Datatilsynet

**The Norwegian Data Protection Authority**

Disqus Inc.
717 Market St, Suite 700
San Francisco CA 94103
USA

| Your reference | Our reference | Date |
|---|---|---|
| | 19/03852-4/OMM | 08.05.2020 |

## Order to provide information – Disqus Inc – Collection and sharing of personal data

Datatilsynet is the Norwegian Data Protection Authority and the national supervisory authority under the European Union General Data Protection Regulation (GDPR). Our task is to supervise compliance of the GDPR and oversee that both public and commercial actors do not violate Norwegian citizens' fundamental right to data protection.

### Case background

Datatilsynet have through news articles by NRK (the Norwegian National Broadcaster) been made aware that Disqus has collected and shared personal data about Norwegian residents to third parties, including ad companies.[1] According to the articles, the collection and sharing happened through the Disqus plugin comment sections on websites of Norwegian companies. This includes online newspapers and broadcasters like TV2 (TV2 Gruppen AS), NRK, Khrono, ComputerWorld and Document.no.

The articles state that NRK and the privacy consulting company Conzentio have conducted tests that show that Disqus collected personal data about data subjects in Norway who used your comment plugin. According to the tests, Disqus subsequently shared the personal data with third party advertising partners of Disqus and its parent company Zeta Global.

The articles state that Disqus' collection and sharing of personal data happened without a valid consent pursuant to the GDPR, and without the data subjects being informed of this. Megan Rose of Zeta Global confirms this in the article from the 18th of December 2019. Rose further says that Disqus collected personal data about Norwegian residents by mistake, and explains that this happened because the company failed to include Norway in their GDPR layout, as it is not an EU member state. Neither Zeta Global, nor Disqus comments the alleged sharing of personal data.

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

According to Rose, Norway, Liechtenstein and Iceland were to be included in their GDPR layout soon. She further states that data about Norwegian citizens were to be deleted soon, but that this would take some time. The data subjects would then have to register again in order to use Disqus' comment field plugins.

The Disqus privacy policy, as per the 20th of April 2020, states that the company works with multiple third party ad partners, including AppNexus, OpenX and Oath. Section 6 of your privacy policy further states that Disqus may share personal data with Zeta Global as an internal third party, as well as an extensive list of external third parties, including LiveRamp and Vigling with the purpose of "helping marketers connect browsers with data from other sources", and in order to "allow advertisers to personalize ads…".

Based on this information, we find it likely that Disqus has processed personal data about Norwegian residents without complying with the fundamental data protection principles pursuant to the GDPR. This case raises several issues as addressed below, which we require your feedback on as further explained in "Order to provide information".

**Territorial scope**
Article 3(2) GDPR prescribes that the Regulation applies to the processing of personal data of data subjects in the European Union by a controller not established in the Union, where the processing activities are related to the offering of goods or services to data subjects in the Union. As the Disqus comment section plugin is available to data subjects in Norway, your processing of personal data about Norwegian residents falls within the territorial scope of the GDPR.

**Competence**
According to the information available to us, it appears that Disqus, Inc. is the controller for the processing of personal data for marketing purposes in the context of the Disqus tool. It also appears that you do not have an establishment in the EEA. Therefore, 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).

**Legal background**

*The responsibility of the controller*

The controller is responsible for, and must be able to demonstrate compliance with GDPR, as stated in Article 5(2).

The responsibility of the controller is also regulated in Article 24 and further specified in Article 25.

*Lawfulness of processing*

According to Article 5(1)(a), personal data must be processed "lawfully, fairly and in a transparent manner in relation to the data subject". This is a fundamental data protection principle.

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

If the controller relies on Article 6(1)(a), consent, Article 4(11) stipulates that consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 7 sets further conditions for a consent to be valid:

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. *If the data subjects consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

*Transparency*
The transparency principle is one of the fundamental data protection principles, see Article 5(1)(a) GDPR.

Article 13 sets forth the specific information the controller must provide when data is collected from the data subject. This includes information about the purposes for processing, the legal basis and recipients of personal data. The controller must provide the information "at the time when personal data are obtained".

Article 12(1) establishes the information requirements and how information should be communicated to the data subject. The article specifies that the controller must take "appropriate measures" to provide any information referred to in Article 13 and any communication under Article 15 "in a concise, transparent, intelligible and easily accessible form, using clear and plain language [. . .]"

*Notification regarding erasure of personal data*
Article 19 states that the controller shall communicate erasure of personal data carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

*Notification of a data breach to the supervisory authority and communication to the data subject*
Article 33 requires the controller to report personal data breaches to the supervisory authority without undue delay, and not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The definition of "data breach" in Article 4(12) includes unlawful disclosure of, or access to personal data, as well as any other form of processing which violates the GDPR.[2]

Article 34 requires the controller to communicate personal data breaches to the data subject where the breach is likely to result in a high risk to their rights and freedoms. Article 34(3) lists the exceptions from this requirement.

*The powers of the supervisory authority*
As a supervisory authority, we have investigative and corrective powers pursuant to Article 58. We have, inter alia, the power to issue warnings and reprimands to a controller, to impose limitations including a ban on processing and to impose an administrative fine pursuant to Article 83.

[2] Guidelines on Personal data breach notification under Regulation 2016/679, p. 7.

**Order to provide information**
Pursuant to the Norwegian Personal Data Act Section 23 and Article 58(1)(a) GDPR, we have the authority to order the controller to provide any information we require for the performance of our tasks.

We require Disqus to provide your response to the facts of the case as presented in this letter, as well as the following information:

1. What types of personal data did Disqus collect about Norwegian residents? When did the collection start, and when did it stop?

2. How many Norwegian residents did you process personal data about?

3. Did you share the personal data with third parties? If so, with whom?

4. What lawful basis did you have for collecting this personal data, and for sharing it with third parties?

5. What information did you provide to Norwegian residents about your processing of their personal data?

6. Have you erased the personal data about Norwegians residents?

7. Have you notified the Norwegian users pursuant to Article 34 GDPR that their data was shared with third parties without a lawful basis? If yes, explain how you notified them. If no, explain why not.

8. Please explain why you have not notified the Norwegian Data Protection Authority about the unlawful processing pursuant to Article 33 GDPR.

9. Have you notified any third parties with whom you may have shared this data pursuant to Article 19 GDPR? If so, please explain how you notified them. If not, please explain why.

10. In the article, Rose states that Norewegian users were soon to be included in Disqus' GDPR compliant layout. Are Norwegian users now included in this layout? If so, please demonstrate the changes you have made to ensure this, including how Norwegian residents may now give and withdraw their consent pursuant to the GDPR.

11. Please inform us of any other relevant measures Disqus has taken to remedy the unlawful processing.

We kindly ask that you reply to us by the **19th of June 2020.**

**The right to not incriminate oneself**
In line with the Norwegian Public Administration Act Section 48, we inform you that you may have a right to not answer questions or disclose documents or objects when the answer or such disclosure may subject you to an administrative sanction.

**The right to appeal**
You may lodge an appeal against the order to provide information in accordance with the Norwegian Public Administration Act Section 14. Note that the right to appeal only applies if you consider that you are not under an obligation or lawfully entitled to provide the information. An appeal must be lodged within three days of having received this letter. If we uphold our order, we will send the appeal case to Personvernnemnda, our appeal body.

**Your access to case documents**
You have a right to acquaint yourself with the documents in the case pursuant to the Norwegian Public Administration Act Section 18, unless Sections 18 to 19 provide otherwise.

**Public access**
We also want to inform you that as a main rule, all case documents are subject to public access in accordance with the Norwegian Act of Freedom of Information Section 3. If you claim there is legal basis to partly or entirely exempt your response from the right of public access, please specify which parts and express your arguments on the matter.

If you have any questions regarding the case, please contact legal advisor Ole Martin Moe by e-mail omm@datatilsynet.no or by telephone +47 22 39 69 00.

Kind regards,

Ylva Marrable
Head of Datatilsynets Section for Private Services

Ole Martin Moe
juridisk rådgiver

*This letter has been electronically approved, and is therefore without signatures.*