Datatilsynet

Shinigami Eyes

Your reference	Our reference	Date
	21/02455-11	14.06.2022

Ban on processing - Shinigami Eyes

1. Background

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 the browser extension/addon "Shinigami Eyes". According to the complaint, and the extensions 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. The complaint in question was received from a Norwegian individual who had been marked through the application.

On this background, Datatilsynet sent Shinigami Eyes an order to provide information on 28 June 2021, with a deadline to respond within 10 August 2021. Datatilsynet did not receive a response. Datatilsynet therefore sent Shinigami Eyes a reminder to provide information, with a revised deadline. Datatilsynet did not receive a reply to this reminder. Datatilsynet has made the case, including the order to provide information, public through our website, and the case has received press coverage from various news outlets.

We also sent an advance notification of our intent to impose a ban on the pertinent processing of personal data, as required by section 16 of the Norwegian Public Administration Act, on 16 December 2021. The notification included our assessment of the case, and our preliminary conclusion, i.e. that the processing of personal data in question was in breach of Article 6(1), Article 12(2) and Article 14 GDPR.

Postal address:	Office address:	Phone:	Ent.reg:	Home page:
P.O. Box 458 Sentrum	Trelastgata 3	+47 22 39 69 00	974 761 467	www.datatilsynet.no/en/
N-0105 OSLO	N-0191 OSLO			

The advance notification also included a reminder, in line with section 17 of the Public Administration Act, that any remarks to the advance notification should be sent to our e-mail address within 17 January 2022, and that we would then reach a formal decision.

We have not received any remarks or comments from Shinigami Eyes within the stated time limit. However, we have received some remarks from the complainant, in three e-mails on 21 December 2021 (cf. our comments to these remarks below in section 4.5).

Even without a response from Shinigami Eyes we have concluded that we have sufficient information in order to conclude on the legality of the browser extension, i.e. that the processing of personal data in question is in violation of Article 6(1), Article 12(2) and Article 14 GDPR.

2. Decision

> *Pursuant to Article 58(2)(f) GDPR, a ban is imposed on all Shinigami Eyes' processing of personal data related to their browser extension, "Shinigami Eyes", on Norwegian territory.*

3. Legal background

3.1. Territorial Scope – Article 3 GDPR

The Norwegian Personal Data Act incorporates the GDPR into Norwegian law.[1] The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

Pursuant to Article 3(2) GDPR, the GDPR applies to the processing of personal data of data subjects in the EEA 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 the Union; or*

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

3.2. Competence and tasks

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*

[1] LOV-2018-06-15-38

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

> *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.*

The concept of "main establishment" and "cross border processing" is further elaborated in Articles 4(16) and 4(23) GDPR.

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;*
>
> […]

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

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.*[2]

3.3. Controller – accountability principle

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

The entity that determine the purposes for which the data are processed and the means of the processing, is the controller, see Article 4(7) GDPR.

3.4. Personal data

[2] 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].

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.

3.5. Lawfulness of processing

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.

The controller must determine whether they have a lawful basis before they begin the processing, and the assessments should be documented.

Article 6(1)(f) 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, the controller must identify a legitimate interest. Second, they 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, the controller must balance the legitimate interests pursued against the data subjects' interests, rights and freedoms.

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

3.6. 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, or the right to object in Article 21 GDPR.

3.7. Obligation to provide information to the data subject

Article 14(1) and (2) GDPR lists the information the controller must provide to the data subject when personal data has not been obtained from the data subject, as well as when it shall be provided:

1. *Where personal data have not been obtained from the data subject, the controller shall provide the data subject with 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) *the categories of personal data concerned;*

    e) *the recipients or categories of recipients of the personal data, if any;*

    f) *where applicable, that the controller intends to transfer personal data to a recipient in 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 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 provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:*

    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) *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*

    c) *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 and to object to processing as well as the right to data portability;*

    d) *where 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;*

    e) *the right to lodge a complaint with a supervisory authority;*

    f) *from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;*

    g) *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. **Our assessment of the case**

4.1. Territorial scope

We have not been able to identify an "establishment" of Shinigami Eyes within the EEA, pursuant to Article 3(1) GDPR.

We must therefore assess whether the regulation applies on the basis of Article 3(2) GDPR.

The complainant informs us that individuals in Norway have had their personal data processed by Shinigami Eyes, hence the processing concerns data subjects "within the Union", see Article 3(2)(b) GDPR.

The subsequent question is whether Shinigami Eyes have been "monitoring" the data subjects' behaviour, see Article 3(2)(b) GDPR.

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.*

The browser extension marks those individuals it deems to be either trans-friendly or anti-trans with a certain colour. This enables other users to 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 in order to analyse and/or predict their attitudes and behaviour. Thus, in our view, Shinigami Eyes is "monitoring" the data subjects' behaviour, see Article 3(2)(b) GDPR.

In conclusion, the GDPR is applicable to Shinigami Eyes' activities, pursuant to Article 3(2) GDPR.

4.2. Competence

As stated above, 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.

Datatilsynet is furthermore competent to handle the complaint lodged against Shinigami Eyes pursuant to Article 55(1) GDPR, and also, there is an obligation pursuant to Article 57(1)(f) GDPR for the supervisory authorities to handle such complaints, cf. also Article 77 GDPR.

4.3. Material scope of the GDPR

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.*

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. The individuals in question will either be using their own names to register on the website (for example on Facebook), but may in other instances choose to use an online identifier that is not directly related to their own name (for example on Twitter). Regardless, processing the name or online identifier would be viewed as "personal data" in this context. Furthermore, Shinigami Eyes will not only be processing the online identifier and/or name of the data subject, but will also have to process personal data pertaining to the posts/behaviour of the data subject that has been reported as being either anti- or pro-trans, in order to conclude on whether they should be marked. When Shinigami Eyes communicates outwards to their users the "decision" they have made (either concluding that the individual is pro- or anti-trans), this will also constitute processing of personal data.

Shinigami Eyes processes "personal data", see Article 4(1) GDPR.

4.4. Controller

As stipulated above, the controller is the entity that determines the purpose and the means of the processing.

The European Data Protection Board (EDPB) states the following regarding how to identify the controller:

> *A controller determines the purposes and means of the processing, i.e. the why and how of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means")*

> *can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.*[3]

Shinigami Eyes determines the purpose of the extension/addon: the identification of those who are pro- or anti-trans. The relevant criteria and a guideline to ensure a coherent practice for marking online users is provided on the extension's GitHub-page.

Shinigami Eyes decides what means should be utilised, and how those means should be implemented in practice. It follows from the Privacy Policy that:

> *If your vote is deemed (through automatic and/or manual means) to be trustworthy, the bloom filter distributed in future versions of the extension **may** be modified to trigger a positive or negative (green/red) response to the entity you voted.*[4]

The Privacy Policy indicates that it is Shinigami Eyes which have a final say regarding which users are marked and added to the bloom filter in the available extension:

> *There is no guarantee that your vote will be taken into account. In all cases, you will however see the color of the labeled entity changing, because your overrides (stored locally by your web browser) always take the precedence over what the bloom filter would otherwise determine.*[5]

It is Shinigami Eyes that choses the marking-mechanism combined with a report system, where users of the extension can make suggestions in relation to which individuals should be marked.

To summarize, Shinigami Eyes determines the purpose of the extension and provides a guideline and criteria for marking online users to ensure that the personal data collected meets the purpose of the processing. In addition, Shinigami Eyes seemingly determines the means of how that personal data is processed from a combination of machine learning and manually vetting the accuracy of the collected personal data.

Datatilsynet concludes on this basis that Shinigami Eyes is the controller for the processing of personal data that occurs through the browser extension.

4.5. Lawfulness of the processing of personal data in the context of Shinigami Eyes

In the order to provide information, Datatilsynet requested information pertaining to the lawful basis relied upon by Shinigami Eyes. As previously stated, we did not receive a response from Shinigami Eyes.

Processing of personal data must have a lawful basis in Article 6(1) GDPR. In this case the most prospective legal basis to rely on is Article 6(1)(f) GDPR.

---

[3] Guidelines 07/2020 on the concept of controller and processor, version 2.0, adopted 07 July 2021
[4] https://shinigami-eyes.github.io/privacy-policy.
[5] Ibid.

As noted above, the controller must meet three cumulative conditions in order to rely on Article 6(1)(f) GDPR for processing personal data. These are the pursuit of a *legitimate interest* by the controller and *necessity* to process personal data for the purposes of the legitimate interests pursued. Lastly, the legitimate interests pursued by the controller or a third party must be balanced against the interests, fundamental rights and freedoms of the data subject (the balancing test[6]), and the interests pursued by the data controller or the third party must outweigh the interests of the data subjects.

The first question is whether Shinigami Eyes meets the condition of "legitimate interest".

Which interests meet 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, see Article 29 Working Party (WP29) Opinion 06/2014.[7]

This opinion is referenced by the EDPB in multiple guidelines relating to the GDPR, and is thus still relevant.[8]

The processing that occurs within the framework of the application is to enable users of the extension to readily identify which individuals are pro-trans or anti-trans. This purpose allows users to, for example, avoid conversations with individuals that may state opinions or otherwise behave in a manner that offends or harm them. On Shinigami Eyes' website the following is stated in relation to the purpose of the application:

> *As a transgender person, I got used to be distrustful towards people. While guessing the attitudes of an openly conservative person or group towards transgender people is easy, this is much more difficult when you deal with communities that tend to be moderately progressive or with intersectional interests, such as the feminist community, the lesbian community, women's associations and the atheist community.*
>
> *The purpose of this extension is to make transgender people feel more confident towards people, groups, and pages they can trust, and to highlight possible interactions with the trans-hostile ones (when this is not already evident, such as when discussing about common LGBT or feminist goals).*

Protecting people from such harm is, in our view, a legitimate interest. Therefore, the processing that occurs within and by Shinigami Eyes, through the browser extension, pursues a legitimate interest.

[6] EDPB Guidelines 8/2020 on the targeting of social media users, p.15.
[7] 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.
[8] See e.g. EDPB Guidelines 8/2020 on the targeting of social media users, para 50.

Subsequent to our advance notification of a ban on processing dated 16. December 2021, we received feedback from the complainant regarding the advance notification. The complainant criticised, in particular, our finding of a legitimate interest for the use of the browser extension.

In summary, the complainant argued that Datatilsynet agreed with the claims made by Shinigami Eyes that the use of the browser extension to map women, women's organizations and lesbians was harm-reducing. The complainant stated that as an extension of that view, Datatilsynet put the complainant and the users targeted by Shinigami Eyes in harms way. The reasoning being that according to the complainant, Datatilsynet depicts what in practice is a targeted harassment campaign against women, including death threats and active attempts at character assassination, as a legitimate activity.

Datatilsynet disagrees with the complainant's characterisation of our findings in the advance notification of 16. December 2021.

Datatilsynet reiterates the identified purpose of the application, mentioned directly above:

> *The processing that occurs within the framework of the application is to enable users of the extension to readily identify which individuals are pro-trans or anti-trans. This purpose allows users to, for example, avoid conversations with individuals that may state opinions or otherwise behave in a manner that offends or harm them.*

As will become clear below, Datatilsynet does not find that this legitimate interest overrides the interests of the data subject.

All three of the cumulative conditions of Article 6(1)(f) GDPR must be assessed separately and objectively, and the first condition of Article 6(1)(f) GDPR, namely the notion of "legitimate interest", is no exception.

In the abovementioned Opinion 06/2014, WP29 highlights the following:

> *In the view of the Working Party, the notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken.*[9]

In conclusion, and taking the complainant's objections into account, Datatilsynet still finds that Shinigami Eyes pursues a legitimate interest for the processing occurring within and by the browser extension for the purpose of identifying which individuals are pro- or anti-trans.

As mentioned, the legitimacy of the interest pursued is merely the first of three cumulative conditions set out in Article 6(1)(f) GDPR.

[9] Opinion 06/2014 p. 24.

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, under directive 95/46/EC:

> *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.*

It is difficult for Datatilsynet to conclude in relation to this criterion with full certainty, given the absence of information provided by Shinigami Eyes. However, the marking of individuals with a red or green colour does appear necessary to fulfil the purpose of the browser extension, which is to allow people to identify who is pro- and anti-trans. Processing their personal data, including reports made by users, is necessary in order to conclude on who should be marked.

The processing, as far as Datatilsynet understand, is "necessary" for the legitimate purpose identified above.

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

The third condition is the balancing test. The controller must perform a 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.

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 if 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, for example 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.[10] 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.*

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

Article 4(4) GDPR, 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[11] 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.*

[10] Opinion 06/2014, p. 30.
[11] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 6 and 7. The guideline was endorsed by the EDPB (01/2018) on its first plenary meeting.

> *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 make predictions about, for example, their:*
>
> - *ability to perform a task;*
> - *interests; or*
> - *likely behaviour.*

In this present case, Shinigami Eyes utilises an automated form of processing, as described on their website:

> *The initial version has been created through a mix of manual labeling and machine learning, but you can contribute with your own labels.*

Furthermore, the processing is performed on personal data, as examined above.

Finally, the purpose of the markings is to evaluate the data subjects, subsequently to communicate that evaluation to the community at large.

On this background, we have concluded that the processing activities in question constitutes "profiling", as defined by Article 4(4) GDPR.

Whether the processing falls within the scope of Article 4(4) GDPR does not directly determine the legality of the processing of personal data pursuant to Article 6 GDPR. It is, however, relevant in the assessment of the potential impact of the processing of personal data.

Furthermore, as stated above, the reasonable expectations of the data subjects is a relevant factor in the balancing test:

> *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.*[12]

In this case, the data subjects has no knowledge about the processing that takes place. The data subject does not have any relationship with Shinigami Eyes. The data subject therefore have no way of expecting that their messages and otherwise their behaviour on certain social media pages will be processed by and through Shinigami Eyes in order to decide whether they

[12] Opinion 06/2014, p. 40.

should be marked as anti- or pro-trans. Furthermore, they cannot have any expectation that this marking will be communicated to any and all who downloads the extension.

It is Datatilsynet's view that to be marked through Shinigami Eyes may entail negative consequences for the data subject, regardless of whether they are marked as being pro- or anti-trans. Being marked as anti-trans could cause one to lose their job, or friendships, and the individual could be the target of hate and mistreatment. Being pro-trans could, in certain communities (for example religious or very conservative communities), be construed as negative as well, similar reactions as described above could be imposed on the data subject. The negative impact must be viewed as particularly intensive, in light of the individualised nature of the marking, in addition to the data subject not having information about the marking nor understanding why they received such a marking. It is therefore also in particular difficult for the data subject to present an opposing view. This could also entail fear, irritation and other broader emotional impacts, which, according to the WP29, must be taken into account in this balancing act.

The negative impact on the data subject could be further enhanced by the fact that the data subject cannot not know the reason behind the marking, and in addition, neither do the users who download the application. This could entail that users may attribute negative aspects to, or make negative inferences about, the data subject, even though the acts of the data subject would not warrant such a reaction. For example, Shinigami Eyes may conclude that a certain individual is anti-trans, while the users themselves would disagree to such characterisation.

Furthermore, the creation and use of such applications may cause a chilling effect on the ability and willingness of individuals to participate in online discourse, through fear of receiving a marking and subsequently suffering negative consequences because of this. WP29 stated as following in their guidelines from 2014:

> *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.*[13]

In addition, it must be taken into account that since the processing is occurring without the appropriate information being provided to the data subjects, the data subject is prevented from exercising their right to object in accordance with GDPR Article 21. The lack of adequate information being provided to the data subject will be further examined below in its own section.

The interests of fundamental rights and freedoms of the data subject identified above must be weighed against the legitimate interests that Shinigami Eyes pursues with its application. As

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

stated above, to communicate to its users which individuals have a different opinion than themselves, or the same opinion, and therefore allowing their users to modify their behaviour accordingly (for example choosing to avoid certain individuals), is a legitimate interest. However, Datatilsynet needs to assess the *strength* of this legitimate interest, in order to make an assessment of the appropriate balance.

While using such tools as Shinigami Eyes could be useful for some, people have – regardless of Shinigami Eyes – the choice to not engage with specific individuals on their own accord. Individuals may, based on their own personal assessment, choose not to enter into a discourse with someone based on what they have said or what they have done. The main element of Shinigami Eyes is that the application removes the need for the individual to make their own assessment of whom they find to be pro- or anti-trans. While perhaps useful in certain situations, such a collective decision-making and categorisation could strengthen the echo chambers found online. Furthermore, such markings could be misused as a tool to specifically target individuals.

Consequently, the legitimate interest pursued by Shinigami Eyes cannot be assessed as one of significant strength or importance.

To summarize, Shinigami Eyes' processing of personal data creates various negative impacts for data subjects. Furthermore, the data subject receives no information regarding the processing, and the processing is clearly beyond the data subjects' reasonable expectation. While Shinigami Eyes pursues a legitimate interest, this legitimate interest is merely a substitute for the users own individual assessment.

Based on this assessment, our conclusion is that the data subjects' interests, rights and freedoms outweigh Shinigami Eyes' interest in providing their marking-application. Shinigami Eyes' processing of personal data does not meet the third condition in Article 6(1)(f) GDPR

Our conclusion is therefore that Shinigami Eyes is processing personal data through their application without a legal basis, which is a violation of Article 6(1) GDPR.

4.6. Information to the data subject

The data subjects' right to information and corresponding information duty for the controller is regulated in Article 14(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 is not obtained from the data subject itself.

The required information includes, but is not limited to, 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 whether there are any transfer of personal data to a third country.

Datatilsynet cannot see that adequate information has been provided to the data subjects. Therefore, we conclude that Shinigami Eyes has failed to provide the information required by Article 14 GDPR.

4.7. Facilitate for data subjects' rights

In accordance with Article 12(2) GDPR, the controller must facilitate the exercise of data subject rights under Article 15 to 22 GDPR.

Datatilsynets inquiries shows us that Shinigami Eyes has not implemented a system or an approach that adequately allows the data subjects to utilise their rights pursuant to Article 15 to 22 of the GDPR.

Shinigami Eyes is therefore in breach of Article 12(2) GDPR.

5. Corrective measures

We have concluded that Shinigami Eyes, through their application, is processing personal data in breach of Articles 6(1), 12(2) and 14 GDPR.

As stipulated above, Datatilsynet has the competence and power to impose a definitive limitation, including a ban, on the processing activity, see Article 58(2)(f) GDPR.

Pursuant to Article 58(2)(f) GDPR, Datatilsynet hereby imposes a ban on all Shinigami Eyes' processing activities that occur in the context of providing the browser extension "Shinigami Eyes", on Norwegian territory.

6. Information on the right to appeal

You may lodge an appeal against Datatilsynet's decision. An appeal must be lodged within three weeks after having received this letter, cf. the Norwegian Public Administration Act Section 28 and 29. If you need the deadline for an appeal extended, you must contact us before the deadline expires.

If we uphold our decision, we will send the appeal case to Personvernnemda, The Norwegian Privacy Appeals Board, cf. the Norwegian Personal Data Act Section 22. In the event, we will ask you for a translation of the appeal in Norwegian.

Datatilsynet can be contacted at postkasse@datatilsynet.no, or at the postal address above.

7. 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 Datatilsynet is subject to freedom of information requests under the Norwegian Freedom of Information Act.

Kind regards

Jørgen Skorstad
Director, law

This letter has electronic approval and is therefore not signed