guidelines for identifying a controller or processor's lead supervisory authority (16/EN WP 244)
[20] Guidelines for identifying a controller or processor's lead supervisory authority, para. 3.3.

Where the GDPR is applicable, the controller is subject to the supervisory authorities' competence, and investigative and corrective powers pursuant to Article 58.

Hence, the NO DPA is competent and has the investigative and corrective powers to conduct an investigation against Disqus and to impose binding decisions pursuant to Article 58 GDPR, such as administrative fines in line with Article 83, where we find Disqus has breached provisions of the GDPR.

To summarize, our conclusion is that the NO DPA is competent to handle the present case, and that it follows from Article 58 GDPR, that we have the investigative and corrective powers to impose binding administrative decisions towards Disqus Inc.

5.5 The accountability principle

The GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5.[21]

The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance, pursuant to Recital 74 GDPR.

According to the EDPB, the WP29 Opinion 3/2010 on the principle of accountability is still relevant for understanding the accountability principle under the GDPR.[22]

WP29 states in a non-exhaustive list that it considers "Establishment of internal procedures *prior* to the creation of new personal data processing operations (internal review, assessment, etc)" (added emphasis) to be a common accountability measure.[23]

The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary.[24]

The principle consists of two key elements. First, the accountability principle makes it clear that the controller is responsible for complying with the principles in Article 5(1), and secondly that the controller must be able to demonstrate its compliance.

According to Article 5(1)(a) GDPR:

[21] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 6.
[22] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 6.
[23] WP29 Opinion 3/2010 on the principle of accountability, p. 11.
[24] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 8.

> *[personal data shall be] processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

Recital 39 GPDR states that "any processing of personal data should be lawful and fair."

According to de Terwange in Kuner et al:

> *...the requirement that data processing must be lawful essentially means that it respects all applicable legal requirements (for example the obligation of professional secrecy if applicable), Article 6 GDPR has been re-tided 'lawfulness of processing' rather than 'criteria for making data processing legitimate' as in the DPD, and one may find in this provision the core conditions for processing to be lawful. In fact, Article 6(1) GDPR states that processing shall be lawful only if and to the extent that at least one of the conditions it lists applies.*[25]

Pursuant to Article 6(1) GDPR, processing shall be lawful only if and to the extent that at least one of the requirements in (a) to (f) applies.

As stated by the EDPB in several guidelines, a lawful basis must be present before starting a data processing:

> *Although the GDPR does not literally prescribe in Article 4(11) that consent must be given prior to the processing activity, this is clearly implied. The heading of Article 6(1) and the wording "has given" in Article 6(1)(a) support this interpretation. It follows logically from Article 6 and Recital 40 that a valid lawful basis must be present before starting a data processing.*[26]

> *The legal basis must be identified at the outset of processing, and information given to data subjects in line with Articles 13 and 14 must specify the legal basis.*[27]

As we have concluded in section 5.2, Disqus was the controller of the processing of personal data subject that occurred when the company tracked, analysed, profiled and disclosed the personal data of visitors to the websites.

As the controller for this processing, Disqus was responsible for ensuring compliance with the principle of lawfulness, and to establish a legal basis in accordance with Article 6(1) GDPR *before* the company started processing the personal data of data subjects in Norway who visited the websites.

Because Disqus was unaware that the GDPR applied to Norwegian users, it is clear that you did not assess the lawfulness of the processing activities that you have conducted in the

[25] "The EU General Data Protection Regulation (GDPR) A Commentary", Chapter II, Article 5, de Terwange, Kuner, Bygrave and Docksey (2020), p. 314.
[26] Guidelines 05/2020 on consent under Regulation 2016/679, para. 90.
[27] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, para. 17.

present case before they started, as required by the Article 6(1) GDPR, cf. Article 5(1)(a) (the principle of lawfulness).

The fact that Disqus between July 2018 and December 2019 was unaware that the GDPR applies to data subjects in Norway, means that you have failed to fulfil your responsibility of complying with and being able to demonstrate compliance with the GDPR.

Our assessment is that your failure to identify the GDPR as applicable data protection law, and thus failing to implement the data protection safeguards the regulation prescribes, constitutes a breach of the accountability principle.

5.6 Information to the data subjects

5.6.1 Transparent information, communication and modalities for the exercise of the rights of the data subject

Between 25 May 2018 and 12 December 2019, Disqus processed personal data about all visitors to the websites by collecting personal data through cookies. This, according to your reply, included both registered Disqus users, and unregistered users of the websites.

In the present case, Disqus has used cookies as a tracking technology to collect personal data. When a user accessed one of the websites running the Disqus Widget, Disqus placed a cookie in the users' web browser, assigned the user a cookie ID, and the tracking, profiling and disclosure to third parties started. Thus, the collection of personal data started when the visitor accessed one of the websites that were running the Disqus Widget.

In our order to provide information, we asked Disqus about what information the company provided to Norwegian residents about the company's processing of their personal data. Disqus has replied the following:

> *The Disqus privacy policy is available at www.disqus.com and has been publicly available for several years prior to the effective date of the GDPR. Note that the current version of the privacy policy is dated June 10, 2020, however, the only material changes to the policy since the effective date of the GDPR relate to requirements under the CCPA (a new law in California), clarification of data sharing relationships used in Disqus' non-GDPR configuration, and the process by which individuals may make requests to exercise their privacy rights. It has not changed in any material respect with regard to GDPR since early 2018.*

In addition to being available on the Disqus website, our understanding is that the company's privacy policy was available through a link in the Disqus widget. The Disqus widget was situated at the bottom of the websites, available for the data subjects to use as a comment field after reading news articles.

The question for the NO DPA is if Disqus, having made the company's privacy policy available on their website and through the widget, satisfied the criteria in Article 12(1) GDPR.

Article 12(1) specifies that information pursuant to Article 13 and 14 relating to processing to the data subject, shall be provided in a "concise, transparent, intelligible and easily accessible form".

In the present case, the requirements of "transparent" and "easily accessible" are particularly relevant.

Recital 58 GDPR states the following regarding information from the controller to the data subject:

> *The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.* (Added emphasis)

Additionally, WP29 has issued guidelines on transparency under the GDPR, which the EDPB has endorsed. [28] The guidelines are relevant for interpreting the information requirements in Articles 12-14 GDPR. WP 29 states the following regarding the principle of transparency and the information requirements in Articles 12-14:

> *A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.*[29]

Regarding the "easily accessible" requirement, the guidelines state the following:

> *The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/ notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc.*

[28] Guidelines on transparency under Regulation 2016/679.
[29] Guidelines on transparency under Regulation 2016/679, para. 10.

As emphasized in Recital 58, the transparency principle and requirements in Article 12(1) GDPR are of particular importance in the context of online advertising, as it is a technologically complex, as well as invasive way of processing personal data. In accordance with the principle of transparency, high risk processing activities strengthens the importance of clear and easily accessible information to the data subjects.

As the WP29 states; "the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them".

Disqus tracked, profiled and shared the personal data of all visitors to the websites, regardless of whether they registered as Disqus users or not, or used the Disqus widget. The large majority of data subjects therefore had no reason to expect Disqus processing their personal data for online behavioural advertising.

The large majority of the data subjects had never interacted with Disqus before they were subject to the company's tracking for online advertising, and had no reasonable expectation for Disqus to process their personal. Information about Disqus processing of their personal data for online behavioural advertising is therefore particularly important. Information is a fundamental prerequisite for the data subjects to assess the risk of a processing activity, and whether they e.g. wanted to object to the processing pursuant to Article 21. Without this information, the data subjects were not able to assess whether they wanted to be subject to Disqus' tracking and profiling.

Pursuant to Article 12(1), Disqus should have provided information to the data subjects at the latest when the tracking started, i.e. when the data subject opened the website. Disqus making the company's privacy policy available through your website and in the widget, situated at the bottom of the websites, does not fulfil the criteria of being "easily accessible" pursuant to Article 12(1), and is not in accordance with the principle of transparency in Article 5(1)(a) GDPR.

In conclusion, our assessment is that Disqus has failed to comply with Article 12(1) and Article 5(1)(a) GDPR.

5.6.2 Information to be provided where personal data are collected from the data subject

In addition to the requirements in Article 12, the data subjects' right to information and corresponding information duty for the controller is regulated in Article 13(1) and (2) GDPR. The Article lists the specific information the controller must provide to the data subjects, where personal data relating to a data subject are collected from the data subject, as well as the timing of this information.

The required information includes the identity and contact details of the controller, the purposes of processing and the legal basis, the recipients or categories of recipients of the personal data, and the existence of the right of access, erasure, and to object to the processing.

According to Article 13(1), the controller must provide the required information to the data subjects "at the time when personal data are obtained".

As we have assessed in section X, Disqus' processing of personal data started immediately when the data subjects accessed one of the websites. Pursuant to Article 13(1), Disqus should have notified the data subjects of the processing as soon as they accessed the website. It is clear that the unregistered visitors did not receive any notification or information about your processing of their personal data, and had no means of understanding that they had been cookied by Disqus.

Therefore, we consider that Disqus has failed to provide information to the unregistered visitors, as required by Article 13 GDPR.

As for the 10 377 Norwegian Disqus users that you inform us registered with your service between 2018 and 2019, you argue that they had access to the Disqus privacy policy and therefore had access to adequate information about the processing as prescribed by the GDPR.

The processing of personal data concerning the registered users is identical to the unregistered visitors. The tracking started as the data subject accessed the website, regardless of whether they were a registered Disqus user or not. Disqus had the same duty to inform registered users at the time they accessed website.

In conclusion, Disqus has failed to comply with Article 13 GDPR.

5.7 **Legal basis**

5.7.1 Disqus' information regarding the processing activities

Disqus' arguments

Disqus has made the following comment on the alleged disclosure of personal data to third parties, and the use of such data to target data subjects in Norway with online behavioural advertising:

> *...any use by Zeta of data collected via cookies placed in error by Disqus would have been minimal, if it occurred at all. If there was any use, it would have been in the context of online display advertising (e.g. to a Norwegian visitor to a U.S. website) where data collected by Disqus would help inform which users were shown which online advertisements.*

Furthermore, Disqus has emphasized that

> *Disqus did not know it had the data, did not knowingly use it to advertise to Norwegian data subjects, did not otherwise profit from use of the data, did not sell or otherwise*

transfer the data to third parties (other than making it available to Zeta Global, Disqus' parent company), immediately changed Disqus' configuration for Norway upon being informed of the error, and promptly deleted the data that had been collected via inappropriately placed cookies.

Disqus has not confirmed whether this data was used to serve targeted advertising to Norwegian users who visited U.S websites on which Disqus run advertisements or not.

The NO DPAs assessments of the facts

As explained in sections 3.2 and 3.3, tests conducted by the NRK and Conzentio showed that the personal data Disqus collected through cookies was shared with third party advertising partners of Disqus and Zeta Global.

The Disqus Privacy Policy contains a list over external third party online advertising companies you share the personal data you collect through cookies with.[30] This includes Viglink, with whom you share data about the users' web browsing activity

You provide the following information regarding "Data recipients" on your website:

> *We work with LiveRamp to help marketers connect browsers and devices with data from other sources that has been obfuscated to remove any directly identifying information. LiveRamp provides a privacy policy and opt-out options.*
>
> *We share [the data subjects] web browsing activity with Viglink to allow advertisers to personalize ads based on the types of products and services in which [the data subjects] seem to be interested. You may read Viglink's privacy policy and opt-out.*
>
> *We share [the data subjects] web browsing activity with Disqus' parent company, Zeta Global, to enable personalized marketing based on [the data subjects] perceived interests. Please see Zeta's privacy policy.* [31]

Your website informs the following concerning Disqus' use of tracking cookies and ad service:

> *Disqus uses "authentication" cookies, e.g., `sessionid`, `disqusauth`, and `disqusauths`, to keep you logged in from your web browser and personalize your Disqus experience.*
>
> *Disqus uses "unique" cookies, e.g., `disqus_unique` and `_jid`, to associate web-based activitieswith a page load and with a web browser, including activities that violate our Terms of Service, andunderstand your interests and product usage.*

[30] https://disqus.com/data-sharing-settings/ (Last seen 26.04.21)
[31] https://disqus.com/data-sharing-settings/ (Last seen 26.04.21)

When Disqus loads ads, we use ad serving technologies from Google that may set cookies for the purposes of personalized marketing, associating ads with later activities, and limiting how you are shown specific ads.

You also explain that "Disqus did not intentionally target Norwegian data subjects for data collection and does not advertise in Norway", and that you cannot confirm whether this data was used to serve targeted advertising to Norwegian users who visited U.S websites on which Disqus run advertisements or not.

Based on Disqus vast online presence, we find it likely that data subjects have visited one of the several hundred thousand websites where Disqus advertises[32].

In light of the information available to us, our assessment is that Disqus used the personal data collected to serve behavioural advertising to data subjects in Norway when they visited a website that used Disqus to advertise.

Based on the tests conducted by the NRK and Conzentio, as well as the Disqus privacy policy, our assessment is that Disqus has shared the collected and analysed personal data with its parent company, as well as its advertising partners.

5.7.2 Disqus' processing activities

The present case involves several processing activities carried out using the personal data Disqus collected through cookies between May 2018 and November 2019.

Having assessed the information available to us, see section 3, we consider that "the processing activities" consists of:

- Tracking the data subjects' online behaviour and collecting information about their IP address, which URLS they have visited, including the time and date stamps of visit;
- analysing the personal data collected through tracking and using it to create aggregated interest group for the purpose of decision-making in behavioural advertising based on inferred interests and characteristics (*profiling)*;
- disclosing the collected and analysed personal data to Zeta Global in real-time;
- disclosing personal data to third party advertising partners of Disqus and Zeta Global. (in accordance with the Disqus privacy policy)
- serving online behavioural advertising to data subjects in Norway when they visited websites where Disqus or Zeta Global advertised.

5.7.3 Our assessment of the legal basis

[32] https://blog.disqus.com/the-numbers-of-disqus (Last seen 26.04.21).

As you recognize in your reply to us, Disqus did not obtain a valid consent from the data subjects before you processed the personal data collected through your cookies. The fact that you were unaware that the GDPR applied to your processing of personal data about data subjects in Norway underlines this.

Despite Disqus' unawareness of the GDPRs applicability in Norway, and failure to identify a legal basis for the processing activities beforehand, we will in the following independently examine if Disqus fulfilled the criteria in Article 6(1)(f) GDPR for the processing activities.

We will however note, that regardless of the outcome of the ex-post assessment of legal basis we are conducting here, Disqus has breached the accountability principle by failing to identify a legal basis beforehand, as discussed under section 5.4.

In the present case, our assessment is that the processing activities have pursued the same interest, namely Disqus' economic interest of online behavioural marketing.

As the assessment of the criteria in Article 6(1)(f) will be more or less identical for each processing activity, we will in the following assess the lawfulness of the activities under one.

In order to rely on Article 6 (1)(f) for processing, the controller must meet three cumulative conditions. These are the pursuit of a *legitimate interest* by the controller, *necessity* to process personal data for the purposes of the legitimate interests pursued, and the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence over the legitimate interests pursued by the controller or a third party – *the balance test*. [33]

The first question is whether Disqus fulfilled the condition of "legitimate interest" or not.

The "legitimate interest" must be acceptable under law and clearly defined before the processing starts.[34]

Which interests fulfil this criterion depends on a consideration of which benefits the processing has for the controller, how important the interest is for the controller, if it happens in the interest of the public, or in the interest of ideal interests which benefits society at large, cf. WP29 Opinion 06/2014.[35] This WP29 opinion is referenced by the EDPB in multiple guidelines relating to the GDPR, and is thus still relevant.[36]

In the present case, the processing activities have happened for the interest of online marketing and the interest of economical profit for Disqus by selling advertising space.

[33] EDPB Guidelines 8/2020 on the targeting of social media users, p.15.
[34] Guidelines 05/2020 on consent under Regulation 2016/679, para. 90.
[35] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, p. 24 and 25.
[36] See e.g. EDPB Guidelines 8/2020 on the targeting of social media users, para 50.

Opinion 06/2014 explicitly mentions “conventional direct marketing and other forms of marketing or advertisement” as an example of a legitimate interest, “without prejudice to whether the interests of the controller will ultimately prevail over the interests and rights of the data subjects when the balancing is carried out.”.

Based on this, Disqus fulfilled the first condition of “legitimate interest”.

The second condition is that the processing of personal data must be *necessary* for the purposes of the legitimate interests pursued.

The necessity condition requires a connection between the processing and the interests pursued. The controller must always consider whether less invasive means are available to serve the same end, and limit the processing to what is necessary for the purposes intended.

WP29 states the following regarding the necessity condition:

> *Finally, the processing of personal data must also be 'necessary for the purpose of the legitimate interests' pursued either by the controller or - in the case of disclosure - by the third party. This condition complements the requirement of necessity under Article 6, and requires a connection between the processing and the interests pursued. This 'necessity' requirement applies in all situations mentioned in Article 7, paragraphs (b) to (f), but is particularly relevant in the case of paragraph (f) to ensure that processing of data based on legitimate interests will not lead to an unduly broad interpretation of the necessity to process data. As in other cases, this means that it should be considered whether other less invasive means are available to serve the same end.*

You argue that you never meant to process the personal data for any purpose. The processing activities were in your opinion a result of a good faith error. You have informed us that the personal data you have collected about data subjects in Norway was not used to provide online behavioural marketing, as Disqus does not advertise on Norwegian websites and did not have the goal of targeting users in Norway. This strongly suggests that the tracking was not necessary, as the tracking did not serve any particular purpose. This indicates that Disqus did not fulfil the necessity condition.

Disqus tracked their data subjects, analysed their behaviour and created aggregated interest groups for the purpose of decision-making in behavioural advertising based on inferred interests and characteristics, disclosed the information Zeta Global real-time and to third parties as part of your business model. In addition, the data subjects were in turn served with behavioural advertising. In our view, the processing is extensive and opaque, and is an invasive way of pursuing your interest in online behavioural advertising.

Furthermore, the processing happened without providing information to the data subjects, and thus prevented the data subjects from exercising their right to object to direct marketing pursuant to Article 21 GDPR. This gave the data subjects little or no possibility to control and end your tracking and analysing of their online behaviour.

In conclusion, the processing activities could have been carried out with less invasive means, and thus Disqus did not fulfil the necessity condition.

Finally, we will also assess the third condition in Article 6(1)(f).

The third condition is the balance test. The controller must do the balancing of interests to determine whether the data subjects' fundamental rights and freedoms precedes the controller's legitimate interest. To carry out the balancing test it is first important to consider the nature and source of the legitimate interests on the one hand, and the impact on the data subjects fundamental rights and freedoms on the other hand.

The legitimate interests pursued by Disqus

In the present case, Disqus has done the processing of personal data for the economic interest of serving online behavioural advertising. Advertising is the business model of the company[37], and Disqus therefore has an economic interest in tracking natural persons to improve the automated decision-making process involved in behavioural advertising.

The interests or fundamental rights and freedoms of the data subjects

The processing activities in the present case impacts both the data subjects' fundamental right to data protection pursuant to Article 8 of the European Convention on Human Rights ("ECHR"), as well as their fundamental freedom of expression and information Article 10 ECHR.

The balancing test

In this balancing test, the controller must take into consideration all aspects of the processing, and how it affects the fundamental rights and interests of the data subject, in order to assess which interest precedes. Relevant aspects include the types of personal data, and whether these are of a particularly private or sensitive character and the data subject have a reasonable expectation of not having this data disclosed.

It is also relevant to consider what negative impact processing of the data in question will have on the data subjects, if the processing may cause fear or unease, and which measures the controller has put in place to reduce the privacy impact on the data subjects.

Legitimate interests of the controller, when minor and not very compelling may, in general, only override the interests and rights of data subjects in cases where the impact on these rights and interests are even more trivial.[38]

[37] https://help.disqus.com/en/articles/1717103-disqus-privacy-policy (Last seen 26.04.21).
[38] Opinion 06/2014, p. 30.

WP29 has stated that the nature of the interests may vary, and that some interests may be more compelling and beneficial to society at large, while others may be less pressing for society as a whole;

> *The nature of the interest may vary. Some interests may be compelling and beneficial to society at large, such as the interest of the press to publish information about government corruption or the interest in carrying out scientific research (subject to appropriate safeguards). Other interests may be less pressing for society as a whole, or at any rate, the impact of their pursuit on society may be more mixed or controversial. This may, for example, apply to the economic interest of a company to learn as much as possible about its potential customers so that it can better target advertisement about its products or services.* (Added emphasis).

The type of processing activity also impacts the balancing test. Some types of processing, such as *profiling*, can easily have a negative impact on the interests or fundamental rights and freedoms of natural persons.

Article 4(4), defines "profiling" as:

> *…any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*;

The WP29[39] states that:

> *Profiling is composed of three elements:*
>
> - *it has to be an automated form of processing;*
> - *it has to be carried out on personal data; and*
> - *the objective of the profiling must be to evaluate personal aspects about a natural person.*
>
> […]
>
> *Controllers carrying out profiling will need to ensure they meet the GDPR requirements in respect of all of the above stages.*
>
> *Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or*

[39] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 6 and 7.

make predictions about, for example, their:

- *ability to perform a task;*
- *interests; or*
- *likely behaviour.*

In the present case, Disqus has tracked the data subjects across websites after they visited one of the websites running the Disqus Widget. The websites are all online newspapers or others types of online news sources. The tracking started as the data subject visited the site running the Disqus Widget, without any notification to the data subjects. Our assessment is that this tracking and analysing of personal data with the output of aggregated interest groups constitutes profiling as defined by Article 4(4) GDPR.

The fact that a processing activity constitutes profiling largely affects the legitimate interest assessment, as profiling in itself may easily affect the interests and fundamental rights and freedoms of the data subjects.

Profiling is a type of processing which poses several threats to the fundamental rights and freedoms of the data subjects. WP29 and the EDPB have therefore in multiple guidelines expressed that processing of personal data for the purpose of profiling or targeting based on observed and inferred data should be based on the explicit consent of the data subject, rather than a legitimate interest test.[40]

WP29[41] describes some challenges concerning profiling in their guidelines:

> *The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.*

The EDPB Guidelines 08/2020 on the targeting of social media users deal with many of the issues of the present case, including profiling. The guidelines state that processing of *observed* or *inferred* personal data shall be based on consent pursuant to Article 6(1)(b) GDPR;

> *In addition, any subsequent processing of personal data, including personal data obtained by cookies, social plug-ins or pixels, must also have a legal basis under Article 6 of the GDPR in order to be lawful. For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that legitimate interest cannot act as an appropriate legal basis, as the targeting relies on the monitoring of individuals' behavior across websites and locations using tracking technologies.*

[40] See e.g. EDPB Guidelines 8/2020 on the targeting of social media users, para. 72.
[41] Guidelines on Automated individual decision-making and Profiling
for the purposes of Regulation 2016/679, p. 9.

> *Therefore, in such circumstances, the appropriate legal basis for any subsequent processing under Article 6 GDPR is also likely to be the consent of the data subject. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection. Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate legal basis in order to respect the principle of fairness.* (Added emphasis).

For the visitors to each website, there was no information that the company running the comment field widget were to start tracking which websites and news articles they read.

WP29 has explicitly mentioned tracking/monitoring as an important factor when considering what impact a type of processing activity may have on the interests and fundamental rights and freedoms of the data subjects:

> *In addition to adverse outcomes that can be specifically foreseen, broader emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been or may be misused or compromised, – for example through exposure on the internet. The chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.*[42]

The processing activities conducted by Disqus in the present case negatively affects the data subjects' right to data protection by monitoring their online activity, as well as their freedom of information by tracking and profiling natural persons based on which online news sources they visit, as well as which articles they read.

The fundamental right to freedom of expression and information is enshrined in Article 10 ECHR:

> *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

[42] Opinion 06/2014, p. 37.

The fundamental right to freedom of expression and information means that natural persons have a right to receive and impart information, particularly information like news articles, as well as a right to hold opinions and discuss said information without interference, unless prescribed by law.

Disqus' tracking of which websites and news articles the data subjects have read, as well as analysing this data, affects the data subjects' exercise of these fundamental rights. The tracking done by Disqus in the present case means that the data subjects have not been able to exercise these fundamental rights freely, as Disqus monitored the information, particularly in the form of news articles, that they have received and potentially expressed their views on through the Disqus Widget.

Hidden monitoring or tracking peoples online activity can result in a chilling effect, meaning that they abstain from lawful behaviour out of a fear of being watched online. The chilling effect on protected behaviour, like freedom of expression and information, that may result from continuous monitoring/tracking, must also be given due consideration in the balancing test.[43]

According to WP29, the way personal data is processed is also a relevant factor when assessing the privacy impact on the data subjects, particularly when the processing is monitoring and behavioural analysis:

> *Assessing impact in a wider sense may involve considering whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes).*[44]
>
> *[...]*
>
> *In addition to potentially leading to the processing of more sensitive data, such analysis may also lead to uncanny, unexpected, and sometimes also inaccurate predictions, for example, concerning the behaviour or personality of the individuals concerned. Depending on the nature and impact of these predictions, this may be highly intrusive to the individual's privacy.*[45]

Collecting personal data about all visitors to online newspapers and other online news sources, tracking the data subjects across other websites and monitoring their online behaviour, analysing this behaviour and creating interest groups, as well as sharing them with third parties adversely affects the fundamental rights and interests of the data subjects in a negative way.

[43] Opinion 06/2014, p. 37.
[44] Opinion 06/2014, p. 39.
[45] Opinion 06/2014, p. 39.

Furthermore, the reasonable expectations of the data subjects is a relevant factor in the balancing test.[46]

> *The reasonable expectations of the data subject with regard to the use and disclosure of the data are also very relevant in this respect. As also highlighted with regard to the analysis of the purpose limitation principle, it is 'important to consider whether the status of the data controller, the nature of the relationship or the service provided, or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use.*

Disqus has tracked the online behaviour of all visitors to the websites, regardless of whether they were registered Disqus users or not. The unregistered users, and arguably the registered users, had no reasonable expectation of this use of their personal data; see also our assessment under section 5.6. The unregistered users had no direct relationship with Disqus, and had no way of expecting the invasive tracking, profiling and disclosure Disqus has conducted when visiting a news site that happened to run the Disqus widget.

The data subjects furthermore had no reasonable expectation of having their personal data used to create aggregated interest groups, and to have their data shared with third party online advertising companies. Natural persons have a reasonable expectation of not being tracked and profiled when reading news articles, unless otherwise informed.

Finally, we consider the following guidance by WP29 as particularly relevant for the present case:

> *In this respect, it is useful to recall the Working Party's Opinion on purpose limitation, where it is specifically stated that 'when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers .... free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research.*[47]

Disqus' interest in providing behavioural online marketing and business interests are less important compared to the adverse negative effects on the data subjects, and must weigh significantly less in the balancing of interests.

We consider the disclosure of personal data to Zeta Global, as well as Disqus' third party advertising partners like Viglink to be a particularly aggravating factor in the present case.

---

[46] Opinion 06/2014, p. 40.
[47] Opinion 06/2014, p. 47.

This constitutes a very negative interference in the data subjects' right to data protection, as well as freedom of expression and information.

You provide the following information regarding "Data recipients" on your website:

> *We work with LiveRamp to help marketers connect browsers and devices with data from other sources that has been obfuscated to remove any directly identifying information. LiveRamp provides a privacy policy and opt-out options.*
>
> *We share [the data subjects] web browsing activity with Viglink to allow advertisers to personalize ads based on the types of products and services in which [the data subjects] seem to be interested. You may read Viglink's privacy policy and opt-out.*
>
> *We share [the data subjects] web browsing activity with Disqus' parent company, Zeta Global, to enable personalized marketing based on [the data subjects] perceived interests. Please see Zeta's privacy policy.* [48]

Your website informs the following concerning Disqus' use of tracking cookies and ad service:

> *Disqus uses "authentication" cookies, e.g., `sessionid`, `disqusauth`, and `disqusauths`, to keep you logged in from your web browser and personalize your Disqus experience.*
>
> *Disqus uses "unique" cookies, e.g., `disqus_unique` and `_jid`, to associate web-based activitieswith a page load and with a web browser, including activities that violate our Terms of Service, andunderstand your interests and product usage.*
>
> *When Disqus loads ads, we use ad serving technologies from Google that may set cookies for the purposes of personalized marketing, associating ads with later activities, and limiting how you are shown specific ads.*

The NRK news articles from November and December 2019[49] described how the privacy consulting company Conzentio has conducted tests of the Disqus widget and your data collection.

The NRK further described how the tests showed that Disqus shared the personal data with third party advertising partners and its parent company Zeta Global. The articles state that Disqus' collection and sharing of personal data took place without a valid consent pursuant to

---

[48] https://disqus.com/data-sharing-settings/ (Last seen 26.04.21)

[49] https://nrkbeta.no/2019/11/18/nettstedet-deres-sendte-besoksdata-til-81-selskaper/ (Last seen 26.04.21)
https://nrkbeta.no/2019/12/18/disqus-delte-persondata-om-titalls-millioner-internettbrukere-uten-at-nettsidene-visste-om-det/ (Last seen 26.04.21)
https://nrkbeta.no/2019/12/20/nrk-fjerner-kommentarfelt-pa-p3-og-ytring-etter-avsloring/ (Last seen 26.04.21)

the GDPR, and without the data subjects being informed by Disqus of this. According to one of the tests, Disqus disclosed personal data collected from rights.no with 81 third parties.[50]

Anders Willstedt of Conzentio states that their tests showed that the Disqus widget sent user data to a large number of third parties without the webpage owner or the users' knowledge. According to the NRK, the number of affected website users in Norway amounts to several hundred thousand.

These recipients may have subsequently disclosed the data to other recipients. Disqus disclosed the data to Zeta Global, which in turn is a marketing and advertising company

> *...that uses software and data about consumers to help advertisers reach selected audiences via online or in-app ads, email, direct mail, or telemarketing. Zeta collects and uses data about individual consumers in order to identify or predict the types of advertisements most likely to appeal to them.*

Zeta Global furthermore states in their privacy policy that

> *Recipients of our data include service providers who perform services for us like web hosting, data security services, or auditing, our advertiser clients, and companies that we may trade data with for purposes of Online Behavioral Advertising (see below).*

The Disqus privacy policy furthermore states that the company works with LiveRamp

> *to help marketers connect browsers and devices with data from other sources that has been obfuscated to remove any directly identifying information."*

The company also shares

> *[the data subjects] web browsing activity with Viglink to allow advertisers to personalize ads based on the types of products and services in which you seem to be interested.".*

The privacy policy also states that Disqus

> *shares [the data subjects] web browsing activity with Disqus' parent company, Zeta Global, to enable personalized marketing based on your perceived interests*

By making the personal data available to Zeta Global and your third party advertising partners as listed on your website, it is likely that the personal data has ended up in the hands of data brokers and other companies in the real-time bidding system[51] to be used for behavioural

[50] Nettstedet deres sendte besøksdata til 81 selskaper (nrkbeta.no) (Last seen 26.04.21).
[51] Real-time bidding is a method of selling advertising space on digital media through open digital automated auctions.

targeting.[52] We also note that Zeta Global, as well as your other third party advertising partners such as LiveRamp[53] and Viglink (now Sovrn)[54], have their own list of third party advertisers with whom they share data.[55]

Finally, we note that Disqus also seems to consider consent pursuant to Article 6(1)(b) GDPR to be the appropriate legal basis for the processing activities in the present case, as you inform us that consent is the legal basis on which you rely in your GDPR compliant layout for the Disqus widget.

Based on this assessment, our conclusion is that the data subjects' interests and rights and freedoms precedes Disqus' economical interest in online behavioural marketing, and that Disqus did not fulfil the balancing of interests when you carried out the processing activities mentioned in section 5.6.2. Disqus did not fulfil the third criteria in Article 6(1)(f) GDPR

Conclusion

Our conclusion is therefore that Disqus has processed the personal data of visitors to the websites between July 2018 and November 2019 without a legal basis pursuant to Article 6(1) GDPR.

6. Corrective measures

6.1 General principles when assessing administrative fines

An "administrative sanction" is a negative reaction that may be applied by an administrative agency in response to an actual breach of a statute, regulation or individual decision, and which is deemed to be a criminal sanction pursuant to the European Convention on Human Rights.[56]

The Norwegian Supreme Court (Rt. 2012 p. 1556) has concluded that an administrative fine is a penalty under Article 6 in the Convention on Human Rights.

As a result, we can only impose a fine where there is clear and convincing evidence of breaches of the GDPR.

Section 46 of the Norwegian Public Administration Act states the following:

> *When a statute prescribes that administrative sanctions may be imposed against an enterprise, such sanction may be prescribed even if no individual person is at fault.*

[52] "Behavioral targeting" describes the practice of monitoring people's online behavior and us-ing the collected information to show people individually targeted advertisements.
[53] https://liveramp.com/privacy/service-privacy-policy/ (Last seen 26.04.21).
[54] https://www.sovrn.com/legal/privacy-policy/ (Last seen 26.04.21)
[55] https://zetaglobal.com/privacy-policy/ (Last seen 26.04.21).
[56] Section 43 of the Norwegian Public Administration Act.

6.2 Whether to impose an administrative fine

We have found that there is clear and convincing evidence that Disqus has breached Articles 5(2), 6(1) and 13 GDPR. We deem it necessary to react against the breaches of GDPR and therefore notify you that we are considering issuing an administrative fine.

When deciding whether to impose an administrative fine, the NO DPA must take the factors listed in Article 83(2)(a)–(k) GDPR into consideration in each individual case. In the following, we will assess the case facts against these factors.

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

The principles of lawfulness, transparency, and accountability are fundamental conditions for processing personal data under the GDPR. In the present case, Disqus has breached these principles.

Disqus has processed a vast amount of personal data without a legal basis through the company's tracking, analyzing, profiling, and disclosure of personal data to third parties. This includes Zeta Global, to which Disqus' disclosed the unlawfully collected personal data in real-time. The third parties have most likely subsequently disclosed the data to a number of recipients and so forth, as this is the way the business model of online behavioral advertising works. The infringements in the present case have a large scope, which adds to the gravity of them.

Furthermore, the unlawful processing activities are invasive in nature, as we have described in section 5.7.3.

Tracking natural persons across websites without a legal basis and without the data subjects' knowledge constitutes a gross infringement of their fundamental right to data protection.

The unlawfully collected personal data was subsequently, analysed and used to profile the data subjects' by placing them in aggregated interest groups.

WP29[57] describes some challenges concerning profiling in their guidelines:

> *The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of*

[57] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 9.

> *comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.*

The EDPB[58] also summarises the risk to fundamental rights that are involved in profiling and targeting based on personal data, as has happened in the present case:

> *The combination and analysis of data originating from different sources, together with the potentially sensitive nature of personal data processed in the context of social media, creates risks to the fundamental rights and freedoms of individuals. From a data protection perspective, many risks relate to the possible lack of transparency and user control. For the individuals concerned, the underlying processing of personal data which results in the delivery of a targeted message is often opaque. Moreover, it may involve unanticipated or undesired uses of personal data, which raise questions not only concerning data protection law, but also in relation to other fundamental rights and freedoms.*

In addition to analyzing and profiling for the purpose of serving online behavioral advertising, Disqus has made the personal data available to multiple third party advertising partners. This large-scale dissemination of personal data related to natural persons online browsing activity could inter alia lead to manipulation of data subjects. This also adds to the gravity of the infringements.

Disqus has also failed to provide the data subjects with the legally required information pursuant to Article 13 GDPR. The data subjects in the present case had no reason to expect that they upon visiting one of the Websites would have their personal data tracked, profiled, and disclosed to third party advertisers. The right to information under the GDPR is one of the fundamental safeguards for enabling data subjects to exercise their data protection rights under the Regulation. By not providing the required information, Disqus made it difficult for the data subjects from exercising their data protection rights. This included their right to object to Disqus' processing of their data pursuant to Article 21 GDPR. The nature and consequence of this breach adds to the gravity.

The number of data subjects affected are one of the relevant conditions when considering whether to impose an administrative fine. According to the WP29 guidelines on administrative fines, the number of data subjects involved should be assessed, in order to identify whether this is an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place.[59]

Upon our request, Disqus is not able to provide us with information on how many data subjects in Norway were affected by the unlawful processing, as you inform us all the data from the relevant period is now erased. You can however confirm that you currently have 10 377 active Norwegian Disqus users that registered between May 2018 and December 2019.

---

[58] EDPB Guidelines 8/2020 on the targeting of social media users, para 4.
[59] WP 253 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, p. 10.

The amount of affected data subjects is therefore a minimum of 10 377. However, the actual number of affected data subjects is most likely to be much higher, as you have confirmed that you placed cookies in the browsers of all users who visited the Websites running the Disqus Widget between May 2018 and December 2019.

NRK.no/ytring, P3.no, tv.2.no/broom, khrono.no, adressa.no, rights.no and document.no are all large Norwegian media outlets with a large number of visitors. The websites owned by NRK have a particularly large number of visitors.

According to publicly available numbers, NRK.no and all its subpages combined had on average 5.4 million unique visits from mobile devices each week in 2019.[60] The same statistics show that NRK.no received over 4 million unique visits from PCs and tablets each week.

This indicated that the number of affected data subjects in Norway affected by the illegal processing activities, from the Websites combined, equals several hundred thousand, if not over a million individual users. This estimate is also supported by the tests conducted by Conzentio and NRK, as referred to in one of the NRK articles.[61] We find this indicative of a systemic breach, which is an aggravating circumstance.

The duration of the infringement may also be illustrative of, for example failure to take appropriate preventive measures.[62]

As the GDPR became applicable in Norway in July 2018, Disqus' illegal processing of personal data happened between 20 July 2018 and 12 December 2019. The processing first stopped when Disqus was made aware of the GDPRs applicability by NRKs news articles in November 2019. By this time, the GDPR had been applicable for more than a year. We find this indicative of a failure to take appropriate preventive measures to protect the personal data of the affected data subjects in this case.

(b) the intentional or negligent character of the infringement

According to Disqus, the processing activities in the present case have been carried out because the company was unaware that the GDPR applies to data subjects in Norway.

Our assessment is that Disqus breach of the accountability principle, as concluded in section 5.5, is indicative of negligence.

---

[60] The Norwegian National Broadcaster (NRK) 2019 Annual Report https://fido.nrk.no/2d7ba53aecb7173b72f7dd0fa736ad942e6ee09573d5035fb86a9fc09c2305b6/allmennkringkasterregnskapet_2019_statistikk_ny%20pr%20270520.pdf, p. 15.
[61] https://nrkbeta.no/2019/11/18/nettstedet-deres-sendte-besoksdata-til-81-selskaper/ (Last seen 15.02.21)
[62] WP 253 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, p. 11.

According to EDPB guidelines, other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence.[63]

According to Disqus' website, Disqus is in use in 191 countries, it has 2 billion "monthly uniques" and 50 million monthly comments, and the company was started in 2007.[64] Disqus is a large professional actor providing comments plugins for websites across the world, as well as a large professional actor within online marketing. According to your privacy policy, "Disqus is a networked community platform used by hundreds of thousands of sites all over the web".

Once Disqus is present on a website, and fulfils the criteria for being a controller pursuant to Article 4(7) GDPR by processing personal data for the company's own economical purposes, Disqus is responsible for ensuring and being able to demonstrate compliance with the GDPR in accordance with Article 5(2).

A large company like Disqus must ensure compliance with all applicable data protection legislation when providing its services. We find the company's failure to identify the applicable law to be indicative of negligence.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

Disqus has informed us that the company has erased the personal collected on data subjects in Norway between May 2018 and December 2019. In principle, this is an action that may mitigate the damage suffered by the data subjects.

However, in the present case Disqus has disclosed the personal data to a number of third party advertising partners, including Zeta Global in real-time, during a time period of about one and a half years.

Disqus' erasure of the personal data does not remedy the infringement that occurred when the personal data was disclosed to a number of third parties without a legal basis. The third party recipients have subsequently most likely disseminated the personal data to a vast amount of their third party advertising partners, as is the nature of online behavioural advertising, thus rendering Disqus' erasure of the personal of little significance to the affected data subjects in the present case. This means that there is no way of ensuring that the illegally collected personal data effectively has been erased.

Based on this, the nature, gravity and duration indicated several aggravating factors and points to the direction that an administrative fine is appropriate.

---

[64] https://disqus.com/company/ (Last seen 02.05.21).

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

We do not consider this relevant.

(e) any relevant previous infringements by the controller or processor

We are not aware of any previous infringements.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

Disqus has cooperated with the NO DPA by providing information and answering our questions. Therefore, we consider that this factor is not relevant in the present case.[65]

(g) the categories of personal data affected by the infringement

The personal data unlawfully processed in the case is online behavioural data, which includes cookie IDs, IP-addresses, browsing history (websites and time of visit), and aggregated interest groups. An IP-address may also infer the user's location at a country or city scale.

Online behavioural data should in itself be processed with due consideration, particularly with regard to which news sites a data subject has visited. Furthermore, tracking a person's visit to news sites can make it possible to infer special category data like their political opinion.

Our assessment is that some of the personal data Disqus has processed in the present case may reveal special category data like the data subjects' political opinion.

Disqus has tracked and profiled natural persons based on what websites they have visited and what content they have read. Information relating to what a natural person read online, and tracking and analysing of this data over time, may reveal a lot about that individual person. This is highly private information, which we consider an aggravating factor.

What news sites a person regularly reads, how a person interacts with that news site, and what articles they read, may over time infer special category data like political opinion pursuant to Article 9 GDPR. In the present case, Disqus has tracked some data subjects across the internet for almost a year and a half.

The websites affected in the present case include rights.no and document.no. These websites are commonly associated with specific political points of view, that may be characterized as marginal, and that are shared by a minority of the population. The views commonly expressed by said sites may in some cases be regarded as controversial or "extremist" in the eyes of the majority. Information about data subjects who are visitors to these websites might therefore

[65] According to the guidelines in WP 253 p. 14, letter (f) could be a mitigating factor in some cases, however it would not be appropriate to give regard to cooperation that is already required by law.

reveal special categories of personal data, which may associate a number of those visitors to certain specific political opinions. Thus, information about those website visitors may be potentially stigmatising. Especially tracking of the data subjects' use of these websites over time may reveal their political opinion.

Furthermore, NRK P3 (p3.no) is the website of the NRK radio channels P3 and MP3. NRK P3 is a radio channel with youth as its target audience, which also produces online content including web series directed towards young adults and teenagers. NRK MP3 is also a radio channel with teenagers as its target audience. [66] As Disqus tracked and profiled all visitors to the websites for online behavioural advertising, we find it highly likely that there are children (natural persons under 18) among the affected data subjects.

Pursuant to Recital 38 GDPR:

> *Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.*

We consider the fact that there highly likely are children among the data subjects to be an aggravating factor.

In conclusion, we consider the categories of personal data to be an aggravating factor, which indicates an administrative fine is appropriate.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

We were made aware of the infringement through news articles by NRK and Computerworld, and not by Disqus. Based on the articles the infringements seemed to have been discovered merely by chance by Conzentio when they were investigating a Swedish website. Had they not pursued the findings, it would have been difficult for the data subjects to discover the processing and take action against Disqus themselves. We therefore consider this to be an aggravating factor.

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

[66] https://www.nrk.no/informasjon/et-bredt-og-variert-medietilbud-1.6511989 (Last seen 27.04.21).

We are not aware of any previously corrective measures against Disqus with regard to the same subject matter.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

We do not find this relevant.

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Disqus has informed us that it does not sell advertisements to Norwegian websites, and that it is not likely that the data Disqus has collected from Norwegian data subjects were used to provide online marketing. However, Disqus has informed us that it cannot guarantee that data subjects in Norway have been served ads.

Disqus is used in 191 countries, and is present on a very large number of websites, including American websites to which it sells advertisements. Based on Disqus' vast online presence, we find it likely that data subjects in Norway have visited one of the several hundred thousand websites where Disqus advertises,[67] and thus have been served ads through online behavioural advertising by Disqus. As advertising is the predominant way Disqus makes money, our assessment is that the infringements have resulted in financial benefits for the company. This is an aggravating factor, indicating that an administrative sanction is appropriate.

Our assessment is that Disqus has collected, tracked, and analyzed vast amounts of personal data for the creation of aggregated interest groups and individual profiling, which in turn has been used to deliver online advertisements, and that these practices constitute the very essence of the business model. Consequently, the unlawful processing has led to financial benefits for Disqus.

According to WP29[68], profit from infringements is a strong indication that a fine should be imposed:

> *Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.*

The arguments we have presented clearly indicates that an administrative fine should be imposed in the present case.

---

[67] https://blog.disqus.com/the-numbers-of-disqus (Last seen 27.04.21).
[68] WP 253 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, p. 16.

6.3 Deciding the amount of the administrative fine

Article 83(1) GDPR provides the following guidance when deciding the amount of administrative fines:

> *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*

In accordance with Article 83(2), the NO DPA must also take due regard to the arguments in 6.2 above when assessing the amount of the administrative fine.

The argumentation in section 6.2. shows several aggravating factors and suggests a high amount.

The infringements found in the case qualifies for the administrative fines under Article 83(5), which is "up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher".

When considering an administrative fine, it is relevant for the NO DPA to take into consideration similar cases from other supervisory authorities in the EEA. We have not found any directly comparable cases. However, we have taken into consideration cases where the supervisory authorities sanctioned infringements of the same Articles of the GDPR as in this case; Articles 5(1) and (2), 6, 12 and 13 GDPR.

The French supervisory authority (the CNIL) imposed an administrative fine of 50 000 000 EUR on Google Inc. In the case, Google was found to have breached the GDPR requirements for transparency and information to the data subjects, as well as lacking a legal basis for online advertising.[69]

The Spanish supervisory authority (the AEPD) imposed an administrative fine of 6 000 000 EUR to Caixabank S.A. for failing to give its customers adequate information pursuant to Articles 13 and 14 GDPR, as well as lacking a legal basis pursuant to Article 6(1) GDPR for disclosing personal data to other companies within the CaixaBank group.[70]

The amount must be "effective, proportionate and dissuasive" in each individual case, pursuant to Article 83(1). We therefore find Disqus' annual turnover relevant in our assessment.

[69] https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc. (Last seen 26.04.21).
[70] https://www.aepd.es/es/documento/ps-00477-2019.pdf. (Last seen 26.04.21).

There is limited public information about Disqus global. However, according to an interview with Disqus CEO Dan Ha in 2018, your global revenue was around 20 000 000 USD (approximately 186 698 000 NOK). [71] Based on the information about Disqus available on the company's website, our assessment is that Disqus' global revenue has increased since then.

We have taken into consideration the nature and gravity of the infringements, including the unlawful and opaque processing of online behavioral data. Furthermore, the present case constitutes a fundamental breach of the accountability principle, the fact that the duration of the infringement was approximately one and a half years, and the amount of data subjects amounting to several hundred thousand. We also consider the disclosure to third parties, with the consequence of an effective loss of control over personal data, as a particularly aggravating factor when calculating the amount. Finally, we refer to our assessment of aggravating factors in section 6.2.

Having considered these factors, our assessment is that a fine of 25 000 000 NOK (approximately 3 000 000 USD or 2 490 000 EUR) will have the effective, proportionate and dissuasive effect the GDPR prescribes, in light of Disqus estimated annual global turnover. The amount constitutes approximately 15 % of Disqus' estimated turnover in 2018.

If the Covid-19 situation has affected you in a way that is relevant to our notified decision, please explain why and provide relevant documentation.

7. Process

If you have comments or remarks to this advance notification, we ask that you send them to postkasse@datatilsynet.no by **Monday 31 May 2021 at 12 noon Oslo time (CET).** A final decision will then be taken.

8. Access to documents

Subject to the Norwegian Public Administration Act Section 18 and 19, you – as a party to this case – have the right to acquaint yourself with the documents in this case. As you have already been informed, correspondence with the NO DPA is subject to freedom of information requests under the Norwegian Freedom of Information Act.

9. Concluding remarks

Although we have chosen to focus our investigation on the legitimacy of Disqus' practice of tracking, profiling, and disclosing personal data between July 2018 and December 2019, there might be additional issues regarding e.g. Disqus' continued processing of personal data related to the user profiles that were registered between 20 July 2018 and 12 December 2019.

[71] https://nathanlatka.com/thetop990/ (Last seen 26.04.21).

The fact that some issues have fallen outside the scope of our investigations, does not mean that those issues should not be addressed. Disqus needs to make sure that the processing of personal data relating to data subjects in the EEA is compliant with the GDPR at all times. We may decide to investigate additional issues later on, following individual complaints or *ex officio*, see the tasks and powers of the supervisory authorities laid down in Articles 57 and 58 GDPR.

If you have any questions regarding this letter, you can contact legal adviser Ole Martin Moe at omm@datatilsynet.no.

Kind regards

Bjørn Erik Thon
Data Protection Commissioner

Ole Martin Moe
Legal Adviser

This letter has electronic approval and is therefore not signed