Datatilsynet

Your reference	Our reference	Date
	21/01315-7	19.08.2022

Rejection of Complaint - Wordfeud.aasmul.net

1. Introduction

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

Between 25 September 2020 and 23 April 2021, Datatilsynet received several complaints regarding the website wordfeud.aasmul.net (hereinafter the "Website"), which led us to open three parallel inquiries (Cases No. 20/03786, 21/01315 and 21/01611).

All complaints came from purported users of the Website who had been allegedly banned from the Website for failing to provide a valid proof of identity, after having received an identity check request from a moderator of the Website.

While the complaints came from three different email addresses and were signed with different names, during the investigation Datatilsynet become wary of the fact that all complaints might actually come from a single individual. Thus, Datatilsynet asked all of the purported complainants to confirm whether they wished to maintain their complaint, and if so, to provide a postal address and telephone number that Datatilsynet could use to communicate with them, in line with our standard practice.[2] Only one complainant responded to Datatilsynet confirming that they wished to maintain their complaint. However, the complainant at hand failed to comply with Datatilsynet's request regarding the contact details, as they provided us with a false postal address and a telephone number that is not in use, as outlined below.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.
[2] See: https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/

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			

In light of the above deceitful behaviour and the need to be able to confirm the identity of the complainants to handle the matter submitted to Datatilsynet, we have decided to refuse to act on the complaints at hand.

2. Decision

Datatilsynet adopts the following decision:

- The complaint in Case No. 21/01315 shall be rejected pursuant to Article 57(4) GDPR due to its abusive and excessive character.

- Cases No. 20/03786 and 21/01611 are hereby closed, as the purported complainants in these cases failed to respond to Datatilsynet's request to provide their contact details and confirm that they wished to maintain their complaint.

An advance notification of the present decision to the complainants has been omitted pursuant to Article 16(3)(b) and (c) of the Norwegian Public Administration Act.[3]

3. Factual Background

Between 25 September 2020 and 23 April 2021, Datatilsynet received three separate complaints regarding the website wordfeud.aasmul.net (hereinafter the "Website") purportedly from three different individuals who claimed that they had been banned from that Website because they failed to provide a valid proof of identity.[4] The individuals in question claimed that such an identity verification was in violation of the GDPR, and one of these individuals also claimed that the Website's administrator failed to comply with an access and erasure request that they submitted pursuant to Articles 15 and 17 GDPR.[5]

The Website appears to be owned and run on a not-for-profit basis by Mr. Eskil Åsmul through a sole proprietorship: AASMUL.NET ESKIL ÅSMUL (hereinafter "AASMUL"). The Website organizes tournaments of Wordfeud and other digital board games. These tournaments are organized in different languages, including Danish, English, Finnish, French, German, Norwegian, Spanish and Swedish. Participation in the tournaments is free of charge, but participants may gain access to "extra statistics and training material" if they make a donation to the Website of at least 90 NOK, $15, €12 or £10.[6]

To participate in the tournaments organized by the Website, an individual user must: (1) create a user name; (2) provide an email address; and (3) select the language in which they want to play.[7] However, a player may voluntarily choose to provide additional information, including

[3] Act of 10 February 1967 relating to procedure in cases concerning the public administration ("Forvaltningsloven").
[4] See emails to Datatilsynet dated 25 September 2020, 19 March 2021, and 23 April 2021.
[5] See email to Datatilsynet dated 19 March 2021.
[6] See <https://wordfeud.aasmul.net/About.aspx>.
[7] See < https://wordfeud.aasmul net/Users.aspx>.

home country, date of birth, real life name, profile picture, and link to a personal website.[8] However, players may use a pseudonym to participate in the tournaments organized by the Website, and the email address and the other information they provide are as a rule not verified by the website.[9]

The Website makes use of a number of volunteers who act as moderators and are responsible for making sure that the tournaments on the Website run smoothly and that players comply with the relevant rules of the game they play.[10] In some cases, moderators may decide to expel a player who violate such rules.[11]

On 21 June 2021, Datatilsynet sent a letter to Mr. Åsmul asking him to provide his views on the issues raised by the complainants, and we received his response on 20 July 2021.[12]

In his letter to Datatilsynet, Mr. Åsmul explained that the Website does not carry out systematic identity checks on players. However, one of the Website's moderators suspected that a player who had been banned from the Website in the past due to misbehavior (e.g., cheating to improve their scores) was trying to regain access to the website under different fake identities. Thus, on an ad hoc basis, he asked some players who behaved suspiciously to prove their identity, in an attempt to prevent that the banned player would regain access to the Website.

This happened for instance with a player who claimed to be an American Professor named [redacted] (i.e., the same name of the complainant in Case No. 21/01315) who was playing exceptionally well on the version in French of Word feud, which was the version of the game that the above-mentioned banned player normally used. The player who claimed to be named [redacted] was asked to prove their identity by the moderator of the Website, and in response they provided a copy of an old library card, which the moderator considered to be an insufficient proof of identity, as it could have been easily forged. As the player refused to provide any other proof of identity, they were excluded from the game.

Mr. Åsmul further explained that, after the exclusion of the player in question, Mr. Åsmul received an access and erasure request from someone who claimed to be [redacted], but he did not comply with such a request as he had doubts concerning the identity of the person making the request.

In his response to Datatilsynet, Mr. Åsmul also cast doubts as to whether the complainant who claims to be [redacted] and the other two complainants in Cases 20/03786 and 21/01611 are in fact the same person.

In light of the above, and given that all complaints had been submitted to Datatilsynet via email (without providing any additional contact details), on 12 April 2022, Datatilsynet wrote to all three purported complainants the following message:

[8] Ibid.
[9] See AASMUL's letter to Datatilsynet of 20 July 2021.
[10] See < https://wordfeud.aasmul net/About.aspx>.
[11] See AASMUL's letter to Datatilsynet of 20 July 2021.
[12] Ibid.

> "[…] If you still wish that we handle your complaint, please respond to the present email and provide us with your full name, postal address and a phone number where we can reach you.
>
> Please note that if you will not respond to this email and provide the above information by 26 April 2022, we will deem that you no longer wish that we handle your complaint and we will therefore close your case."[13]

On 12 April 2022, the complainant who claims to be named [redacted] replied that they wished that their complaint be handled by Datatilsynet adding: "You can reach me via e-mail at [redacted]".[14]

Given the circumstances, on 12 April 2022, Datatilsynet replied that to handle the case we needed a postal address and a telephone number within the said deadline. Otherwise, Datatilsynet would record the information provided as a tip, which may be used for future investigative purposes.[15]

On 17 April 2022, the complainant responded as follows:

> "[…] Name:
>
> Dr. [redacted]
>
> Postal Address:
>
> [redacted]
>
> Phone Number:
>
> [redacted]
>
> E-mail Address:
>
> [redacted]
>
> Please keep correspondence to e-mail. I do not wish to be contacted via post or phone."

The other purported complainants did not respond to Datatilsynet within the above-mentioned deadline.

[13] See email to the complainants dated 12 April 2022.
[14] See email to Datatilsynet dated 12 April 2022.
[15] See email to the complainant dated 12 April 2022.

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

> […] *applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

Moreover, Article 3(1) GDPR provides that the Regulation:

> […] *applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

> "*personal data" means 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Pursuant to Article 4(2) GDPR:

> *"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, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

Pursuant to Article 4(7) GDPR:

> *"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

4.3. Rights of the Data Subject

Article 15 GDPR reads:

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

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

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

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

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) 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.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Pursuant to Article 17 GDPR:

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the

right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) *for the establishment, exercise or defence of legal claims.*

Furthermore, Article 12(2) and (6) GDPR provides that:

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

[…]

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

In addition, Article 77 GDPR reads:

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

4.4. Competence and Tasks of Supervisory Authorities under the GDPR

Pursuant to 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.

Further, Article 56(1) reads as follows:

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 term "cross-border processing" is defined in Article 4(23) as follows:

> *"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.*

Pursuant to Article 57(1)(f) GDPR:

> *Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:*
>
> […]
>
> *(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.*

Further, Article 57(4) GDPR provides:

> *Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.*

4.5. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area ("EEA") Agreement by means of Decision of the EEA Joint Committee No 154/2018 ("EEA Joint Committee Decision").[16]

Article 1(b) of the EEA Joint Committee Decision provides that:

[16] 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 OJ [2018] L 183/23.

[…] *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.*

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.[17] The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet's Competence

The Website is run by Mr. Eskil Åsmul through a sole proprietorship in Norway, which constitutes the single establishment of the controller. However, the games on the Website are targeted at players in different EU/EEA countries, as the tournaments are organized in different languages, including Danish, English, Finnish, French, German, Norwegian, Spanish and Swedish. Thus, the processing of players' personal data takes place in the context of the activities of a single establishment in the EU/EEA, but it is likely to substantially affect data subjects in several EU/EEA countries. Therefore, it qualifies as cross-border processing under Article 4(23)(b) GDPR.

In light of the above, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that the single establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. Therefore, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections within a period of four weeks after having been consulted in accordance with Article 60(3) GDPR.

6. Datatilsynet's Assessment

Datatilsynet's view is that the demeanour assumed by the complainant in Case No. 21/01315 qualifies as an "abuse of rights", which entails that their request is manifestly excessive. Consequently, the complaint should be rejected as "manifestly excessive" pursuant to Article 57(4) GDPR.

The prohibition of abuse of rights is a general principle of EU and EEA law.[18] A determination of abuse of rights under EU/EEA law is based on a cumulative test combining objective and subjective elements. The objective element requires that it be evident from the specific set of circumstances in question that, despite formal observance of the conditions laid down by the EU/EEA rules, the purpose of those rules has not been achieved. The subjective element

[17] Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").
[18] CJEU, Case C-321/05, *Kofoed v Skatteministeriet*, para. 38; EFTA Court, Case E-1/20*, Kerim v The Norwegian Government*, para. 36.

requires an abusive intention to obtain an advantage from the EU/EEA rules by artificially creating the conditions laid down for obtaining it.[19]

The prohibition applies also with respect to the rights laid down in the GDPR, including the right to lodge a complaint set out in Article 77 GDPR, as other supervisory authorities have previously noted.[20] Therefore, the scope of the right set out in Article 77 GDPR cannot be extended to cover abusive practices that are conducted for the purpose of deceitfully obtaining advantages that ordinarily could have resulted from a lawful use of such a right (e.g., obtaining that a supervisory authority orders the controller to stop a certain processing operation, such as identity verification).

Whilst identification of the complainant is not invariably a condition for the exercise of the right laid down in Article 77 GDPR, the effective exercise of the powers that supervisory authorities enjoy under the GDPR may require that the competent authority be able to confirm the identity the complainant, in particular in cases that concern alleged infringements of data subject rights.

Of relevance in this regard is the following statement by the EFTA Court in Joined Cases E-11/19 and E-12/19, *Adpublisher*:

> "the effective functioning of data protection compliance under the GDPR may require disclosing the complainant's personal data to the data controller. This would be the case, inter alia, when the data subject, in accordance with point (c) of Article 58(2) of the GDPR, requests to exercise his or her rights or alleges infringement of his or her rights by the controller. Acting on this request, *a supervisory authority may need to disclose the identity of a complainant to the controller* to enable the latter to fulfil the order. In turn, *the supervisory authority's exercise of its powers*, in accordance with, inter alia, points (e) to (g) and (j) of Article 58(2) of the GDPR, *may necessitate disclosing the identity of the complainants to the controller*."[21] (emphasis added)

Furthermore, Article 12(2) and (6) GDPR – which a supervisory authority must take into account when assessing whether a controller has legitimately refused to act upon a data subject's request – provides that:

> "[…] the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, *unless the controller demonstrates that it is not in a position to identify the data subject*.
>
> […]

[19] EFTA Court, Case E-1/20, *Kerim v The Norwegian Government*, para. 37; CJEU, Case C-202/13, *The Queen, on the application of Sean Ambrose McCarthy and Others v Secretary of State for the Home Department*, para. 54.
[20] See Spanish Supervisory Authority (AEPD), Procedimiento Nº: E/00739/2021.
[21] EFTA Court, Joined Cases E-11/19 and E-12/19, *Adpublisher*, para. 51.

> Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller *may request the provision of additional information necessary to confirm the identity of the data subject*." (emphasis added)[22]

Moreover, if a supervisory authority has reasonable doubts concerning the complainant's identity, but nonetheless issues orders related to such an identity without eliminating these doubts, it may run the risk of applying the law incorrectly or causing harm to other data subjects should the identity at hand prove to be false.

Thus, in some cases, such as the present one, supervisory authorities need to be able to confirm the identity of the complainant.

This is reflected in the guidance on "How to Complain to the Norwegian Data Protection Authority" available on Datatilsynet's website, which indicates that a complaint should include, among other things, "contact information (name, phone and postal address only)".[23] Providing contact information is not an invariable condition for lodging a complaint with Datatilsynet. Additionally, Datatilsynet accepts anonymous tips, although these are generally taken into account only for planning possible future investigative activities.[24] However, as set out above, in some cases we need to be able to confirm the identity of the complainant to handle the relevant complaint with all due diligence.

In Case No. 21/01315, the complainant claims, among other things, that the controller failed to act on their request for exercising their rights under Articles 15 and 17 GDPR. At the same time, in the context of our investigation, Mr. Åsmul raised concerns that the purported complainant is engaging in fraudulent behaviour, operating under a false identity (or identities) to try to be readmitted to the Website following their exclusion, and that they may be trying to manipulate Datatilsynet accordingly in their quest.

Further, Mr. Åsmul's specific doubts with regard to the identity of the complainants, as well as a closer scrutiny of the different complaints, made Datatilsynet wary of the fact that all such complaints might have been submitted by a single individual under multiple pretended identities. In this respect, it should be noted that the complaints present very similar features and linguistic patterns. For example, they all came from Gmail accounts; they all used the term "GDPR violations" in the subject line; they all complained about a Norwegian company called "Wordfeud League of Honour", which does not exist; they all used the term "raise a complaint", which is rather unusual and not in line with standard data protection terminology;[25] they all used the term "data privacy policy", which is not a standard term under the GDPR; and none of the complaints provided any contact details other than an email address, despite the fact that on Datatilsynet's website it is clearly indicated (also in English) that a complaint should include "name, phone and postal address".

---

[22] See further Recital 64 GDPR, which states: "The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services […]."
[23] See: https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/
[24] See: https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/tips-oss/
[25] The common terminology is "submit" or "lodge" a complaint.

Under this specific set of circumstances, Datatilsynet deemed it necessary to confirm the identity of the complainants to handle their complaints, also in light of its duty to handle complaints with all due diligence.[26] Hence, on 12 April 2022, it sent the following message to all of the purported complainants:

> "[…] If you still wish that we handle your complaint, please respond to the present email and provide us with your full name, postal address and a phone number where we can reach you.
>
> Please note that if you will not respond to this email and provide the above information by 26 April 2022, we will deem that you no longer wish that we handle your complaint and we will therefore close your case […]."[27]

Only the complainant in Case No. 21/01315 replied to the above massage within the said deadline. However, they first insisted to be contacted via email and did not provide any other contact information.[28] Only upon our further insistence, they provided us with the following contact information on 21 April 2022:

> "Name:
>
> [redacted]
>
> Postal Address:
>
> [redacted]
>
> Phone Number:
>
> [redacted]
>
> E-mail Address:
>
> [redacted]
>
> Please keep correspondence to e-mail. I do not wish to be contacted via post or phone."[29]

[26] CJEU, Case C-311/18, *Facebook Ireland and Schrems*, para. 109.
[27] See emails to the complainants dated 12 April 2022.
[28] See email from the complainant dated 12 April 2022.
[29] See email from the complainant dated 21 April 2022.

Upon receiving such information, Datatilsynet realized that the address provided by the complainant corresponded to the address of an UPS store in West York (USA),[30] which offers mailbox services.[31] Datatilsynet contacted the store in question to confirm whether a person named [redacted]" rented a mailbox at that store, possibly mailbox "#341". The store manager responded that no one named "[redacted]" rented a mailbox at their store, and there was no mailbox with a number as high as 341 at the store. Thereafter, Datatilsynet tried to call the phone number provided by the complainant, which turned out to be not in use. Therefore, it became apparent that Datatilsynet had been provided with false information, presumably to lure us into taking action against AASMUL, which would facilitate the complainant's readmission to the Website.

In light of the above, in our view, the complainant in Case No. 21/01315 committed an abuse of the right set out in Article 77 GDPR. This is because they acted in bad faith by providing Datatilsynet with false personal information, and tried to deceitfully obtaining advantages that could have ordinarily resulted from a lawful use of such a right. Moreover, the fact that none of the other complainants replied to Datatilsynet and the identified similarities among the various complaints received by Datatilsynet suggest that the same person attempted to lure Datatilsynet into believing that several different individuals experienced similar data protection issues with the Website. Further, the person in question appears to have done all this not so much to uphold their data protection rights, but to seek Datatilsynet's support in bypassing their exclusion from the Website, which is not the purpose of the complaint mechanism set out in the GDPR. Thus, the complainant's behaviour qualifies as an "abuse of rights" under EU/EEA law.

The abusive character of the request of the complainant is indirectly confirmed by the fact that several recitals of the GDPR make clear that identity frauds and other forms of frauds should be limited and prevented.[32]

An abusive request is "manifestly excessive" for the purposes of Article 57(4) GDPR, as it goes manifestly beyond the purposes for which the complaint mechanism set out in the GDPR was envisaged.[33] This is further confirmed by the EFTA Court's finding in *Campbell* that the scope of EEA law—which includes the GDPR and its complaint mechanism—cannot be extended to cover abuses.[34] In this respect, it should be noted that the words "in particular" in Article 57(4) indicate that a request may be considered "excessive" not only when it is "repetitive".

Thus, Datatilsynet has decided to refuse to act on the complaint in Case No. 21/01315 in accordance with Article 57(4) GDPR. Datatilsynet has also decided to close Cases 20/03786 and 21/01611, as the purported complainants in these cases failed to respond to Datatilsynet's request to provide their contact details (hence making their identification impossible) and confirm that they wished to maintain their complaints.

[30] See: https://locations.theupsstore.com/pa/york/2159-white-st
[31] See: https://locations.theupsstore.com/pa/york/2159-white-st/mailbox-services
[32] See e.g., Rec. 47, 75, 85 and 88.
[33] The purpose of the right to lodge a complaint is to ensure adequate protection of the rights of the data subject. See Rec. 141 GDPR.
[34] EFTA Court, Case E-4/19, *Campbell*, para. 69.

However, this is without prejudice to the possibility of opening future inquiries into AASMUL's compliance with the GDPR, including with respect to sporadic identity checks.

7. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.[35]

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

Recipient(s): [redacted]

Copy to: AASMUL.NET ESKIL ÅSMUL

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