Datatilsynet
P.O. Box 458 Sentrum
NO-0105 Oslo

Per E-Mail: postkasse@datatilsynet.no

Vienna & Oslo, 03.06.2026

noyb Case-No:	**C106**
Complainant:	[redacted]
represented under Article 80(1) GDPR by:	*noyb* – European Center for Digital Rights Goldschlagstraße 172/4/3/2, 1140 Vienna
Respondent:	**Schibsted Media AS ("Schibsted")** Postboks 490 Sentrum NO-0105 OSLO
Regarding:	Article 5(1) GDPR Article 6(1) GDPR Article 7 GDPR

COMPLAINT ACCORDING TO ARTICLE 77(1) GDPR

This complaint is filed by *noyb* in cooperation with Forbrukerrådet (Norwegian Consumer Council).

1. REPRESENTATION

1. *noyb* – European Center for Digital Rights is a not-for-profit organisation active in the field of the protection of data subjects' rights and freedoms with its registered office in Goldschlagstraße 172/4/2, 1140 Vienna, Austria, registry number ZVR: 1354838270 (hereinafter: *„noyb"*) (**Attachment 1**).

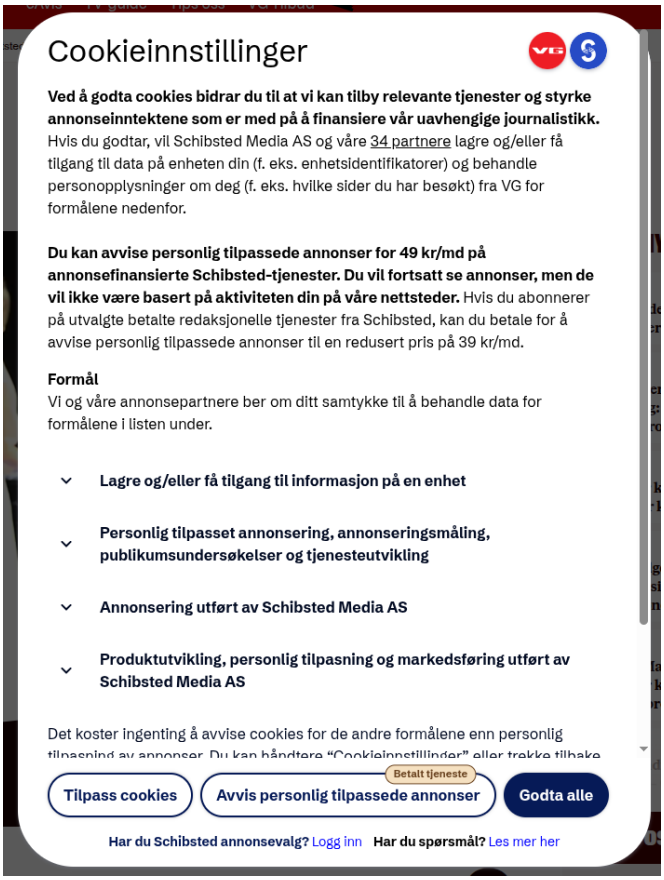
2. *noyb* is representing the complainant under Article 80(1) GDPR (**Attachment 2**).

2. FACTS PERTAINING TO THE CASE

2.1. Website visit

3. On 2nd June 2026 around 11:17 AM the complainant visited the website https://www.vg.no/ to read the news.

4. The complainant was presented with the following banner requesting them to either consent to the processing of their personal data for "personalised advertising" or to pay 49 NOK each month (39 NOK/month if one is a paid subscriber) to avoid the processing of their personal data (**Attachment 3**):



Screenshot of the banner on vg.no on 2nd June 2026 (taken on a different device)

5. The banner required interaction before access to journalistic content was possible.

6. Selecting the "consent" option ("Godta alle") required one single click. The alternative option required

   - clicking on the button "reject personalised advertising" ("Avvis personlig tilpassede annonser"),
   - selecting if the complainant had a subscription or had no subscription,
   - logging into a Schibsted account typing in their email address and then their password,[1]
   - choosing the Vipps payment option,[2]
   - typing in their phone number, including selecting the correct country code,[3]
   - authorizing the payment through the Vipps app.

7. The complainant selected the "consent" option option ("Godta alle"). The complainant documented their website interaction in a HAR-file (**Attachment 4**) and created a corresponding video (**Attachment 5**).

2.2. Situation of the complainant

8. The complainant is a regular reader of the visited website. They are willing to pay for journalistic work directly and they are a paid subscriber to https://www.vg.no. The complainant is not willing to pay for their right to data protection.

9. In addition, Forbrukerrådet (the Norwegian Consumer Council) has received several complaints by users worried about their data and privacy due to Schibsted's new model. Between 28th April 2026 when Aftenposten's subscribers were contacted about the new model to be implemented and 2nd of June 2026, 64 consumers contacted Forbrukerrådet with questions and comments regarding Schibsted's "pay or ok" system. Many of the consumers contacting Forbrukerrådet, find the solution invasive, unfair and question the legality of it. Some use the term 'blackmail', and some express that they hope that somebody, such as Forbrukerrådet, will do something to stop it.

2.3. The role of Schibsted

10. Schibsted runs the website https://www.vg.no/, as well as several others in Norway and beyond. Schibsted is one of Norway's biggest commercial news publishers and reaches 80 %

[1]Had the complainant not had a previous Schibsted account they would have had to create a Schibsted account with an email address and a password and additionally confirming her email address through a link sent via email. Only then would they have been in a position to log in.

[2]Other payment options were not available, excluding anyone who does not or cannot use Vipps.

[3]If the user is not registered with Vipps, the user would have to register which would require the identification of said person and includes additional effort.

of the Norwegian and Swedish population every week.[4] VG is Norway's most read media outlet, having a daily coverage of almost 1,9 million[5] and over 3,2 million users every week.[6]

11. Schibsted had previously introduced similar banners as the one present in the case at hand for its Swedish websites. It announced its intention to roll out such a "pay or okay" system in Norway, too.[7] In an interview with Swedish SVT a Schibsted representative explained that the new banners are introduced to avoid that people refuse consent:

    "*Studier visar att om du gör detta utan någon typ av betalning kopplat till det kommer väldigt många användare att tacka nej."*[8]

    In English: *"Studies show that if you do this without offering any kind of payment linked to it, a large number of users will decline."* (automated translation) (emphasis added)

12. The representative highlighted in the associated video:

    "*Varan man köper då, det är att att vi ehh du är befriad från att vi samlar in datan."*[9]

    In English: "*So what you're buying here is that that we—uh—you're exempt from us collecting that data.*" (automated translation)

3. ABOUT "PAY OR OKAY"

13. "Pay or okay" (also called "consent or pay") describes consent requests, where refusing consent costs money and usually requires you to sign up to a subscription. "Consenting", however, is free of charge.

14. Such system was first introduced by the Austrian newspaper "Der Standard" in 2018 and spread quickly to Germany (e.g. Die Zeit, Der Spiegel) and later also Italy (e.g. Il Corriere), Spain (e.g. El País), France (e.g. Le Monde) and others. Meta switched to "pay or okay" for Facebook and Instagram in 2023.

15. While the European Data Protection Board was quick to consider its use by big online platforms very likely illegal,[10] the European Supervisory Authorities cannot agree on more general guidelines since 2024. It seems some authorities want to greenlight "pay or okay" due to heavy media pressure or political ideals, while others insist that this is legally not feasible.

16. "Pay or okay" is popular among publishers because it nudges users to "consent" in 99.9 % of all cases (see below 4.3.1.1). Publishers seek such "consent" to process personal data for advertising purposes and to obtain additional revenue.

---

[4]Ole J. Mjøs, Schibsted, The Digital Transformation of a Nordic Media Giant, p. 1, available here: https://api.pageplace.de/preview/DT0400.9781040383476_A62556202/preview-9781040383476_A62556202.pdf

[5]https://www.medietall.no/index.php?liste=persontall&r=PERSONTALL&pid=53545&p=2512&gs=1

[6]https://advertising.schibsted.com/no/brands/vg/

[7]https://schibsted.com/2026/02/03/schibsted-introduces-a-new-solution-to-safeguard-the-funding-of-journalism/

[8]https://www.svt.se/kultur/aftonbladets-lasare-maste-betala-for-att-slippa-datainsamling

[9]https://www.svt.se/kultur/aftonbladets-lasare-maste-betala-for-att-slippa-datainsamling

[10]EDPB, Opinion 08/2024.

17. Different from how it is depicted by media companies on a regular basis, such additional revenue is rather small.[11] It is unlikely that such small additional revenue would change the financial viability of a media company. However, it furthers dependence on Google, Meta and generally the online advertising industry.

18. If the "pay or okay" approach of the respondent was considered lawful or was tolerated, it would be logical that other websites, apps and platforms in Norway adopt a similar approach to obtain almost 100 % consent, too. This can already be seen in Germany and Austria were hundreds of websites (e.g. recipe websites, dictionaries, online forums, etc.) use "pay or okay".[12] Refusing consent on the top 100 German websites amounted to a yearly cost of more than 1,500 € (~ 16,132 NOK) per person in 2024.[13]

19. It is therefore clear that without clear opposition, the fundamental right to data protection would become a luxury.

4. GROUNDS FOR THE COMPLAINT

4.1. Violations

20. The respondent violated the following provisions:

    (a) **Article 6(1) GDPR**: The respondent lacks a legal basis for processing the personal data of the complainant.

    (b) **Article 5(1)(a) GDPR**: Due to the lack of a legal basis, the processing of personal data at hand is unlawful.

    (c) **Article 7(4) GDPR**: The respondent tries to bundle consent with a service, where this is objectively not necessary.

    (d) **Article 7(3) GDPR**: Withdrawing consent is not as easy as giving it.

21. In essence, in the case at hand (i) the protection of personal data is only available upon a payment contrary to the provision in Article 6(1) GDPR, (ii) the respondent lacks a legal basis in accordance with Article 6(1) GDPR for processing personal data of the complainant and in particular does not obtain valid consent, (iii) withdrawing consent is not as easy as giving it and (iv) the protection of personal data is considered a commodity contrary to it being a fundamental right available to everyone.

[11] https://noyb.eu/en/noybs-pay-or-okay-report-how-companies-make-you-pay-privacy

[12] https://www.contentpass.net/en/publications holds a list of websites using their "pay or okay" solution.

[13] https://noyb.eu/en/pay-or-okay-1500-eu-year-your-online-privacy

4.2. Data Protection only upon payment

4.2.1. Data processing requires a legal basis

22. Article 6(1) GDPR provides for a general prohibition on the processing of personal data, subject to certain exceptions. Accordingly, for the lawful processing of personal data, one of the legal bases set out in Article 6(1) of the GDPR must apply.

23. For this reason, the respondent tries to obtain consent through its "pay or okay" banner.

4.2.2. Burden of proof

24. It is for the respondent to demonstrate that its data processing is lawful, fair and transparent (Article 5(1)(a) and 5(2) GDPR). The respondent shall also be able to demonstrate that the complainant has consented to processing of their personal data (Article 7(1) GDPR).

25. The competent authority may thus require the respondent to demonstrate how the processing at hand is lawful.

4.2.3. Reversal of the initial protection granted by the GDPR

26. The general protection granted by the prohibition of processing of personal data (Article 6(1) GDPR) is reversed by requiring a fee for refusing consent. In the situation at hand only those who pay enjoy protection of their personal data.

27. However, the legislator did not foresee a "data protection fee" for refusing consent in the GDPR. In other exceptional cases, the GDPR allows for payments in relation to data protection (Articles 12(5)(a), 15(3), 57(4) GDPR). If the legislator intended to do so for refusing consent, too, it had included a corresponding provision in the GDPR.

28. Thus, granting protection of personal data only upon a payment is contrary to Article 6(1) GDPR. It turns data protection into a luxury for the few.[14]

4.3. No legal basis: The controller does not obtain freely given consent

4.3.1. No freely given consent

29. Article 4(11) GDPR defines "consent"

> "[…] *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;*" (emphasis added)

30. Recital 42 GDPR, last sentence, states in that regard:

[14]That personal data is not a tradable commodity, is the long-standing opinion of the European Data Protection Board (EDPB) (EDPB Guidelines 2/2019, para. 54; EDPB Opinion 08/2024, para. 130; EDPB Binding Decision 3/2022, para. 101).

"*Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*" (emphasis added)

31. The EDPB considers in that regard:

"*The element 'free' implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid.* [...] *Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment."*[15] (emphasis added)

32. Thus, consent is only valid if it is "freely given". Thereby the European legislature aims to ensure that a renunciation of the fundamental right to data protection occurs only if this corresponds to the actual subjective will of the data subject. In this respect, the GDPR serves a protective function by safeguarding the free will of data subjects and, thereby, their informational self-determination.

33. The question of whether an indication of wishes is "freely given" is a psychological matter concerning the individual's inner will in a specific situation and, as such, a question of fact. From a legal perspective, it must therefore be determined whether the decision was "free" or whether certain factors manipulated or undermined the indication of wishes.

34. In this sense, the "pay or okay" model relies on deliberately making the process of refusing to give consent cumbersome, complicated, and unattractive in terms of time, effort and cost, in order to persuade as many consumers as possible to give their "consent".

4.3.1.1. Unrealistic consent rates of more than 99 %

35. Such a model influences data subjects directly in their choices, as shown by empirical evidence.

36. Providers of "pay or okay" systems promote these systems by claiming that they achieve consent rates of 99.9%.[16] An academic analysis of real-world data of a German publisher showed a consent rate of more than 99%.[17] Numbers circulated by the German lobby organization BVDW also show that less than 1% of users opted for a subscription ("pay") on several news sites running "pay or okay" (**Attachment 6**).[18]

37. A consent rate of such magnitude is itself already an indicator of "unfree" consent where users do not have a genuine choice. It defies common sense that users of various platforms and websites – who come from diverse backgrounds in terms of origin, age, worldview, education, ethnicity, etc., and accordingly reflect a broad spectrum of views on data protection and the

---

[15] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, V. 1.1, para. 13.

[16] Morel et al., Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls, p. 155, https://dl.acm.org/doi/pdf/10.1145/3603216.3624966

[17] T. Müller-Tribbensee, K. Miller, B. Skiera, Paying for Privacy: Pay-or-Tracking Walls, p. 35, https://arxiv.org/pdf/2403.03610;

[18] https://iabeurope.eu/wp-content/uploads/PUR-Modelle-bvdw_20231004-en.pdf

commercialization of personal data –, would reach such a homogeneous consensus on the question of consent.

38. In stark contrast to the previous numbers, neutral studies suggest only about 3% of users are willing to accept marketing cookies.[19] Other surveys show that at most 10% of users are fine with their data being collected for advertisement.[20] Only 4,7% of users feel "okay" with third-party tracking.[21]

39. This creates a huge discrepancy with users' actual intentions. The "pay or okay" system structurally undermines these intentions, and over 90% of those affected are pressured into giving "consent" that does not reflect their true free will. Public comments by Schibsted representatives show this was acknowledged and taken into account by Schibsted (see above 11).

40. Hence, from an empirical perspective, the complainant did not consent freely.

4.3.1.2. High effort to refuse consent

41. Furthermore, refusing to give consent requires far more effort than giving it. Instead of one simple click on a button, users must (i) click on the button "reject personalised advertising" ("Avvis personlig tilpassede annonser"), (ii) select if they have a subscription or have no subscription, (iii) create a Schibsted account with an email address and a password and additionally confirm the email address through a link sent via email (if they have no account), (iv) log into their Schibsted account typing in their email address and then their password, (v) choose the Vipps payment option (no other payment option is available), (vi) type in their phone number, including selecting the correct country code, (vii) register with Vipps if they are not yet registered and (viii) authorize the payment through the Vipps app. While this usually takes several minutes, consent can be given in a fraction of a second.

42. The EDPB has already determined with regard to standard cookie banners that it is not permissible to require users to navigate through additional layers in order to reach a "reject" button (to refuse consent).[22,23] After all, according to the CJEU, the very effort required to uncheck a pre-checked box already prevents valid consent.[24]

---

[19]Utz et al., (Un)informed Consent: Studying GDPR Consent Notices in the Field, p. 10, https://arxiv.org/pdf/1909.02638#page=10

[20]Gallup Institut, Facebook and Advertising – User-Insights, p. 7, https://noyb.eu/sites/default/files/2020-05/Gallup_Facebook_EN.pdf

[21]Coopamootoo et al., "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country, p. 6, table 2, https://arxiv.org/pdf/2202.04682

[22]This is the view of the vast majority of all data protection authorities in the "Report on the work undertaken by the Cookie Banner Taskforce" of the EDPB, January 2023, para. 8, https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf;

[23]See e.g. the Judgment of the Austrian Federal Administrative Court of 31 July 2024, W108 2284491-1, para. 3.3.2.4., according to which a "reject" option located on the second layer of a banner results in invalid consent, https://www.ris.bka.gv.at/JudikaturEntscheidung.wxe?Abfrage=Bvwg&Dokumentnummer=BVWGT_20240731_W108_2284491_1_00; Summary in English available here: https://gdprhub.eu/index.php?title=BVwG_-_W_108_2284491-1;

[24]CJEU, Judgment of 1 October 2019, C-673/17, Planet49, paras. 62–63.

43. There is no reasonable justification for applying a different standard to (significantly more cumbersome) payment processes.

44. In addition, recital 80 of Regulation (EU) 2024/900 on the transparency and targeting of political advertising states the following regarding consent under the GDPR:

> "*Refusing to give consent or withdrawing consent should not be more difficult or time-consuming to the data subject than giving consent.*" (emphasis added)

45. Therefore, additional time required for the rejection is not compatible with the authentic interpretation by the European legislator.

46. The CJEU had already expressed itself similarly:

> "*Furthermore* [...] *the free nature of that consent appears to be called into question by the fact that, if that consent is refused, Orange România* [...] *required the customer concerned to declare in writing that he or she did not consent to a copy of his or her identity document being collected or stored.* [...] *such an additional requirement is liable to affect unduly the freedom to choose to object to that collection and storage* [...]."[25]

47. This undue additional burden for rejecting the consent request exists regardless of the fee charged. Even if the fee charged by the respondent were a fraction of a Norwegian krone, this would not alter the additional mental and time-related effort that leads users to choose the simpler consent option.

48. Therefore, the additional effort required from the complainant to refuse consent precludes freely given consent.

4.3.1.3. Unlawful bundling of consent

49. Article 7(4) GDPR states:

> *"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."*

50. The respondent offers in essence two options for the provision of its services:

- Option A: Access to its website without data processing for personalized advertising against a fee.

- Option B: Access to its website only insofar as consent for data processing for personalized advertising[26] was given.

[25]CJEU, Judgment of 11 November 2020, C-61/19, Orange România, para. 50.

[26]Which entails invasive user tracking. See e.g. https://www.forbrukerradet.no/out-of-control/ and the corresponding report "Out of Control", as well as https://netzpolitik.org/2025/databroker-files-all-you-need-to-know-about-how-adtech-data-exposes-the-eu-to-espionage/.

51. There is, in principle, nothing to object to the defendant offering access to its website only for a fee (Option A).

52. However, Article 7(4) of the GDPR prohibits an offer such as the one for Option B, since the provision of its website is made contingent upon consent to data processing for personalized advertising, even though such data processing is not necessary to provide the website. This is particularly evident because in the past no such "consent requirement" existed.

53. This therefore constitutes precisely the kind of "bundled" consent that Article 7(4) GDPR prohibits. Due to this clear violation of Article 7(4) GDPR consent was not freely given.

4.3.1.4. Price is highly excessive and not "appropriate"

54. The respondent requested a payment of 39 NOK from the complainant for refusing consent, given that they were a previous subscriber.

55. A paid alternative does not constitute an equivalent option to consent, as the refusal option comes with a (financial) detriment. In such cases, it can no longer be assumed that there is a genuine or free choice within the meaning of recital 42 GDPR.

56. However, even if paid alternatives for refusing consent were considered acceptable in principle – which is not the position of the complainant –, it is clear that the price of the subscription of the respondent is massively inflated.

57. Research has shown that the average advertising revenue (for any advertisement, including tracking-based advertising) for a bigger news publisher is about € 0,24 a month per user.[27] The subscription of the respondent is substantially higher: 39 NOK (~3,6 €) or 49 NOK (~ 4,5 €) per month.

58. In addition, the same research estimates that without targeted advertisement news publishers would earn € 0,20 a month per user.[28] That means publishers earn only about 4 cents (~ 0,43 NOK) per month and user with tracking-based advertising (which is the type of advertising that the respondent asks consent for).

59. Similar results can be drawn from the ad spend numbers by the industry. The IAB AdEx report for 2023[29] shows an average programmatic ad spend of € 41,3 per Norwegian user and year (~ € 3,44 per user and month).[30,31]

---

[27] T. Müller-Tribbensee, K. Miller, B. Skiera, Paying for Privacy: Pay-or-Tracking Walls, p. 23, https://arxiv.org/pdf/2403.03610;

[28] T. Müller-Tribbensee, K. Miller, B. Skiera, Paying for Privacy: Pay-or-Tracking Walls, p. 38, https://arxiv.org/pdf/2403.03610;

[29] https://iabeurope.eu/wp-content/uploads/2023/07/IAB-Europe_AdEx-Benchmark-2022_REPORT.pdf#page=42

[30] Internet use per country: https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_ifp_iu/default/table?lang=en&category=isoc.isoc_i.isoc_iiu

[31] € 189.000.000 were spent on programmatic ads in Norway in 2022. At the beginning of 2022 5.425.270 people lived in Norway (https://ec.europa.eu/eurostat/databrowser/view/tps00001/default/table?lang=en&category=t_demo.t_demo_pop). In 2022 99,7 % of the population aged 16 to 89 in Norway used the internet (Eurostat link from previous footnote and https://ec.europa.eu/eurostat/cache/metadata/EN/isoc_i_simsih2_no.htm#shortstat_popDisseminated) that is ~ 4.575.607 people. € 189.000.000 devided by 4.575.607 is € 41,3 per year.

60. This is the total amount of money spent on programmatic ads on all websites combined that an average user in Norway visits in an entire year (or month). A good part of that ad spend does not go to the individual websites, but to ad exchanges, Google and alike.

61. This average number shows, that the subscription fee for refusing consent of https://www.vg.no/ alone (39 NOK (~3,6 €) or 49 NOK (~ 4,5 €)) costs more than the entire programmatic advertisement spend per user in Norway per month (€ 3,44).

62. The price the complainant would pay for refusing consent is thus highly excessive and may even be regarded as usury or unjust enrichment.

63. Therefore, it is clear that the "pay or ok" model implemented by the respondent is not about supplementing allegedly "lost" income,[32] but to open up new revenue streams and to nudge users to consent.

4.3.1.5. Overall costs will likely become unsustainable in the future

64. While "pay or okay" is new for Norwegian controllers, it has been adopted widely in other European countries, among others by online platforms, media companies and common websites, like cooking, gaming, sports and weather forecasts sites. Prominent examples are news outlets such as *Le Monde*, *El País*, *La Repubblica*, *Der Spiegel*. The development in Norway may be similar.

65. Due to the easy accessibility on the internet, data subjects browse through numerous websites on a daily basis and are likely confronted with several "pay or ok" banners.

66. However, rejecting consent on the top 100 websites in different EU countries leads to substantial expenses. Back in 2024 refusing consent would cost data subjects € 1.529,36 in Germany[33], € 1.463,88 in Spain[34], € 1.135,44 in Austria[35], € 1.182,36 in France[36] and € 1.008,98 in Italy[37] per year.

67. These high costs result in a foreseeable erosion of data protection online.

68. Particularly, it affects those with less financial means: More than 21 % of the EU population, that is approximately 93.3 million people, are at risk of poverty or social exclusion.[38] Against this background, one fifth of the EU population simply does not have a real choice when faced with "pay or ok", as they are not in a situation where they would be able to afford such a payment. In Norway 15,7 % of the population are at risk of poverty or social exclusion.[39]

69. This is obviously discriminatory towards anyone enduring financial hardship, rendering data protection a luxury, not a fundamental right.

70. In addition, the widespread use of "pay or okay" models, makes it even less likely that data subjects pay for refusing consent as it requires even more effort and money to do so for several

---

[32] See the public statement of the respondent at https://schibsted.com/2026/02/03/schibsted-introduces-a-new-solution-to-safeguard-the-funding-of-journalism/

[33] https://noyb.eu/sites/default/files/2024-03/Cost%20Top%20100%20Websites%20in%20Germany.pdf

[34] https://noyb.eu/sites/default/files/2024-03/Cost%20Top%20100%20Websites%20in%20Spain.pdf

[35] https://noyb.eu/sites/default/files/2024-03/Cost%20Top%20100%20Websites%20in%20Austria.pdf

[36] https://noyb.eu/sites/default/files/2024-03/Cost%20Top%20100%20Websites%20in%20France.pdf

[37] https://noyb.eu/sites/default/files/2024-03/Cost%20Top%20100%20Websites%20in%20Italy.pdf

[38] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250430-2

[39] https://ec.europa.eu/eurostat/databrowser/view/ilc_peps01n__custom_16248875/bookmark/table?lang=en&bookmarkId=f324bf0e-5b63-446f-b243-94089a70015a&c=1744619026707&page=time:2024

websites. Thus, the widespread use creates an additional nudging factor and may become relevant in Norway, too.

4.3.1.6. Subscription

71. The nudging of data subjects towards the consent option is further accentuated by the fact that the refuse option is offered only as a monthly subscription.

72. Therefore, data subjects have to cancel or manage the subscription in the future. This, in turn, requires additional effort and time (see above on additional effort for refusing consent).

73. Moreover, data subjects run the risk of losing track of automatically renewing subscriptions. This will regularly deter data subjects further from refusing consent.

74. Hence, the refusal option being available only as a subscription undermines the free choice of the complainant.

4.3.1.7. Summary: Highly effective distortion of data subjects' will

75. The extremely high consent rates in "pay or okay" systems as the one of the respondent are a result of at least the outlined nudging factors:

    (i) Refusing consent requires disproportionate time and effort in comparison to consent (with less time-consuming nudging strategies being already prohibited),

    (ii) Unlawfully bundling consent with access to the website,

    (iii) The pricing is excessive on an individual level,

    (iv) The price may altogether become substantial taking into account future widespread use,

    (v) The reject option is only available as a subscription, which requires future interaction by the data subject and further deters them from refusing consent.

4.3.2. No legal basis

76. For the reasons outlined above, the respondent did not obtain valid consent from the complainant. Therefore, the controller lacks a legal basis under Article 6(1) GDPR to process the personal data of the complainant.

77. Thus, the controller is processing personal data unlawfully and is also in violation of Article 5(1)(a) GDPR.

4.3.3. Position of the EU Commission, EDPB and CJEU

78. The EU Commission has held that it considers that the "pay or okay" system implemented by Meta is contrary to the Digital Markets Act.[40] In this context, the Commission refers to

[40] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_1085/IP_25_1085_EN.pdf

Article 5(2) of the Digital Markets Act, which in turn refers to consent under Article 4(11) GDPR — the same provision that the controller relies on under Article 6(1)(a) GDPR.

79. In its Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms the EDPB states (para. 179):

"It has to be concluded that, in most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee."

80. The EDPB Opinion is intended for large online platforms, but acknowledges that all controllers must obtain valid consent (para. 30) and sets out various general grounds against recognizing "pay or okay".

81. In its judgment of 4 July 2023, Case C-252/21, the CJEU made a very vague reference to "pay or okay" in a six-word subordinate clause. In this context, the referring court had merely asked the CJEU whether users of a "social" online network can give valid consent if that network holds a dominant position in the market (para. 140). The CJEU did not have access to facts regarding this type of consent (such as consent rates and the financial circumstances surrounding consent).

82. Paragraph 150 of this CJEU judgment is therefore, as far as can be seen, a classic *obiter dictum.* In its response, the CJEU stated (para. 150):

"Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, <u>if necessary</u> for an <u>appropriate</u> fee, an equivalent alternative not accompanied by such data processing operations."

83. The judgment did not elaborate further on what "if necessary" and "appropriate" mean in this context. It should also be noted that this statement was not made in isolation. In the same judgment, the CJEU states that the free will of the individuals concerned must be respected in any case, for example in paragraph 143.

84. In its Opinion 08/2024, the EDPB also assumes, based on the above CJEU ruling, that when faced with a choice between payment and consent, valid consent is not given, at least "as a rule" (or "in most cases").

4.4. Withdrawing consent is not as easy as giving it

85. Article 7(3) GDPR reads: "*It shall be as easy to withdraw as to give consent.*"

86. Under the respondent's "pay or okay" system, granting consent requires users to make a quick selection on a prominent banner that is displayed and designed to be interacted with. Withdrawing consent, in turn, not only requires the complainant to laboriously locate the option within the website options, but also involves creating a new Schibsted account or logging into their existing account and making a payment with the corresponding effort (see above 4.3.1.2).

87. This creates a detriment resulting from the withdrawal, contrary to recital 42 GDPR, as it leads to costs. The EDPB states:

"*The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.*"[41]

88. This therefore constitutes a violation of Article 7(3) of the GDPR. This lack of the right to freely withdraw consent also renders the complainant's consent invalid.

4.5. The protection of personal data is not a commodity

4.5.1. *The protection of personal data is a fundamental right*

89. Fundamental rights are, by definition, inalienable.

90. Article 102 of the Constitution of Norway establishes that everyone has the right to the respect of their privacy and family life, their home and their communication, and that the authorities of the state shall ensure the protection of personal integrity. Article 8(1) ECHR states that everyone has the right to respect for his private and family life, his home and his correspondence.

91. The fundamental right to data protection is binding upon the respondent, too, pursuant to Article 1(2) GDPR, at the very least.

92. When the protection of personal data is made conditional upon payment, it is no longer available to everyone and loses its very essence as a fundamental right.

93. Therefore, the commodification of the protection of personal data is not compatible with its nature as a fundamental right.

94. This core principle of European data protection law has been appropriately recognized by the EDPB in both its guidance and its decisions:

"The GDPR, pursuant to EU primary law, treats personal data as a fundamental right inherent to a data subject and his/her dignity, and not as a commodity data subjects can trade away through a contract."[42] (emphasis added)

"Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity."[43] (emphasis added)

95. In particular the EDPB highlights that the right to data protection applies to everyone, independently of their financial situation:

*"The EDPB wishes to recall first and foremost that **personal data cannot be considered as a tradeable commodity**. The right to data protection is enshrined inter alia in Article 8 of the Charter for Fundamental*

[41] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, V. 1.1, para. 46.

[42] EDPB, Binding Decision 3/2022, para. 101.

[43] EDPB, Guidelines 2/2019, para. 54.

Rights and is a right that applies to all, regardless of payment or financial status."[44] (first emphasis in original, last emphasis added)

96. However, in situations where "pay or ok" systems are used, the fundamental right to data protection is made conditional upon a payment. Only if you pay your right to the protection of personal data will be respected.

97. This degrades the right to data protection to a commodity. Data protection may become a luxury only available to the well-off. This is incompatible with its nature as a fundamental right.

4.5.2. No legal basis for limiting the right to data protection

98. Any limitation of the fundamental right to data protection must be provided for by law (cf. Article 8(2) ECHR and Norwegian Supreme Court decision HR-2015-206, para. 57).

99. However, the GDPR does not contain any provision that allows controllers to require a data subject to pay for refusing consent. Nor does the GDPR require a payment in order to enjoy the protection foreseen in Articles 6 or 9 of the GDPR.

100. In the absence of such a provision, the "pay or ok" model of the respondent imposes an unlawful limitation on the fundamental right to data protection of the complainant.

101. If the legislator had intended to allow controllers to charge data subjects for refusing consent, the GDPR would explicitly allow such a practice and would precisely lay out the conditions in which it is permissible, as was done for some other exceptional situations (see also above 4.2.3).

5. REQUESTS AND SUGGESTIONS

5.1. Request to investigate

102. In light of the above, the complainant requests a prompt investigation and decision on their case, as the facts are sufficiently clear and only the related legal issues need to be addressed. This case concerns a practice that the complainant considers highly problematic and unlawful. Since a significant and well-known Norwegian actor now chooses to introduce "pay or okay", it is necessary that the Norwegian Data Protection Authority acts efficiently in accordance with its mandate.

5.2. Request for a declaratory decision

103. In light of the above, the complainant requests the competent authority to declare:

(a) the respondent's processing of the complainant's personal data for personalized advertising to be unlawful, as it lacks a legal basis under Article 6(1) GDPR,

(b) that the respondent did not obtain valid consent from the complainant,

[44] EDPB, Opinion 08/2024, para. 130.

(c) that the respondent is in violation of Article 5(1)(a) GDPR due to processing the personal data of the complainant without a legal basis,

(d) that the respondent is in violation of Article 7(4) GDPR by bundling the consent request to the complainant with a service, where this is objectively not necessary, and

(e) that the respondent is in violation of Article 7(3) GDPR, as the complainant could not withdraw consent as easily as they could give it.

5.3. Request for an order

104. In light of the above, the complainant requests the competent authority to order the respondent:

(a) to permanently cease processing the complainant's personal data for the purpose of personalized advertising without a valid legal basis (Article 58(2)(f) GDPR),

(b) to erase the complainant's personal data that has been processed for the purpose of personalized advertising (Article 58(2)(g) in conjunction with Article 17(1)(d) GDPR), and to notify all recipients of this deletion (Article 58(2)(g) in conjunction with Article 19 of the GDPR), and

(c) bring its processing operations into compliance with the GDPR (Article 58(2)(d) GDPR), and in particular obtain valid consent from the complainant.

5.4. Suggestions

105. The complainant suggests that the competent authority order the respondent to bring its processing operations into compliance with the GDPR (Article 58(2)(d) GDPR) and in particular to obtain valid consent from all data subjects.

106. The complainant suggests imposing an effective, proportionate, and dissuasive fine for the violations. In this regard, particular consideration should be given to the fact that the respondent:

(a) intentionally and systematically violates the GDPR (Article 83(2)(b) GDPR),

(b) to safeguard its business model (Article 83(2)(a) GDPR), and

(c) in doing so, knowingly accepts the violation of the rights of millions of its readers (Article 83(2)(a) GDPR), while

(d) it derives direct financial benefits from these violations (Article 83(2)(k) GDPR), and

(e) at the same time prevents fair, undistorted competition (Article 83(2)(k) GDPR),

(f) even though it has ample financial resources at its disposal to implement legally compliant technical consent requests (Article 83(2)(k) GDPR).

6. CONTACT

107. Communications between *noyb*, the NCC and the competent authority in the course of this procedure can be done by email at [redacted] and [redacted] with reference to the **Case number C106** or [redacted].