

Your reference

Our reference
21/02455-2

Date
28.06.2021

Order to provide information regarding "Shinigami Eyes"

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 with the GDPR and oversee that both public and commercial actors do not violate the rights of data subjects in Norway.

Datatilsynet has received a complaint against "Shinigami Eyes".

Case background

According to the complaint, and your website (<https://shinigami-eyes.github.io>), Shinigami Eyes is a browser extension/addon that highlights transphobic and trans-friendly social network pages and users with different colours. The addon is available for Chrome, Firefox and Firefox for Android.

We have received a complaint from individuals who have been marked through your abovementioned application.

Competence of the Norwegian Data Protection Authority

Territorial scope – Article 3 GDPR

Where the controller or processor do not have an establishment within the EEA, the GDPR may still be applicable in accordance with Article 3(2) GDPR:

This 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*
- b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

The complaint informs us that individuals in the EEA/Union have had their personal data processed by Shinigami Eyes.

The subsequent question is whether Shinigami Eyes have been "monitoring" the data subjects' behaviour, as far as it takes place within the EEA/Union.

Recital 24 of the GDPR provides relevant guidance:

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

As far as we understand, Shinigami Eyes will mark those individuals it deems to be either trans-friendly or anti-trans with a certain colour. This enables other users to quickly identify individuals that have in the past and might again in the future make statements that they view as either trans-friendly or anti-trans. Shinigami Eyes' purpose appears to be to track individuals on the internet/social media in order to analyse and predict their attitudes and behaviour. Thus, in our view Shinigami Eyes is monitoring the data subjects' behaviour

In conclusion, the GDPR is applicable to Shinigami Eyes' processing in question, based on Article 3(2) GDPR.

Competence – Article 56 GDPR

We have not been able to identify any establishments for Shinigami Eyes within the EEA. Therefore, pursuant to Article 56(1) GDPR, the cooperation mechanism set out in Chapter VII Section 1 GDPR does not apply, and therefore the Norwegian Data Protection Authority is competent to handle the matter pursuant to Article 55(1) GDPR.

Legal background

Controller – accountability principle

The controller shall be responsible for, and be able to demonstrate, compliance with the GDPR, see Article 5(2) GDPR.

To the extent that you determine the purposes for which the data are processed and the means of the processing, you are a controller, see Article 4(7) GDPR.

Lawfulness of processing

GDPR applies to the processing of personal data, wholly or partly by automated means.

Personal data only includes information relating to natural persons (data subjects) who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information. This may include online identifiers, see Article 4(1) GDPR.

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

You must determine whether you have a lawful basis before you begin the processing, and the assessments should be documented.

Article 6(1) GDPR prescribes that personal data can be processed lawfully if the:

(...) 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

There are three elements to this assessment. First, you must identify a legitimate interest. Second, you must demonstrate the necessity to process personal data for the legitimate interests pursued. Thirdly, the fundamental rights and freedoms of the data subject whose data require protection must not take precedence over the legitimate interests pursued. Thus, you must balance the legitimate interests pursued against the data subjects' interests, rights and freedoms.

The legitimate interests can be your own or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.

Special categories of personal data

Article 9(1) GDPR prohibits the processing of special categories of personal data. This includes personal data revealing political opinions and personal data concerning a person's sex life or sexual orientation.

However, there are exceptions to this general prohibition in Article 9(2) GDPR.

Right to object

To the extent personal data is being processed based on, inter alia, Article 6(1)(f) GDPR, Article 21 GDPR provides the data subject with the right to object to their personal data being processed. In that case, the controller shall not process the personal data in question unless the controller is able to demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Obligation to facilitate for the rights of data subjects

Article 12(2) GDPR states that the controller is responsible for facilitating the exercise of data subject rights under Articles 15 to 22 GDPR. This implies that the controller must dedicate sufficient resources and implement the necessary systems to be able to address, for example, access requests from the data subjects in accordance with Article 15 GDPR.

Right of access to personal data

The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning the data subjects are being processed, and, where that is the case, access to the personal data, see Article 15 GDPR.

The data subject has a right to receive information as described in Article 15(1) letters a-h, including information on whether the establishment has transferred the data subjects personal data, and if so, to whom the data has been transferred.

According to Article 15(3) GDPR, the data subject has a right to receive a copy of the personal data that is processed. The data subject shall receive this free of charge.

Obligation to respond to data subject requests

Pursuant to Article 12(3) GDPR, the controller is required to respond to access requests without undue delay, and usually within one month of receipt of the request.

Order to provide information

Pursuant to the Article 58(1)(a) GDPR, Datatilsynet can order you to provide any information we require to perform our tasks. On that basis, we ask you to answer the following questions:

1. What is your lawful basis to process personal data? We are particularly interested in the lawful basis for the processing that takes place when an individual is marked as either trans-friendly or anti-trans. Please provide relevant documentation. If the processing is based on your legitimate interests, please provide your assessment pursuant to Article 6(1)(f) GDPR.
2. What measures have been implemented in order to respond to data subjects that choose to exercise their rights in accordance with GDPR? This includes facilitating for the right of access, rectification, objection and deletion.
3. To the extent that you are relying on Article 6(1)(f) GDPR as a legal basis, how do you assess any objections received from data subjects concerning the processing of their personal data, pursuant to Article 21 GDPR?
4. The purpose of Shinigami Eyes appears to be to identify what political opinions certain individuals have, and to mark them accordingly. If this is correct, what exception under Article 9(2) GDPR are you relying on? If you object to this description, please clarify the purpose of the processing.
5. How do you provide information to the data subjects concerning the processing of their personal data? Please provide relevant documentation.
6. What measures have been implemented in order to ensure that the reports your application receive from its users (i.e. reports that identify which individuals your users believes should be marked as either anti-trans or trans-friendly by your application) is in fact based on the criteria you have set out in the guideline on your website? In other words, how do you ensure that the marking individuals receive through your application is correct in light of the purpose of the application?

7. Did you conduct any risk assessment as to the consequences for the data subjects' rights and freedoms before launching Shinigami Eyes? This includes, but is not limited to, the varying risk of data subjects receiving sanctions or other negative reactions because of the marking they have received by Shinigami Eyes. This could include negative reactions both to being marked as either anti-trans or trans-friendly.
8. Provide further insight and explanation as to the technical sides of the application, and what data you are processing. In particular, we want information on whether you have a database/overview of all the data subjects marked as anti-trans and/or trans-friendly. Furthermore, whether you have a database/overview on the individuals who are merely reported as either anti-trans or trans-friendly, even though this reporting has not necessarily led to the data subject being marked in the extension/addon.
9. What safety measures are in place in order to ensure that the database/information you have obtained through the application is not disclosed in an unauthorised manner to third parties?
10. Provide information as to whether you are sharing the information/data you have obtained through your application with any third parties.

We kindly ask that you reply to us **by the 10th of August 2021**. Please attach relevant documentation to support your answers. You may find our postal address on the first page of this letter.

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 Personvernemnda, 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.

Publicly accessible and duty of confidentiality

We would like to inform you that the documents in this case are publicly accessible in accordance with Norwegian law. If, in your view, there is any reason to except this document from being publicly accessible, we request you to provide us with a justification.

Datatilsynet is required to maintain confidentiality of the complainant's identity and other personal information. We hereby inform you that you should not share with others any information concerning the complainant, which you receive from us.

Jørgen Skorstad
Director, law

Carl Emil Bull-Berg
Legal advisor

Kristian Bygnes
Legal advisor

This letter has electronic approval and is therefore not signed

Copy: Complainant