

Xandr Inc.

Exempt from public disclosure:

Offentlighetsloven § 13 jf. forvaltningsloven § 13 (1) nr. 2

Your reference
[Click here to enter text.](#)

Our reference
20/03541-37

Date
02.10.2026

Administrative fine – Unlawful processing of personal data

Table of Content

Executive Summary	2
1. Introduction.....	3
2. Decision	3
3. Background of the case	4
3.1. About Xandr Inc. and its services	4
3.2. About Grindr LLC and the Grindr app.....	4
3.3. Complaints from the Norwegian Consumer Council.....	5
3.4. Scope of the investigation of the NO DPA.....	7
3.5. Timeline of the NO DPA's investigation	8
4. Relevant GDPR provisions	10
4.1. Material scope.....	10
4.2. Controller and Processor	10
4.3. Territorial scope	11
4.4. The Supervisory Authority.....	11
4.5. Accountability obligations	12
4.6. Legal basis and valid consent	13
4.7. Processing of special categories of data.....	14
4.8. General conditions for imposing administrative fines	14
5. Competence, Tasks and Powers of Supervisory Authorities under the GDPR.....	16

6.	The NO DPA's assessment of the case	17
6.1.	Initial remarks.....	17
6.2	Introduction to the Real-Time Bidding process.....	17
6.3	Xandr's role in the Real-Time Bidding process.....	18
6.4	Processing of ad and bid requests.....	21
6.5	Personal data.....	25
6.6	Controllorship.....	26
6.7	Accountability.....	33
6.8	Special categories of data.....	34
6.9	Legal basis.....	38
7	Imposition of an administrative fine	39
7.1	Introduction.....	39
7.2	Whether to impose an administrative fine	39
7.3	Deciding the amount of the administrative fine	50
8	Right of appeal	54
9	Access to documents.....	54

Executive Summary

Following a complaint from the Norwegian Consumer Council, the Norwegian Data Protection Authority (hereinafter “NO DPA”) has decided to impose an administrative fine of NOK 92 000 000 on Xandr Inc. for processing personal data of Grindr users in Norway without a legal basis in violation of Article 6(1) GDPR, and for processing special category personal data concerning sexual orientation without a valid exemption, in violation of Article 9(1) GDPR.

The case concerns real-time bidding. The NO DPA has found it proven by clear preponderance of probability that Xandr processed Grindr users' personal data, at least the fact that individuals were using Grindr, their advertising ID and IP addresses, during real-time bidding. These are personal data under Article 4(1) GDPR and data concerning sexual orientation under Article 9(1) GDPR.

Xandr is considered a joint controller for the processing, both as supply-side and demand-side platform. Since the data were special category data, explicit consent under Article 9(2)(a) was the relevant legal basis for the processing. Xandr did not obtain consent itself, but relied on Grindr's consent, which were invalid under Articles 4(11) and 7 GDPR. The NO DPA holds that accountability cannot be outsourced; each joint controller must independently verify that consent is valid and covers its own processing.

The infringements were at least negligent. In light of the fact that the infringements concern some of the most central provisions in the GDPR, including sensitive data, the NO DPA regards the infringements of high seriousness.

1. Introduction

In 2020, the NO DPA received complaints from the Norwegian Consumer Council (“NCC”) against Grindr LLC (hereinafter “Grindr”, “it”), Xandr Inc. (“previously known as AppNexus Inc., hereinafter “Xandr”, “it”) and four other AdTech companies. The complaints from the NCC are based on two reports¹ regarding the AdTech industry and its alleged infringements of the General Data Protection Regulation (“GDPR”).²

The background of the case, including the NO DPA’s investigation, is described in section 3. Information on legal background can be found in sections 4 and 5, and NO DPA’s assessments are contained in sections 6 and 7.

This decision takes Xandr’s response of 2 June 2025 to NO DPA’s advance notification into full consideration. In NO DPA’s view, Xandr’s comments do not warrant changes to NO DPA’s assessments, as further explained in the sections below. While not every individual argument will be addressed separately in the decision, each has been examined and weighed in reaching the final conclusions.

NO DPA hereby adopt the following decision in which NO DPA impose an administrative fine to Xandr for the reasons outlined below.

2. Decision

Pursuant to Article 58(2)(i) GDPR, cf. Article 83 GDPR NO DPA impose an administrative fine against Xandr Inc. of NOK 92 000 000 for

- *having processed personal data of Grindr users in Norway without a legal basis, which constitutes a violation of Article 6(1) GDPR*
- and*
- *having processed special category personal data of Grindr users in Norway without a valid exemption from the prohibition in Article 9(1) GDPR.*

¹ See NCC Report (<https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf>) and “Technical report: Out of Control” (<https://storage02.forbrukerradet.no/media/2020/01/mnemonic-security-test-report-v1.0.pdf>).

² 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.xz

3. Background of the case

3.1. *About Xandr Inc. and its services*

AT&T acquired AppNexus Inc. pursuant to a transaction closed on 15 August 2018.³ AppNexus Inc. was renamed Xandr Inc. on 1 July 2019,⁴ and on 6 June 2022, Microsoft Corporation (hereinafter “Microsoft”), acquired Xandr.⁵ Xandr Inc. is thus a U.S based company, now a part of Microsoft.

Xandr is an advertiser technology company, providing “a data-enabled technology platform with tools that help power a diverse ecosystem connecting marketers and media owners through first-party, data-led advertising solutions across its network.”⁶

According to Xandr’s Privacy Policy which applied in 2019,⁷ Xandr’s platform allows buyers and sellers to engage in various forms of targeted and behavioural advertising, and to buy and sell data:

[...] buyers and sellers and their partners use our Platform to engage in a variety of techniques, including interest-based advertising, real-time (or programmatic) advertising, contextual, and location-based advertising.

[...] Buyers, sellers, and other companies may also use our Platform to buy and sell data to help make the ads that end users see more relevant.

For more information regarding Xandr’s services and its role in connection to the scope of the complaint, see Section 6.2 and 6.3 below.

3.2. *About Grindr LLC and the Grindr app*

Grindr is a U.S. company founded in 2009. Grindr markets its mobile application (hereinafter “app” or “Grindr app”) as the world’s largest network for gay, bi, trans and queer adults.⁸

According to Grindr, the Grindr app is a social networking app designed to permit users to share information about themselves with other users in order to facilitate user interactions and connections. Grindr states that it is the number 1 social network for the LGBTQ+ community with more than 13 million monthly active users and users in virtually every country in the world.⁹

³ https://about.att.com/story/2018/att_appnexus.html [last accessed 19 March 2025].

⁴ Reply to order to provide information 16 July 2020 – Cross-Border Processing

⁵ Reply to order to provide information 26 May 2023.

⁶ <https://about.ads.microsoft.com/en-us/blog/post/december-2021/microsoft-to-acquire-xandr-to-accelerate-its-digital-advertising-and-retail-media-solutions> [last accessed 19 March 2025].

⁷ NCC Report p. 132, refers to Xandr’s Privacy Policy (last updated October 24, 2019). <https://www.appnexus.com/platform-privacy-policy#infocollect> (now invalid link).

⁸ <https://www.grindr.com/about/> [last accessed 12 August 2026].

⁹ <https://investors.grindr.com/overview/default.aspx> [last accessed 19 March 2025].

The app has a version that may be downloaded and used free of charge (hereinafter “free version”). Users can upgrade to the “XTRA” or “Unlimited” versions of the app, which include various premium features, for a paid subscription.¹⁰

As a part of its free application service, Grindr displays advertising banners in its app. Grindr also lets third party advertisers collect information about its users, as part of this process. The Grindr app includes SDKs (software development kit – a piece of software that can be incorporated into another software for functional or advertising purposes) from some companies, one of which was MoPub. MoPub collected data through the SDK and managed requests from other third-party companies such as Xandr.¹¹

3.3. Complaints from the Norwegian Consumer Council

On 14 January 2020, the NO DPA received complaints from the NCC against, amongst others, Grindr and Xandr, representing a Norwegian data subject pursuant to GDPR Article 80(1).¹² The complaint against Xandr must be seen in connection with the complaint against Grindr.

The subject matter of the complaint is alleged unlawful processing and sharing of users’ personal data between Grindr and several advertising partners, including Xandr. The complainant claims that these companies process personal data unlawfully under Article 6 and 9 GDPR.

When referring to the Grindr app herein, the NO DPA exclusively mean the free version of the app.

The complaint was accompanied by, *inter alia*:

- The NCC’s Report “Out of Control” (hereinafter “NCC Report”),¹³
- a related technical report prepared by the company Mnemonic, which the NCC had commissioned (hereinafter “Mnemonic technical report” or “technical report”),¹⁴
- Xandr’s Privacy Policy (downloaded 8 January 2020),
- MoPub’s Privacy Policy (downloaded 10 December 2019),
- List of MoPub Partners (downloaded 16 December 2019), and
- MoPub Publisher Best Practices (downloaded 11 January 2020).

¹⁰ <https://help.grindr.com/hc/en-us/articles/1500008656241-Grindr-XTRA> and <https://help.grindr.com/hc/en-us/articles/1500008656741-Grindr-Unlimited> [last accessed 19 March 2025].

¹¹ The complaint Section 2.1. For more information on SDK’s see the NCC Report pp. 17-18.

¹² The public version on the complaint can be found here, <https://storage02.forbrukerradet.no/media/2020/01/20200114-complaint-grindr-twitter-mopub-appnexus-openx.pdf> [last accessed 19 March 2025].

¹³ See footnote 1.

¹⁴ See footnote 1.

3.3.1. The Grindr complaint

According to the complaint against Grindr, Grindr's consent mechanism applicable at the time of the NCC's inquiry infringed the requirements for valid consent in Articles 4(11), 6(1)(a), 7 and 9(2)(a) of the GDPR. As a result, the NCC argued that Grindr lacked a legal basis for sharing personal user data with its advertising partners when providing advertising in the Grindr app. Furthermore, the NCC claimed that Grindr had infringed the prohibition set out in Article 9(1) of the GDPR by sharing data "concerning" a natural person's "sexual orientation".

According to both the Privacy Policy in effect before 31 December 2019 and the Privacy Policy in effect from 31 December 2019, Grindr shared the following data with third party advertising companies:

[...] your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Location Information, and some of your demographic information with our advertising partners.

In its Privacy Policy in effect from 31 December 2019, Grindr stated that it shared the following personal data with its advertising partners:

Personal Data we collect from you, including: Hardware and Software Information; Profile Information (excluding HIV Status and Last Tested Date and Tribe); Location and Distance Information; Cookies; Log Files and Other Tracking Technologies. Additional Personal Data we receive about you, including: Third-Party Tracking Technologies.

In the NCC Report, NCC refers to the Grindr Privacy Policy which only names one such advertising partner, namely MoPub. MoPub, on the other hand, lists 160 partners.¹⁵

The NCC had concerns over Grindr's statement that it does "not control the use of these tracking technologies" while asking users to read the privacy policies of any third parties that may receive personal data. The NCC claims it is not clear how the user would be able to read the privacy policy of any other advertising partners, and that Grindr does not take adequate responsibility as a controller of personal data collected and shared through its services.

With regards to the processing by Grindr, the NO DPA imposed a fine of NOK 65 000 000 on the company on 13 December 2021, due to lack of valid legal basis pursuant to Article 6(1) GDPR for the processing of personal data by disclosure to advertising partners for advertising purposes in the time period 20 July 2018 and 7 April 2020.¹⁶ Furthermore, NO DPA found that Grindr processed data "concerning" a natural person's "sexual orientation" unlawfully

¹⁵ NCC Report p. 74.

¹⁶ NO DPA decision in the case against Grindr, 13 December 2021. The public version of the decision can be found here:

<https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/>

pursuant to Article 9(1) by sharing personal data on a specific user alongside app name or app ID to advertising partners.¹⁷

These conclusions were later upheld by the Norwegian Privacy Appeals Board,¹⁸ Oslo District Court¹⁹ and Borgarting Court of Appeal.²⁰

3.3.2. The Xandr complaint

In summary, the NCC makes the following allegations in its complaint against Xandr:²¹

1. The collection and further processing of Grindr user's data by Xandr does not have a valid legal basis under Article 6 GDPR.
2. The collection and further processing of information on Grindr user's sexual orientation by Xandr does not fall within the exceptions provided in Article 9(2) GDPR and is therefore not lawful according to Article 9(1) GDPR.

3.4. *Scope of the investigation of the NO DPA*

3.4.1. Temporal scope

The NCC commissioned the cybersecurity company mnemonic AS to perform technical testing of the data flow from the Grindr app to third party companies. The tests were performed between 8 July and 31 December 2019 ("mnemonic investigation period").

The NO DPA's investigation in the Grindr case were limited to the time period between 20 July 2018 and 7 April 2020.²² Xandr has confirmed that it did receive requests for bids to display ads on the Grindr app relating to Grindr users in Norway and that it processed data contained in those bid requests to display ads to Norwegian users of the Grindr app within this time period.²³ According to Xandr's understanding, however, they did not receive such requests in every month of this period.²⁴

¹⁷ *Ibid.*

¹⁸ PVN-2022-22. The public version of the decision can be found here, in Norwegian: <https://www.personvernemnda.no/pvn-2022-22>.

¹⁹ 23-160384TVI-TOSL/04 p. 26. The public version of the decision can be found here, in Norwegian: <https://lovdata.no/dokument/TRSIV/avgjorelse/tosl-2023-160384?q=23-160384TVI-TOSL/04>

²⁰ 24-154313ASD-BORG/02 of October 21st 2025 pp. 9-37. Public version can be found here in Norwegian: [104-01-dom-av-21.-oktober-2025.pdf](https://lovdata.no/dokument/TRSIV/avgjorelse/104-01-dom-av-21-oktober-2025.pdf)

²¹ In the following, NO DPA will refer to the company against which the complaint is lodged as Xandr. However, please note that the original complaint was made against AppNexus Inc. Having been in contact with Xandr, it is the NO DPA's understanding that Xandr absorbed AppNexus Inc. and later it became a part of Microsoft.

²² The investigations were limited to the time period when Grindr's previous Consent Manager Platform was used. The new Consent Manager Platform was deployed for data subjects in Norway as of 8 April 2020. The NO DPA also limited the investigation to the time period following the entry into effect of the GDPR in Norway. As mentioned below in Section 4.3, the GDPR entered into force in Norway on 20 July 2018.

²³ Reply to order to provide information 6 December 2024.

²⁴ Reply to order to provide information 6 December 2024.

Thus, the NO DPA has limited the investigations to the time period between 20 July 2018 and 7 April 2020 also for the Xandr complaint (hereinafter “investigation period”).²⁵

3.4.2. Material scope

The NCC Xandr complaint requested that the NO DPA took actions to determine:

- which processing operations Xandr engage in;
- for which purpose they are performed, and
- which legal basis Xandr rely on.

In addition, the NCC requested that Xandr is compelled “to erase all unlawfully processed personal data without undue delay (Article 17(1)(d) GDPR) and to prohibit the relevant processing operations in accordance with the powers vested in you, including by Article 58(2)(d), (f), and (g) GDPR.”²⁶

Xandr has stated that all personal data it may have processed about Grindr users would have been deleted in accordance with Xandr’s retention policy.²⁷ The NO DPA therefore limited the investigation to the lawfulness under Article 6 and 9 GDPR of the collection²⁸ and sharing of Grindr user’s data by Xandr.

The fact that some issues have fallen outside the scope of the NO DPA’s investigation does not preclude those issues from being addressed in the future. Xandr must make sure that all processing of personal data of data subjects in the EEA is compliant with the GDPR at all times. The NO DPA may decide to investigate additional issues at a later stage, following individual complaints or *ex officio*, in accordance with Articles 57 and 58 GDPR.

Furthermore, it should be noted that, even though information about Grindr and MoPub is included in the following, the NO DPA has not conducted any legal assessments concerning these companies’ activities in the present case.

3.5. *Timeline of the NO DPA’s investigation*

- On 21 February 2020, the NO DPA sent Xandr an order to provide information about cross-border processing.
- Xandr asked for an extended deadline to reply to the order to provide information, and as per Xandr’s request, the NO DPA extended Xandr’s deadline from 16 March 2020 to 17 July 2020.
- Xandr submitted its response to the NO DPA on 16 July 2020.

²⁵ Note in some of its submissions Xandr refers to July 20th 2018 to April 7th 2020 as the “new investigation period”. Whenever Xandr in its submissions before the advance notification referred to “investigation period”, it refers to the mnemonic investigation period of 8 July-31 December 2019.

²⁶ The complaint p. 24.

²⁷ Reply to order to provide information 26 May 2023.

²⁸ “Collecting” and “receiving” will be used interchangeably throughout this decision to describe the same action

- On 6 February 2023, the NO DPA sent Xandr an order to provide information about the processing of personal data shared by Grindr, including, amongst other, questions related to which personal data Xandr collected/shared, for which purposes and under which legal bases. The deadline for reply was set to 27 February 2023.
- Due to change in staff, the letter was not forwarded to the correct recipient within Xandr until 28 March 2023. In its letter of 6 April 2023, Xandr requested an extension of the deadline to 2 May 2023.
- On 2 May 2023, Xandr contacted us with an additional extension request. The reason for this request was in part because Xandr's business relationship with Grindr was terminated in October 2021, and certain of the requested information appeared to no longer be available to Xandr. Furthermore, Xandr requested access to the documents in the case pursuant to Sections 18 and 19 of the Norwegian Public Administration Act.
- On 2 May 2023, it was agreed over the phone to extend the deadline to 26 May 2023. This was also confirmed in an email from the NO DPA on 3 May 2023.
- On 5 May 2023, the NO DPA replied to the access request.
- On 26 May 2023, Xandr responded to the order to provide information about the processing of personal data shared by Grindr.
- On 23 August 2023, the NO DPA requested a copy of the International Data Addendum ("IDA") between Grindr and Xandr that was in force during the investigation period, in addition to information about the relationship with MoPub.
- On 25 August 2023, Xandr sent a template IDA in addition to request an extension to 8 September 2023 to provide a complete response for the question on its relationship with MoPub.
- On 8 September 2023, Xandr requested a further extension until 2 October 2023 to respond.
- On 2 October 2023, Xandr responded to the additional request for information.
- On 27 November 2024, the NO DPA sent Xandr an additional order to provide information about, *inter alia*, the temporal scope of processing, the data flows and the matching process. The deadline for reply was set to 6 December 2024.
- On 29 November 2024, Xandr replied and requested an extension until 20 December 2024.
- On 29 November 2024, the NO DPA replied and agreed to extend the deadline for some of the questions.
- On 6 December 2024, Xandr replied to question 1.
- On 20 December 2024, Xandr responded to the remaining questions in the order to provide information.
- On 27 February 2025, an informal digital meeting was held between the NO DPA and Xandr upon request from the NO DPA. The meeting was voluntary, and the purpose was to ensure accuracy and a common understanding of the factual elements of the case.
- On 18 March 2025, the NO DPA sent Xandr an order to provide information about its total worldwide annual turnover in the preceding business year.
- On 25 March 2025, Xandr submitted its response.

- On 3 April 2025, NO DPA sent Xandr an advance notification of intention to issue an administrative fine.
- On 2 June 2025, Xandr replied and sent their comments to the advance notification, including new information on its total worldwide annual turnover.
- On 20 June 2025, Xandr sent their input and suggestions for redaction of the advance notification.
- On 23 June 2025, NO DPA confirmed receipt of documentation.
- On 3 June 2026, NO DPA sent Xandr an order to provide information about its total worldwide annual turnover in the preceding business year.
- On 15 June 2026, Xandr replied and sent new information on its total worldwide annual turnover.

4. Relevant GDPR provisions

4.1. *Material scope*

Article 2(1) GDPR provides that the Regulation applies to “the processing of personal data wholly or partly by automated means [...]”.

Article 4(1) GDPR defines “personal data” as:

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.

Article 4(2) GDPR defines “processing” as:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means [...]

4.2. *Controller and Processor*

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 [...].

Pursuant to Article 4(8) GDPR, “processor” means:

a natural or legal person, public authority, agency or other body which processes personal data on behalf of controller;

4.3. Territorial scope

The Norwegian Personal Data Act incorporates the GDPR into Norwegian law.²⁹ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

Article 3(1) GDPR reads as follows:

This 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 Union³⁰, regardless of whether the processing takes place in the Union or not.

Article 3(2) GDPR provides that:

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*

4.4. The Supervisory Authority

Pursuant to Article 51(1) GDPR:

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

The NO DPA is the national GDPR supervisory authority in Norway, pursuant to Section 20 of the Norwegian Personal Data Act.

Article 55(1) GDPR regulates the supervisory authority's competence:

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.

²⁹ Act relating to the processing of personal data 15 June 2018 no. 38 ([The Personal Data Act](#)) (Lov om behandling av personopplysninger (personopplysningsloven)). A link is provided to an unofficial translation of the law to English. The Norwegian law text prevails.

³⁰ Should be understood as the European Economic Area (EEA), pursuant to Protocol 1 Section 8 of the EEA Agreement.

Article 57(1) GDPR sets forth the tasks of the supervisory authority:

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;

[...]

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

[...]

Article 58(2) GDPR regulates the supervisory authority's corrective powers:

Each supervisory authority shall have all of the following corrective powers:

[...]

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

[...]

4.5. Accountability obligations

Pursuant to Article 5(2) GDPR:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

According to Article 24(1) and (2) GDPR the responsibility of the controller entails that:

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

4.6. Legal basis and valid consent

Pursuant to Article 6(1) GDPR:

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

[...]

(f) 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.

Article 4(11) GDPR provides that:

‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 7 GDPR on the conditions for consent provides that:

- 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*
- 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*
- 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*
- 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*

4.7. Processing of special categories of data

Article 9(1) GDPR provides that:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Article 9(2) GDPR further provides that:

Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

[...]

(e) processing relates to personal data which are manifestly made public by the data subject;

[...]

4.8. General conditions for imposing administrative fines

Article 83 GDPR provides that:

- 1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.*
- 2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:*
 - (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
 - (b) the intentional or negligent character of the infringement;*

- (c) *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
 - (d) *the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
 - (e) *any relevant previous infringements by the controller or processor;*
 - (f) *the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
 - (g) *the categories of personal data affected by the infringement;*
 - (h) *the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;*
 - (i) *where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*
 - (j) *adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;*
 - (k) *any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*
3. *If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*
5. *Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:*
- (a) *the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;*
- [...]

5. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

The NO DPA refers to Articles 55(1), 56(1), 58(1) and 58(2) GDPR regarding NO DPA's competence, tasks and powers. Pursuant to Article 3(1) GDPR, the GDPR applies to processing of personal data by Xandr where the company acts as controller, joint controller and/or processor, regardless of whether the processing activities take place in or outside the EEA. With respect to the processing activities covered by the scope of the investigation, Xandr qualifies as processor (cf. Article 4(8) GDPR) or controller (cf. Article 4(7) GDPR) depending on the processing at hand.

According to Xandr's response of 16 July 2020 to the NO DPA's order to provide information, Xandr does not consider any of its EEA establishments to be a main establishment.³¹ It upholds that Xandr's establishments in the EEA are sales offices, involved in promoting Xandr's advertising services which relate to the serving of adverts to individuals in the EEA. They do this by building business relationships with actual and potential Xandr clients on both the supply side (i.e. publishers) and bid side (i.e. advertisers).

According to Xandr, their EEA offices do not make decisions on purposes and means of processing. The NO DPA emphasizes, in order to determine that the processing takes place 'in the context of the activities of establishments' of a controller or processor, it does not need to be carried out directly by that establishment.³² It is enough that the processing is inextricably linked to the activities of that company. The NO DPA considers that the processing in this case is covered by the territorial scope in Article 3(1) GDPR.³³

Based on the response provided by Xandr, Xandr did not have a "main establishment" within the EEA area pursuant to Article 4(16) GDPR during the investigation period, and that, consequently, the processing of personal data in question at that time does not qualify as "cross-border processing" pursuant to Article 4(23) GDPR.³⁴

The fact that Xandr subsequent to the investigation period has been acquisitioned by Microsoft does not change this. For Xandr's processing that took place in the investigation period, no Microsoft establishment could have "take[n] the decisions on the purposes and means of the processing of personal data and [had] power to have these decisions implemented", which is a requirement in order to qualify as a main establishment.³⁵

Therefore, the cooperation mechanism set out in Article 56(1) and Chapter VII Section 1 of the GDPR does not apply. For this reason, the NO DPA is competent to perform our tasks under the GDPR in relation to the Xandr complaints in accordance with Article 55(1).

³¹ Reply to order to provide information 16 July 2020 – Cross-Border Processing, p.3.

³² CJEU case C-131/12, Google Spain, para. 52–53, and CJEU case C-230/14, Weltimmo, para. 25 and 35.

³³ Even if Xandr had not been established in the EEA, the GDPR would apply pursuant to Article 3(2) as the processing was related to the offering of services to data subjects in Norway.

³⁴ Reply to order to provide information 16 July 2020 – Cross-Border Processing. This is in line with the EDPB's view, see [EDPB Report of the work undertaken by the ChatGPT Taskforce](#) 23 May 2024, para. 8.

³⁵ [EDPB Opinion 04/2024](#) on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR, para 27.

The NO DPA's competence in this case is limited to safeguarding the data protection rights of users within Norwegian territory. Therefore, this decision is without prejudice to the competence of GDPR supervisory authorities in other EEA territories.

6. The NO DPA's assessment of the case

6.1. *Initial remarks*

In assessing Xandr's compliance with the GDPR, the NO DPA has relied on the relevant facts available in this case, including the statements submitted by Xandr.

In its response to the advance notification, Xandr has stated that the NO DPA repeatedly makes assumptions that are unfavourable to Xandr and states that, given the legal uncertainty, the NO DPA should accept Xandr's position.³⁶ The NO DPA notes, however, that Xandr has modified its position on several substantive issues in the course of its response to the advance notification.³⁷

Furthermore, upon the NO DPA's request, Xandr has been unable to produce certain documentation, arguing that it has been deleted in accordance with Xandr's legal obligations and good practice data retention policies during the period from 16 July 2020 to 6 February 2023. This deletion occurred notwithstanding that Xandr had been aware of the NO DPA's investigation since 21 February 2020.³⁸ The NO DPA takes the view that the deletion of potential evidence after the commencement of an investigation cannot be invoked in Xandr's favour. On the contrary, the NO DPA maintains that the burden of demonstrating compliance and accountability pursuant to Article 5(2) GDPR rests upon Xandr itself. Any alternative approach would establish an unacceptable precedent, as it would in practice incentivise undertakings to erase documentation in order to circumvent supervision by data protection authorities.

6.2 *Introduction to the Real-Time Bidding process*

Before assessing Xandr's role and which personal data of Grindr users Xandr processed, the NO DPA will provide a general overview of the Real-Time Bidding ("RTB") process and the personal data flow in this process, in order to clearly state the facts on which our assessment is made. The NO DPA will also provide definitions of central concepts. It should be noted that the following provides a somewhat simplified overview of a complex process.

RTB plays a central role in the AdTech industry and digital marketing. It can be explained as an automated process in which ad space – also known as "ad inventory" or "digital inventory" – is bought and sold through an auction that occurs in real-time. It takes place every time a user visits a website or app where digital inventory is available. The industry considers that

³⁶ Response to the advance notification 2 June 2025 p. 3 and 4.

³⁷ Response to the advance notification 2 June 2025 p. 3, 4 and 32. This decision p. 24.

³⁸ Response to the advance notification 2 June 2025 p. 3.

RTB enables advertisers to target the users of the website or app more precisely and allows publishers to maximize revenue by selling their inventory at the highest price.

RTB relies on several key actors in the AdTech ecosystem. The main actors can be categorised as follows:

1. **Publishers (Supply-Side)** provide the digital platforms – such as websites and mobile apps – where advertisements are displayed. They own the ad inventory being sold in RTB. Their goal is to monetize their platforms by selling ad space to the highest-paying advertisers. In this context, Grindr would be the publisher.
 - Publishers often use a **Supply-Side Platforms (“SSPs”)** to manage and optimize the sale of their ad inventory.
2. **Advertisers (Demand-Side)** are the brands, businesses, or organizations that want to display ads to reach their target audience. They buy ad impressions, i.e. for people to see their ads, through RTB auctions, and hence they may also be referred to as buyers.
 - Advertisers often use **Demand-Side Platforms (“DSPs”)** to analyse requests to buy advertising space and decide how much to bid.
3. **Ad Exchanges (Marketplaces).** The ad exchange is the technology platform that connects SSPs (publishers) with DSPs (advertisers) to facilitate RTB auctions. It receives bid requests from the SSPs, runs the auction among DSPs, and sends the winning ad back to the publisher.
 - Through these ad exchanges, a number of **third-party vendors or major platforms** are often involved in the RTB process, including for example analytics vendors and data brokers.³⁹
4. **Users (Audience).** The user is the individual visiting the publisher’s platform, triggering the RTB process. User data, e.g., location, device, and browsing behaviour, is used to match the user to the right advertiser. The user’s goal may be unrelated to advertising, such as consuming content or using an app, but their interaction drives the demand for targeted ads. In this context, the audience would be the Grindr users in Norway.

6.3 Xandr’s role in the Real-Time Bidding process

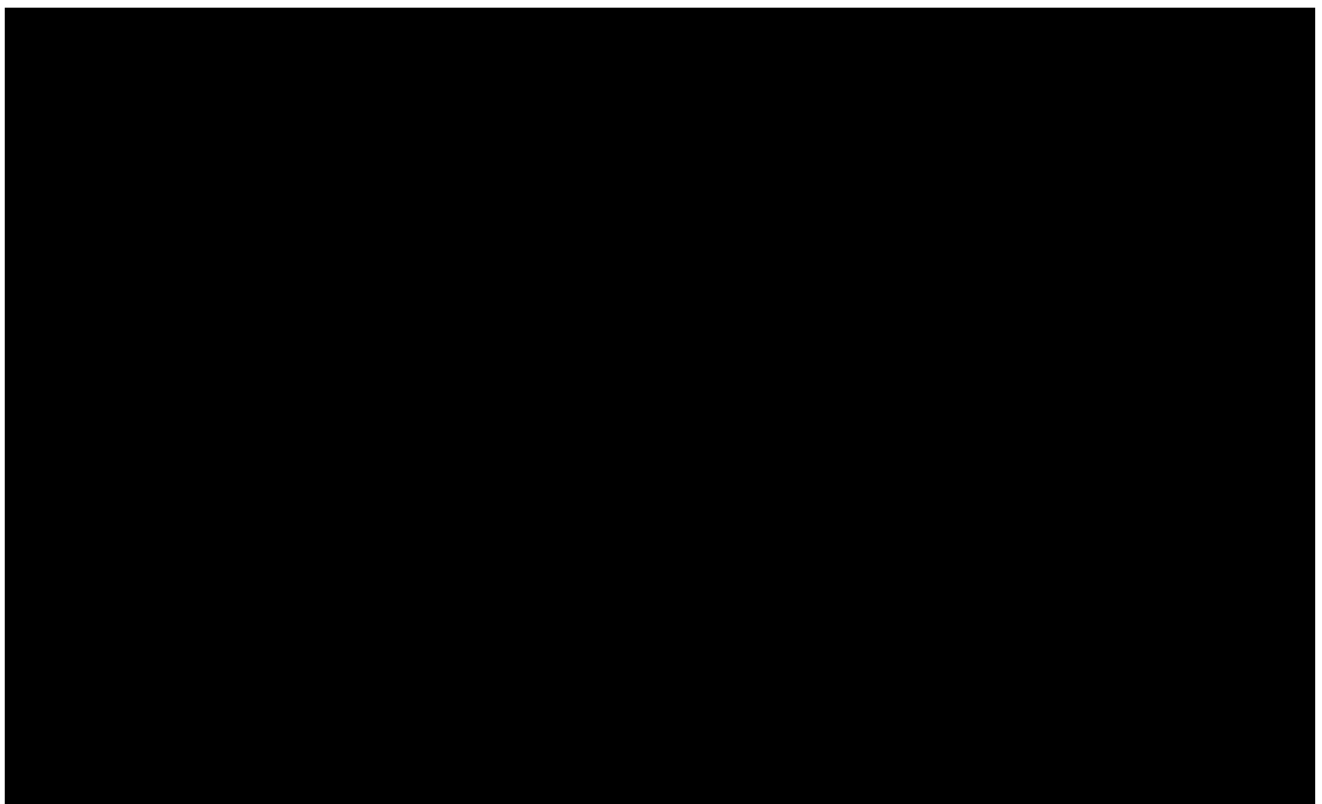
To reiterate, **Xandr’s Platform** allows buyers and sellers to engage in various forms of targeted and behavioral advertising, and to process data on data subjects:

[...] buyers and sellers and their partners use our Platform to engage in a variety of techniques, including interest-based advertising, real-time (or programmatic) advertising, contextual, and location-based advertising.

³⁹ NCC Report pp. 14-15.

*[...] Buyers, sellers, and other companies may also use our Platform to buy and sell data to help make the ads that end users see more relevant.*⁴⁰

The NO DPA is of the understanding that the platform is the underlying technology infrastructure (back-end infrastructure) that powered Xandr's AdTech services, including, *inter alia*, ad exchanges and the systems that enable RTB and ad delivery. Thus, at the time of investigation, Xandr provided both a supply side platform and a demand side platform, meaning that it facilitated parts of the RTB system for a large number of AdTech actors.⁴¹ This is also in line with the Overview of Ad Call Data Flow for RTB-auctions (hereinafter the "Overview"):⁴²



Xandr's console ("Console"), on the other hand, is the front-end tool for its providers/clients to interact with the Xandr Platform. Thus, the Console allowed Xandr's clients (including Grindr and MoPub) to conduct, optimize and track their advertising transactions.⁴³

In line with the Overview provided by Xandr, which was further explained to the NO DPA during the 27 February 2025 meeting, the RTB process applicable at the time of investigation can be illustrated as follows:

⁴⁰ NCC Report p. 132, refers to Xandr's Privacy Policy (last updated October 24, 2019).

⁴¹ NCC Report p. 131.

⁴² Reply to order to provide information 20 December 2024, Exhibit A.

⁴³ Reply to order to provide information 20 December 2024 and Reply to order to provide information 26 May 2023.

1. A user would visit the digital property (here: the Grindr app) and an ad space in the app triggers an ad request.
2. An ad request is the signal sent by the publisher to facilitate the placement of an ad through RTB. The ad request would be transmitted to Xandr's platform either directly from Grindr or via MoPub.
3. Through its platform, Xandr would share certain elements in the ad request with third-party segment data providers ("3P Segment Data") in order to enrich the bid request with information about which segment(s) a user belongs to. For example, Xandr could enrich that bid with segment IDs received from buyers.⁴⁴
4. Through its platform, Xandr would share certain elements in the ad request with real-time and context third-party data providers ("Real-time & contextual 3P data") in order to get back contextually relevant data. This could for example be the time or the weather at the user's location.
5. A bid request is a signal sent by an SSP or ad exchange to multiple DSPs, inviting them to bid on the inventory being displayed to a specific user, as described in the ad request. Through Xandr's platform, bid requests would adhere to the OpenRTB Protocol applicable at the time.⁴⁵ This bid request could be enriched with additional contextual and targeting data collected in step 3 and 4. According to the Overview, Xandr would send the bid request to its own DSP and/or other, third-party DSPs.
6. The final step is the auction and response: The DSPs and other demand partners would evaluate the request to determine whether to bid on the ad inventory. The winning bidder's ad is delivered to the digital property.

6.3.1 Xandr's role as an SSP

Xandr has stated that it during the investigation period provided services to help Grindr make its advertising inventory (i.e., space on the Grindr app) available to potential buyers and that Xandr was a SSP in this context.⁴⁶

According to Xandr's Overview, ad requests would be transmitted to the Platform from Grindr, as a "Direct Client". This is also in line with the template IDA. Xandr has stated that for processing outside of that contract, it would not be an SSP.⁴⁷

6.3.2 Xandr's role as a DSP

At the time of investigation, Grindr used MoPub for ad mediation. As stated above, Grindr had integrated the MoPub SDK into its app, and would through the SDK send an ad request to the MoPub server where an ad should be placed in the Grindr app. Subsequently, MoPub would send data to its advertising third parties.⁴⁸ Xandr has also provided that MoPub, during

⁴⁴ Reply to order to provide information 20 December 2024.

⁴⁵ See <https://iabtechlab.com/standards/openrtb/> [last accessed on 19 March 2025].

⁴⁶ Reply to order to provide information 26 May 2023, p. 1.

⁴⁷ As stated by Xandr in meeting 27 February 2025.

⁴⁸ NCC Report p. 127.

the investigation period, had access to controls within the Console.⁴⁹ MoPub's list of partners includes more than 160 demand side platforms and/or mediation partners,⁵⁰ and Xandr was listed as an "Advertising Demand Partner",⁵¹ i.e. DSP. Xandr itself has also confirmed that it acted as a DSP in relation to MoPub.⁵² Thus, in the context of bid requests received through MoPub as a "Third Party SSP", Xandr would be a DSP.

Xandr has stated that its ad buying platform bid to display ads to Norwegian users of the Grindr app, i.e. that Xandr acted as a DSP, both in instances where data was received through MoPub and where data was received directly from Grindr.⁵³

6.4 Processing of ad and bid requests

As a starting point, it should be noted that data processing is the backbone of RTB, enabling advertisers to deliver the right message to the right audience at the right time. Thus, RTB requires collection, accumulation and dissemination of personal data about the data subject in order to, *inter alia*, target and personalize the advertisement and optimize the bid.

Ad and bid requests for ad space on Grindr would have included several categories of data. Although Xandr has not been able to identify or verify the personal data of Grindr users it processed as part of its services to Grindr, Xandr confirms that it "processed data contained in those bid requests to display ads to Norwegian users of the Grindr app" during the investigation period.⁵⁴

In this regard, the technical findings in the mnemonic report confirms that Xandr collected App name as well as the advertising ID and IP address of users from the Grindr app. Xandr also confirmed during the 27 February 2025 meeting that those data were processed as part of handling ad requests and bid requests.

This is consistent with Xandr's Privacy Policy effective at the time of investigation, which stated that Xandr collected, *inter alia*, Android Advertising ID (now Google Advertising ID), IP Address and information about activity in the relevant app from its end users.⁵⁵ It should also be noted that the template IDA also lists, among other things, "IP Address" and "data that could be used for device fingerprinting", as types of personal data comprising the processor data. Furthermore, Grindr stated in response to the complainant's access request that it shared IP address and Google Advertising ID ("if allowed by user") with Xandr.

On a side note, according to its SDK user documentation, MoPub had set up its SDK to pseudonymize/truncate the IP addresses of EU and EEA-based end users, to

⁴⁹ Reply to order to provide information 26 May 2023, p. 2.

⁵⁰ NCC Report p. 129.

⁵¹ Attachment to the complaint, List of MoPub Partners (downloaded 16 December 2019).

⁵² As stated by Xandr in meeting 27 February 2025.

⁵³ Reply to order to provide information 2 October 2023, p. 1.

⁵⁴ *Ibid.*

⁵⁵ NCC Report p. 133, refers to Xandr's Privacy Policy (last updated October 24, 2019).

protect user privacy in compliance with the GDPR.⁵⁶ However, the technical testing showed that the MoPub SDK was transmitting the full IP address to Xandr.⁵⁷

Subsequent to processing an ad request from Grindr on its Platform, Xandr shared bid requests with DSPs to carry out RTB. On this topic, Xandr's Privacy Policy updated 25 May 2018 informed users that:

As such, at the instruction of our clients, we share information with clients and third party providers:

so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you using their data and our and our partners' technology

*so that certain of them can create demographic and interest profiles to help our clients choose the best ad for you using our and our partners' technology (...).*⁵⁸

The Privacy Policy updated 24 October 2019 stated that Xandr may, upon instructions from its clients share data with third-party providers:

(...) so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you using their data and our and our partners' technology

so that certain of them can create demographic and interest profiles to help our clients choose the best ad for you using our and our partners' technology

*so that they can improve their products and services for use by us and others across the broader online advertising ecosystem (...).*⁵⁹

Xandr has also stated that:

*For the limited processing that Xandr is aware it carried out when providing services to Grindr, Xandr's position, consistent with the Xandr Privacy Policy, is that it "share[s] information with advertisers and third-party providers in accordance with the **Digital Property's instructions** so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you using their data and our and our partners' technology" (emphasis added). In this case, Grindr was the Digital Property.*⁶⁰

⁵⁶ MoPub GDPR Publisher Integration Guide, attached to the complaint (downloaded 11 January 2020).

⁵⁷ NCC Report p. 127 and Chapter 7.2.

⁵⁸ Attachment to reply to order to provide information 2 October 2023.

⁵⁹ Attachment to the complaint (downloaded 8 January 2020).

⁶⁰ Reply to order to provide information 26 May 2023, p. 3.

In reply to the NO DPA's order to provide the Digital Property's (in this case Grindr's) instructions as referred to in its reply above, Xandr provided that:

We understand that this request for information relates to the statement in the Xandr Privacy Policy, cited on page 5 of the May 2023 Response, that where Xandr provided services to digital properties like Grindr—i.e., where it acted as a supply-side platform and was a processor on behalf of the digital property—it “share[d] information with advertisers and third-party providers in accordance with the Digital Property's instructions so that they can decide whether to bid on ad inventory or serve an advertisement and choose the best ad for you using their data and our and our partners' technology” (emphasis added).

Clause 9(a) of the IDA—which Xandr provided to the Datatilsynet on 25 August 2023—states that “[b]y using the Services (including as set forth in each Service Agreement and/or your use and configuration of features in the Services) . . .” (emphasis added). As set out in the May 2023 Response, Xandr's Services involved providing Grindr with access to the AppNexus console (“Console”), which is a technology platform that Xandr's clients use to conduct, optimize and track their advertising transactions. As also set out in that Response, Grindr had access to controls within the Console allowing them to select the precise categories of data included in bid requests and the precise recipients of that data, which constituted Grindr's instructions to Xandr.⁶¹

Based on Xandr's explanations during the 27 February 2025 meeting, the NO DPA understands that the “instructions” of Grindr (and MoPub) is comprised of the settings within the Console on the platform, allowing them to exclude certain categories of data from bid requests or to exclude certain recipients from receiving those bid requests. Xandr clarified in the meeting that this option to deselect elements would enable blocking elements from being sent within the bid request (e.g. “don't use location”) or exclude specific DSPs or categories (e.g. “no porn” or “no ads from DSP XYZ”). Thus, bid requests would not be shared to third parties on the demand side if they were blacklisted by Grindr.

Further, it is the NO DPA's understanding that Xandr relied on the OpenRTB 2.4⁶² as the primary protocol for RTB during the time of investigation. Open RTB 2.4 provides an open industry standard for communication between buyers of advertising space and sellers of publisher inventory.⁶³ RTB transactions are initiated when a supply source (such as an SSP or ad exchange) sends a bid request to a bidder.

According to the OpenRTB 2.4 Protocol, fields in the bid request could either be “required”, “recommended” or “optional”:

⁶¹ Reply to additional order to provide information 20 December 2024, pp. 3-4.

⁶² OpenRTB Spec v. 2.4, released March 2016, was the dominant standard in the programmatic advertising ecosystem during this time.

⁶³ OpenRTB Spec v.2.4 p. 2, <https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-4-FINAL.pdf> [last accessed: 19 March 2025].

- “Required”: Not many objects in the standard are “required”, but the required fields entail that their omission would technically break the protocol.
- There are multiple “recommended” attributes. These do not apply in all situations (e.g. apply only when a device cannot receive video), but when they do, the creator of the bid request should include them: “A minimal viable interface should include the required and recommended parameters, but the scope for these parameters may be limited to specific scenarios”⁶⁴.
- “Optional”: These attributes should be included “to ensure maximum value is delivered by the parties”.⁶⁵

According to the protocol, information about “app”, “device” and “user” are recommended attributes to be included, to ensure a minimal viable interface.⁶⁶ Information about “app” is defined as “Details of the application calling for the impression”. Information about “device” is defined as “Details of the device on which the content and impressions are displayed”. Information about “user” is defined as “Human user of the device; audience for advertising”.⁶⁷

In order to enable advertisers, their DSPs and Xandr’s own DSP service to feasibly evaluate and bid on an ad impression, specific attributes about the user, device and app in which the ad is to be displayed, would have to be shared. Without sharing such data, DSPs cannot determine whether a given impression matches their targeting criteria, making the ad exchange’s facilitation of bidding ineffective and bid requests unsuccessful.

Xandr has contested that this is “a logical precondition for RTB to function”,⁶⁸ asserting that such conditions are merely recommended and not technically necessary for the RTB to function.⁶⁹ Xandr has argued that because Xandr no longer has information about the types of personal data it processed in the course of providing services to Grindr, the NO DPA should have assumed that Xandr did not process these data points.⁷⁰ Although the NO DPA agrees that these attributes are not strictly technically required, the NO DPA maintains they are integral to making the services profitable. In the NO DPA’s understanding such processing was standard procedure for such business models at the time.⁷¹

Furthermore, in the 27 February 2025 meeting, Xandr confirmed that information such as the IP-address and advertising ID of the data subject as well as the app URL would be shared with third-party DSPs. Xandr has however altered its position on this point, stating that

⁶⁴ OpenRTB Spec v.2.4 p. 1, <https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-4-FINAL.pdf> [last accessed: 19 March 2025].

⁶⁵ *Ibid.*, p. 1.

⁶⁶ *Ibid.*, pp. 1 and 9.

⁶⁷ *Ibid.*, pp. 1 and 9.

⁶⁸ Advance notification of April 3 2025, p. 23.

⁶⁹ Response to the advance notification 2 June 2025 p. 4.

⁷⁰ Response to the advance notification 2 June 2025 p. 4.

⁷¹ NCC Report pp. 34-39

although this might be correct in relation their services in general,⁷² they do not have any evidence that it shared personal data relating to Norwegian Grindr users with third parties.⁷³

In the NO DPA's opinion, Xandr should be in a position to verify the nature of personal data it processed in the course of providing services to Grindr or how the specific data was processed, since Xandr knew the NO DPA started investigating the business relationship with Grindr from 21 February 2020.

Moreover, the NO DPA's investigation into Grindr uncovered that Grindr shared information about the user, device and app with its advertising partners to facilitate personalised advertising and maximise profits from its ad inventory. Xandr has not made any credible representations to suggest any reason why this information would suddenly not be processed during ad and bid requests where Xandr was involved, or why any of the parties involved would deviate from common industry practices in those instances. The NO DPA therefore finds it far more likely than not that these data were processed during ad and bid requests.

6.5 Personal data

The app name, app ID or app URL in a given ad and bid request would disclose what app an individual is using. If that individual is identifiable, directly or indirectly, these data elements would constitute personal data related to them.

As explained above, Xandr was processing online identifiers such as advertising ID and IP addresses. Online identifiers are explicitly mentioned as an example of information that can make a natural person identifiable in Article 4(1) GDPR.

Moreover, Recital 30 GDPR further elaborates on online identifiers as follows:

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.

⁷² Which personal data Xandr processed in the investigation period is described in their privacy policy, including what information it shared with third parties, updated May 24 2018: "Where permitted, we provide clients and third-party providers access to their Platform Data that they collect, acquire, or use on the Platform, and typically they may remove it from the Platform for their own use. For a current list of third-party providers who may, subject to our clients' permission, receive your data, see here. AppNexus may also provide Platform Data to partners and service providers for the purpose of operating, managing, maintaining, or enhancing our services, including for the safety and security of the Platform and the online industry, or as required by law. AppNexus does not share the information collected on the Platform with other third parties, unless legally required."

⁷³ Response to the advance notification 2 June 2025 p. 4.

The information transmitted to Xandr from Grindr, including the fact that a given individual was using Grindr, therefore constitute “personal data” pursuant to Article 4(1) GDPR, as it is information relating to a natural person who can be identified indirectly by reference to the aforementioned online identifiers. This is also supported by the conclusion reached by Personvernneemnda (The Privacy Appeals Board),⁷⁴ the Oslo District Court and the Borgarting Court of Appeal in the aforementioned Grindr case.⁷⁵

Based on the above, the NO DPA finds it proven by a clear preponderance of probability (in Norwegian: *klar sannsynlighetsovervekt*) that Xandr processed (including by way of sharing) at least the following personal data about Grindr users (both to the extent data was collected through MoPub, and where data was collected directly from Grindr): **The fact that they were using Grindr, advertising ID and IP Address.**

6.6 Controllershship

As the NO DPA has established that Xandr processed personal data related to Norwegian Grindr users, the next question to be assessed is whether Xandr can be considered a controller in relation to that processing, including the sharing of personal data of Grindr users, during the time of investigation.

The European Data Protection Board (“EDPB”) Guidelines 07/2020 on the concepts of controller and processor in the GDPR state that the concepts of controller and processor are functional.⁷⁶ A controller decides key elements about processing, and makes decisions as to both the purposes and means, i.e. “why the processing is taking place (i.e., ‘to what end’; or ‘what for’) and how this objective shall be reached.”⁷⁷

Furthermore, the EDPB elaborates that while certain decisions on the means may be left to the discretion of the processor, decisions on essential means are reserved to the controller. The Guidelines provide that:

*“Essential means” are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed (“which data shall be processed?”), the duration of the processing (“for how long shall they be processed?”), the categories of recipients (“who shall have access to them?”) and the categories of data subjects (“whose personal data are being processed?”).*⁷⁸

Pursuant to Article 26(1) GDPR, decisions may be taken jointly by two or more controllers, in which case they are joint controllers. The EDPB Guidelines explain that the overarching criterion is whether there is “joint participation of two or more entities in the determination of

⁷⁴ PVN-2020-12, PVN-2022-22.

⁷⁵ 23-160384TVI-TOSL/04 pp. 10-11 and 24-154313ASD-BORG/02 pp. 15-19.

⁷⁶ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 12.

⁷⁷ *Ibid.*, para. 35.

⁷⁸ *Ibid.*, para. 40.

the purposes and means of a processing”, but that that this may take several forms, for example by way of a common decision or converging decisions.⁷⁹

The EDPB Guidelines describe converging decisions as follows:

The situation of joint participation through converging decisions results more particularly from the case law of the CJEU on the concept of joint controllers. Decisions can be considered as converging on purposes and means if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. (...) [A]n important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties’ participation in the purposes and means in the sense that the processing by each party is inseparable, i.e. inextricably linked.⁸⁰

6.6.1 Xandr as a DSP

In its submission dated 2 October 2023, Xandr confirmed that it acted as a joint controller with Grindr when Xandr’s own ad buying platform placed bids to display ads to Norwegian users of the Grindr app. It processed any personal data contained in bid requests for purposes related to bidding on inventory:

Bidding on inventory. This entailed identifying whether the device visiting the Grindr service through the Grindr app was assigned to any interest segments that Xandr made available to advertiser clients for them to bid on;

Delivering ads to the device on the Grindr app. If a Xandr bid succeeded in purchasing ad space on the Grindr app, Xandr would process the device’s pseudonymous identifiers, including advertising ID and IP address to deliver the appropriate ad.⁸¹

Furthermore, Xandr stated that it may have processed personal data for the following purposes:

Creating measurement and attribution reporting on ads delivered. Xandr would process data about user interactions with ads it delivered, and potentially subsequent interactions with advertisers’ websites and apps, to create aggregate reporting for advertiser customers; and

Frequency and recency capping. This entailed processing device identifiers to ensure that the same ad or ad campaign would not be shown more than a certain number of times on that device for a given time period.⁸²

⁷⁹ *Ibid.*, para. 53-54.

⁸⁰ *Ibid.*, para. 55.

⁸¹ Reply to order to provide information 2 October 2023.

⁸² Reply to order to provide information 2 October 2023.

In Xandr's submission of 2 June 2025, it says: "When creating ad campaigns, Ad Buyers would select a "segment" for a particular campaign. Ad Buyers could upload their own segments to Xandr's services, or they could choose to target segments that Xandr made available. In all cases, however, Xandr did not create the segments it made available; instead, it obtained them from third-party providers. Xandr therefore had no role in determining the circumstances in which a device would be added to a segment. Ad Buyers selected which segments they wished to target, which ad they wished to target to those segments, and how much they wished to bid to display ads to those segments."⁸³

The NO DPA does not agree that Xandr had no role in this. Ad buyers could select segments from a standard that Xandr made available for them to choose from, thereby Xandr did influence the processing.

It is therefore clear that Xandr operated in the role as joint controller for the processing of personal data described in Section 6.3.2 when acting as a DSP.

6.6.2 Xandr as an SSP

Apart from instances where its own ad buying platform placed bids to display ads, Xandr has taken the position that it was partly a controller and partly a processor when processing ad and bid requests originating from Grindr. Xandr states that it was operating as controller when processing personal data:

- *for frequency and time capping (that is, to ensure that the same adverts are not shown repeatedly to the same end user, or at times that the advertiser does not want);*
- *to ensure the security of services;*
- *to detect invalid inventory and fraud; and*
- *to improve the overall platform.*⁸⁴

Concerning the last point, Xandr explained in its 16 July 2020 submission that "personal data is also processed in the course of training Xandr's ad delivery and bidding algorithms in order to improve overall platform optimization."⁸⁵ However, Xandr claims in its response to the advance notification that "there is no evidence in the record that Xandr processed Norwegian Grindr users' personal data for this purpose, and in any event, it did not process personal data of European users for these purposes during the Investigation Period." Xandr says it [REDACTED]

[REDACTED]—for this purpose, and that it did not use [REDACTED]⁸⁶ Xandr's response to the advance notification seems to be in direct contradiction to what Xandr stated in the beginning of the investigation on this issue. In any case Xandr's claim in their response to the advance notification does not change the NO DPA's conclusion that Xandr was operating as a

⁸³ Response to the advance notification 2 June 2025 p. 6

⁸⁴ Reply to order to provide information 26 May 2023.

⁸⁵ Reply to order to provide information 16 July 2020 – Cross-Border Processing, p. 2.

⁸⁶ Response to the advance notification 2 June 2025 p. 3.

controller in regards to ad delivery and bidding. In Xandr's response to the advance notification it says:

Xandr's information indicates that Grindr did not share bid requests relating to Norwegian users of the app with Xandr's SSP—either directly or via Twitter's MoPub—in certain months during the Investigation Period.⁸⁷

The NO DPA reads this as Xandr confirming Grindr did share bid requests in certain months with Xandr's SSP, in regard to Xandr's response of 16 July 2020 where it describes that Xandr is a controller in relation to ad delivery and bid requests.⁸⁸ It is reasonable to state that Xandr acted as a controller for their own purposes when processing personal data obtained from Grindr as every other customer in general, such as training Xandr's ad delivery and bidding algorithm in order to improve the overall platform.⁸⁹

Apart from this, Xandr maintains that it was operating as a processor:

In this instance, the facts suggest that Xandr acted as a processor of Grindr data for the limited processing operations described above. In particular, where Grindr shared data with Xandr to sell ad space (either directly or through Twitter's MoPub), Grindr would typically determine the purposes of that processing (i.e., deciding to share data with third parties with the ultimate aim of displaying ads on its app, or to display specific ads without sharing data with third parties) and the essential means (including the categories of data processed and the recipients of the data). During the investigation period, Grindr (and MoPub) had access to controls allowing them to select the precise categories of data included in ad calls and the precise recipients of data. Xandr would not have had any role in those decisions.⁹⁰

As far as Grindr is concerned, it has asserted that “Grindr and Xandr [did] not have a controller-processor relationship as regards the personal data in question.”⁹¹

The question to be assessed is which entity or entities that made decisions regarding the purpose of processing and essential means, recalling that the realities and not the formalities will be decisive.

The NO DPA reiterates that Xandr is an advertiser technology company, providing “a data-enabled technology platform with tools that help power a diverse ecosystem connecting marketers and media owners through first-party, data-led advertising solutions across its

⁸⁷ Response to the advance notification 2 June 2025 p. 6.

⁸⁸ Reply to order to provide information 16 July 2020 – Cross-Border Processing p. 2

⁸⁹ See section 6.4 in this decision, pp. 20-24.

⁹⁰ Reply to order to provide information 26 May 2023, p. 2.

⁹¹ Grindr's response to the NO DPA's order to provide information dated 2 June 2021, in the NO DPA's case 20/02254. In Xandr's response to the advance notification 2 June 2025 p. 3: “Grindr's assertion was apparently based on its belief that it did not have any direct relationship with Xandr, but this is inconsistent with Xandr's submissions in this case.” Grindr's assertion is not decisive for the NO DPA's conclusion. The concepts of controller and processor are functional according to EDPB's Guidelines 07/2020, p.3.

network.”⁹²As explained above, Xandr could offer services as both an SSP, a DSP, and as an ad exchange. It is evident that Xandr offered a suite of services in order to pursue its own objective of being a facilitator of data-driven exchanges between publishers and advertisers on its multi-sided platform – a platform on which Xandr would define the infrastructure and constraints for exchanges. The success of the platform would depend on there being a sufficient number of participants on both the supply and demand side, as well as on Xandr’s ability to offer ‘precise marketing’, in order to maximize value for advertisers and publishers.⁹³ In this regard, the NO DPA notes for example that Xandr had measures in place to enrich the ad requests from digital properties before disseminating the corresponding bid requests – both the enrichment and dissemination being equally in Xandr’s interest as in Grindr’s. Xandr’s use of data from its clients to improve the platform fits logically into this picture.

Xandr has consistently maintained that Grindr (and MoPub) had access to Xandr’s Console in which they could instruct Xandr about the categories of data contained in bid requests as well as the recipients of such bid requests. As explained above in Section 6.4, this entailed that Grindr could block certain data points from being used for RTB as well as blacklist particular DSPs or advertisers. At the same time, the NO SA understands that it was Xandr that provided the framework for exercising such choice, including which DSPs and advertisers Grindr was able to interact with (and potentially blacklist).⁹⁴ Where Grindr did not tweak the settings in the Console, the bid request would be circulated according to the standards selected by Xandr to the recipients that Xandr had partnered up with to include on its platform.

In CJEU case C-604/22 (IAB Europe) the Court finds that:

*Participation in the determination of the purposes and means of processing can take different forms, since such participation can result from a common decision taken by two or more entities or from converging decisions of those entities. Where the latter is the case, those decisions must complement each other in such a manner that they each have a tangible impact on the determination of the purposes and means of the processing.*⁹⁵

In the NO DPA’s opinion Xandr had tangible impact on the determination of the purposes and means of the processing by providing the framework and presenting the Console with the standard selected by Xandr.

⁹² <https://about.ads.microsoft.com/en-us/blog/post/december-2021/microsoft-to-acquire-xandr-to-accelerate-its-digital-advertising-and-retail-media-solutions> [last accessed 19 March 2025].

⁹³ According to AT&T in 2019, “Advertisers are interested in capitalizing on our (...) ability to offer more precise marketing to customers through a digital platform.”, see <https://www.sec.gov/Archives/edgar/data/732717/000156276220000064/t-20191231.htm> p. 4 [last accessed 19 March 2025].

⁹⁴ As stated by Xandr in meeting 27 February 2025.

⁹⁵ CJEU Judgement in Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, para. 59.

Xandr has stated that it expressly prohibited Grindr from sharing special category data in clause 6.1 of its standard Master Service Agreement.⁹⁶ Such an agreement does however entail that Xandr did instruct Grindr on the categories of data shared with it, and as such, the NO DPA does not agree that Xandr had no say in what categories of data were contained in bid requests.

As noted by the EDPB when outlining instances of joint controllership,

This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up. (...)

Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities.⁹⁷

In this regard it should be recalled that, as noted by the Advocate General in the *Wirtschaftsakademie* case regarding joint controllership, it is not necessary for a controller

to have complete control over all aspects of data processing. (...) Consequently, any interpretation which focusses on the existence of complete control over all aspects of data processing is likely to result in serious lacunae in the protection of personal data.⁹⁸

The Court of Justice of the European Union (“CJEU”) confirmed the Advocate General’s finding in the case that there was joint controllership between a social media fan page administrator, setting the parameters for the fan page, and the social media operator.⁹⁹

Additionally, the CJEU opined that the concept of ‘controller’ is defined broadly in order to ensure effective and complete protection of the data subjects.¹⁰⁰

This is a key consideration in the present case. The AdTech industry is particularly opaque and consists of a large number of companies exchanging personal data about troves of data subjects along complex value chains. In this ecosystem, one company alone is unlikely to fully control how data is processed; rather, some control is exercised by each of the numerous actors in the RTB process. If those companies would not be held responsible and accountable for their processing of personal data, it would lead to a diffusion or even elimination of

⁹⁶ Reply to order to provide information 2 October 2023, p. 5 and Response to the advance notification of 2 June 2025 p. 14.

⁹⁷ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 65-67.

⁹⁸ Opinion of Advocate General in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, para. 62.

⁹⁹ CJEU Judgement in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, para. 44.

¹⁰⁰ CJEU Judgement in Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, para. 28.

responsibility, rendering the data subject's rights illusory. In that respect the NO DPA emphasizes that the aim of the GDPR is "ensuring a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data."¹⁰¹

This is particularly obvious in the present case, where Grindr does not agree that Xandr acted as its processor. This means that it would not in practice be possible for data subjects to exercise their GDPR rights in relation to personal data processed by Xandr vis-à-vis Grindr. Since Xandr considers itself a processor for many of the processing activities taking place, it would also not be possible for them to exercise their rights vis-à-vis Xandr for those processing activities, as Xandr would then need to forward any data subject rights requests to Grindr, which again did not accept controllership. The result would be that data subjects' rights would be entirely undermined.

Xandr has contested this stating that the NO DPA has overlooked Exhibit E, Clause 5(a) and (d)(iii) of the International Data Agreement, stipulating the handling of data subject requests.¹⁰² The NO DPA has taken note of the agreement. The NO DPA does, however, also note that there has been no demonstration that such handling of data subject requests actually took place.

As the practical functioning of the agreement in relation to data subject rights was based on a disputed premise, namely that Grindr was the controller and Xandr was the processor for the personal data in question, it would in any event not have been possible for data subject rights to have been fulfilled in accordance with the GDPR. This is because neither Grindr nor Xandr considered itself as a controller for the processing in question.

As pointed out by the EDPB, the notions of controllers and processor are functional concepts, and being formally designated as a controller or a processor in a contract is not decisive. A formal agreement therefore cannot solve a situation where no entity accepts controllership in practice.¹⁰³

The No DPA's interpretation is confirmed in CJEU case C-604/22 (IAB Europe). The CJEU finds that the objective of GDPR article 4(7) "is to ensure, through that broad definition of the concept of 'controller', effective and complete protection of data subjects"¹⁰⁴

IAB Europe is a sectorial organization that has established a voluntary framework of rules relating to consent management in the context of RTB, namely the Transparency & Consent Framework (TCF). The CJEU concluded that IAB Europe, by devising such a framework "which contains not only binding technical rules but also rules setting out in detail the arrangements for storing and disseminating personal data relating to such consent, must be classified as a 'joint controller' ..., jointly with its members."¹⁰⁵

¹⁰¹ CJEU Judgement in Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, para. 53.

¹⁰² Response to the advance notification of 2 June 2025 pp. 10-11.

¹⁰³ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 12.

¹⁰⁴ CJEU Judgement in Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, para 55.

¹⁰⁵ CJEU Judgement in Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, para 77.

The CJEU states:

In that regard, although each joint controller must independently meet the definition of ‘controller’ which is set out in Article 4(7) of the GDPR, the existence of joint controllership does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed in the light of all the relevant circumstances of the particular case. In addition, the joint controllership of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned.¹⁰⁶

On this basis, it is clear that both Grindr as well as Xandr were pursuing their respective interests and purposes in processing the personal data, and they both exercised decisive influence on the essential means for the processing. The processing in question could clearly not have taken place without both parties’ participation in deciding the purposes and means.

The NO DPA’s conclusion is therefore that Xandr was a joint controller with Grindr for its processing of personal data contained in ad and bid requests, also when Xandr was acting as an SSP.

In sum, the NO DPA finds it proven by a clear preponderance of probability that Xandr was a joint controller in respect of the processing of personal data, both in its role as SSP and DSP, during the investigation period.

6.7 Accountability

As the NO DPA’s assessment shows, Xandr is a joint controller with Grindr. In this regard, it should be noted that “joint responsibility does not necessarily imply equal responsibility”, and that “the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.”¹⁰⁷

Pursuant to Article 26(1) GDPR, joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR. However, this does not absolve any of the parties of their duties under the GDPR. Rather, the point is to distribute tasks – in the words of the EDPB, “joint controllers need to set ‘who does what’”.¹⁰⁸ Furthermore, the EDPB notes that joint controllers “can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing”.¹⁰⁹

¹⁰⁶ CJEU Judgement in Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, para 58.

¹⁰⁷ CJEU Judgement in Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, para. 43.

¹⁰⁸ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 162.

¹⁰⁹ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 168.

As noted by the EDPB:

*In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing.*¹¹⁰

The accountability principle contained in Article 5(2) GDPR as well as the obligations under Article 24 GDPR apply to both controllers. They are both responsible for ensuring and demonstrating that processing is performed in accordance with the GDPR. For example, where one controller is tasked with requesting consent from data subjects, both controllers remain responsible for ensuring that such consent provides a valid and appropriate basis for their processing. Compliance can never be outsourced.

6.8 Special categories of data

Having established Xandr's role and responsibilities, the next question is whether Xandr processed special categories of data when processing the app name, advertising ID and IP address of Grindr users, and if so, whether such processing was in line with the GDPR.

Article 9(1) GDPR prohibits processing of personal data "concerning a natural person's sex life or sexual orientation", but this prohibition does not apply if one of the exemptions in Article 9(2) applies to the processing.

Consequently, in order to lawfully process special categories of data, the controller must fulfil one of the exemptions in Article 9(2), in addition to having a valid legal basis pursuant to Article 6(1).

6.8.1 Whether the processing falls within the scope of Article 9

As a starting point, the NO DPA will reiterate the conclusion in the case against Grindr, since it is relevant in the present case:

*The NO DPA finds that Grindr processed data "concerning" a natural person's "sexual orientation" pursuant to Article 9(1) by sharing personal data on a specific user alongside app name or app ID to advertising partners.*¹¹¹

Data revealing the fact that someone is a Grindr user strongly indicates that they belong to a sexual minority, and that data concerning a person's sexual orientation constitutes special category data under the GDPR.¹¹²

¹¹⁰ EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, para. 167.

¹¹¹ NO DPA decision in the case against Grindr, 13 December 2021, p. 44.

¹¹² For more information on the assessment of Article 9 in the Grindr-case, see the NO DPA's decision in the case against Grindr, Section 5.5.1.

This assessment was later upheld by the Norwegian Privacy Appeals Board,¹¹³ the Oslo District Court¹¹⁴ and the Court of Appeal.¹¹⁵ The Oslo District Court found that, by providing the App ID, Grindr shared with the advertisers that the origin of the information came from Grindr - meaning that the information came from a registered user of Grindr, and that information about a person being a registered user of Grindr is to be considered as information about someone's sexual orientation.¹¹⁶ This was confirmed by the Court of Appeal.¹¹⁷

It should be noted that the NO DPA's conclusion in the Grindr case is fully in line with the jurisprudence of the CJEU. The CJEU has ruled that the notion of special category data should be interpreted broadly and encompass personal data that are liable to indirectly reveal sensitive information, for example as concerns visits to apps that relate to one of the categories listed in Article 9(1). This is the case regardless of whether the information revealed is correct.¹¹⁸

In light of the findings in the Grindr case, compared to the NO DPA's assessment and conclusion above, i.e., that Xandr processed App name/ID/URL, IP address and advertising ID about Grindr users, the NO DPA does not deem it necessary to go into further detail on this issue. The NO DPA finds it proven by at least a clear preponderance of probability that Xandr processed data "concerning" a natural person's "sexual orientation" pursuant to Article 9(1) by processing Grindr users' advertising ID and IP address alongside app name/ID/URL to advertising partners.

In its reply to the NO DPA, Xandr states that it was not aware of regulatory guidance that stated (and certainly it was not market practice to consider) that the mere fact that an individual was a user of Grindr or similar apps could in itself constitute special category data under Article 9(1) GDPR. It submitted that the question of what data constitutes special category data was so unclear that it has been the subject of CJEU cases, all of which were decided after the end of the investigation period.¹¹⁹ In this regard, the NO DPA notes that Xandr's narrow interpretation of Article 9 appears to have no support in legal sources. On the contrary, the CJEU has confirmed that Article 9 stipulates a broad definition in relation to other special category data under Directive 95/46/EC.¹²⁰ Furthermore, as stated in the CJEU judgement in Case C-184/20 (OT), "a wide interpretation of the terms 'special categories of personal data' and 'sensitive data' is confirmed by the objective of Directive 95/46 and the GDPR (...) which is to ensure a high level of protection of the fundamental rights and

¹¹³ PVN-2022-22, pp. 12-14.

¹¹⁴ 23-160384TVI-TOSL/04, p. 17.

¹¹⁵ 24-154313ASD-BORG/02, pp. 15-19.

¹¹⁶ 23-160384TVI-TOSL/04, pp. 14 and 17.

¹¹⁷ 24-154313ASD-BORG/02, pp 18-19.

¹¹⁸ CJEU Judgement in Case C-184/20, OT v Vyriausioji tarnybinės etikos komisija; Judgement in Case C-252/21, Meta Platforms Inc. and Others v Bundeskartellamt; Judgement in Case C-21/23, ND v DR (Lindenapotheke).

¹¹⁹ Reply to order to provide information 2 October 2023.

¹²⁰ CJEU Judgement in Case C-101/01, Lindqvist, para. 50-51.

freedoms of natural persons, in particular of their private life with respect to the processing of personal data concerning them”.¹²¹

In any case, CJEU judgements apply retroactively (*ex tunc*).¹²²

6.8.2 Whether the processing falls within the exceptions in Article 9(2)

Article 9(2)(e) GDPR provides that special category data can be processed where the personal data “are manifestly made public by the data subject”.

In the Grindr case, the NO DPA concluded that the fact that the data subjects were Grindr users were not “manifestly made public” by the data subjects, cf. Article 9(2)(e).¹²³

Both the reasoning and conclusion in the Grindr case is applicable in the present case, since it relates to the same data subjects and functionalities in the Grindr app. Thus, the NO DPA will rely on the same conclusion here. Therefore, the fact that the data subjects were Grindr users were not “manifestly made public” by the data subjects pursuant to Article 9(2)(e).

The only other possible exception in the present case is Article 9(2)(a) GDPR. Article 9(2)(a) provides that special category data can be processed where the data subject has given “explicit consent” to the processing of those personal data for one or more specified purposes.

Article 4(11) of the GDPR defines consent as: “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.”

It is stated in the EDPB Guidelines 05/2020 on consent that:

*When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful.*¹²⁴

It is undisputed that Xandr never obtained any consent directly from the data subjects (here: the Norwegian Grindr users) before or during the processing in question. Instead, Xandr relied

¹²¹ CJEU Judgement in Case C-184/20, OT v Vyriausioji tarnybinės etikos komisija, para. 125.

¹²² CJEU Judgement in Case C-73/08, Nicolas Bressol and Others, Céline Chaverot and Others v Gouvernement de la Communauté française, para. 90.

¹²³ For the full reasoning see pp. 45-48 in the NO DPA decision against Grindr, 13 December 2021.

¹²⁴ EDPB Guidelines 05/2020 on consent under Regulation 2016/679, para. 3.

on Grindr to assess whether consent was required and contractually obliged them to obtain valid consent if applicable.¹²⁵

The NO DPA however found that Grindr failed to fulfil the requirements of “freely given”, “specific”, “informed”, “unambiguous” and “as easy to withdraw as to give consent”, pursuant to Article 4(11) and Article 7, when collecting consents in their previous Consent Management Platform (“CMP”). Consents collected in the previous CMP for the disclosure of personal data to advertising partners for advertising purposes were therefore not valid.

The conclusion that Grindr’s consents were not valid was later upheld by the Norwegian Privacy Appeals Board,¹²⁶ Oslo District Court¹²⁷ and the Court of Appeal.¹²⁸

Furthermore, and as explained above, each controller operating jointly must have a valid legal basis for its processing (both under Article 6 and 9). Grindr’s responsibility for the collection of consent from its users for the processing in question, does not except Xandr from its accountability obligations under Article 5(2) and 24 GDPR to ensure and demonstrate compliance, nor from its duty pursuant to Article 7(1) GDPR to be able to document that the data subject had given their consent. In other words, while it is possible (and sometimes necessary) to contractually agree that one controller collects consent on behalf of another controller, this only applies if both controllers ensure that consent meets all requirements in Article 4(11) and Article 7 GDPR, including that it is properly documented and covers the specific processing activities of both of them. This is not the case here, since the consents Grindr collected were not valid. Additionally, Xandr did not take any measures, in order to discharge of its accountability obligations, to verify that consent was valid and that it covered its processing activities.

Xandr argues that it expressly prohibited Grindr from sharing special category data in clause 6.1 of its standard Master Services Agreement. The NO DPA holds that such a formality in the form of a contractual commitment between controllers does not relieve Xandr of its responsibility, when it *de facto* processed sensitive personal data pursuant to Article 9. This is also in line with the principle of accountability as explained above. In addition, the CJEU has confirmed that it is not relevant whether the controller is acting with the aim of obtaining information that falls within one of the categories referred to in Article 9(1) GDPR.¹²⁹ This is justified by the significant risks to their fundamental rights and freedoms that data subjects inherently face if such sensitive data is processed.

¹²⁵ Xandr had a similar contractual clause with MoPub, where Clause 1 of the DPA that Xandr had in place with MoPub, expressly obliged both parties to “comply with the obligations applicable to it under Applicable Data Protection Law with respect to the processing of MoPub European Data”. Xandr argues that, as a result of the fact that MoPub’s role under this DPA was to collect and provide any personal data contained in bid requests that it shared with Xandr, MoPub thereby committed itself to ensuring there was a valid legal basis for all processing of such data.

¹²⁶ PVN-2022-22.

¹²⁷ 23-160384TVI-TOSL/04, p. 26.

¹²⁸ 24-154313ASD-BORG/02, p. 26.

¹²⁹ CJEU Judgement in Case C-252/21, Meta Platforms Inc. and Others v Bundeskartellamt, para. 69 (and 73).

In conclusion, Xandr's processing activities did not meet any of the exceptions in Article 9(2). Consequently, the NO SA finds it proven by at least a clear preponderance of probability that Xandr breached the prohibition in Article 9(1) when processing personal data of Norwegian Grindr users.

6.9 Legal basis

Processing of personal data is only lawful if the controller has a valid legal basis pursuant to Article 6(1) GDPR.

Xandr did not answer the following question regarding the use of Article 6(1)(f) as a legal basis in the NO DPA's order to provide information¹³⁰:

Please demonstrate under which legal basis or bases you processed the personal data of Grindr users in relation to the processing referenced in question 2–5. If processing was based on different legal bases, please indicate which processing was based on which legal basis:

i. In case the legal basis is Article 6(1)(f) GDPR, please demonstrate which legitimate interests as well as which interests or fundamental rights and freedoms of the data subjects you have taken into account before the processing, and how you have assessed the balancing of these elements.

Instead, Xandr answered the question related to Article 6(1)(a) and referred to the Privacy Policy available at the time, which stated, *inter alia*, that “[w]e normally rely on legitimate interests to collect and use personal data” and “[in] some cases, we may rely on your consent which is obtained for us by the operator of the Digital Properties that use our technology or use technology that interacts with our Platform”.

Xandr has not in plain text confirmed to the NO DPA which legal basis it relied on when processing the personal data of Grindr users. The NO DPA finds the descriptions in the Privacy Policy too vague to provide sufficient information as to the legal basis for the specific processing operation in question. Although Xandr has been somewhat ambiguous in its submissions concerning the question on legal basis, the facts point towards the use of Article 6(1)(a) as the legal basis on which Xandr based its processing on.

In any case, since the personal data in question qualify as special category data pursuant to Article 9(1), consent would be the only applicable legal basis under Article 6(1).

As established above, the consents collected were not valid, and Xandr remains accountable for this.

¹³⁰ As put forth in the order to provide information 6 February 2023.

The NO DPA therefore finds it proven by at least a clear preponderance of probability that Xandr processed personal data of Grindr users without a valid legal basis in Article 6(1) GDPR.

7 Imposition of an administrative fine

7.1 Introduction

The NO DPA can impose administrative fines for infringements of the GDPR according to Article 58(2)(i), cf. Article 83 GDPR. An administrative fine is deemed to be a criminal penalty pursuant to the European Convention on Human Rights (ECHR).¹³¹

In order to impose a fine, there has to be clear preponderance of probability of infringements of the GDPR. An administrative fine can only be imposed where a controller has intentionally or negligently infringed the GDPR.¹³²

As established in Sections 6.8 and 6.9 above, the NO DPA has found that there is clear preponderance of probability that Xandr has breached Articles 6(1) and 9(1) GDPR.

Moreover, the NO DPA concludes that there is a clear preponderance of probability that the requirement of culpability is met in this case, as further elaborated in Section 7.2.2 below.

The assessment of whether to impose an administrative fine, as well as the amount of the fine, depends on an overall assessment of several elements, pursuant to Article 83 GDPR. Similar elements can be found in Section 46 of the Norwegian Public Administration Act.

The NO DPA has found that the imposition of an administrative fine is warranted in this case. In the following, the NO DPA explain the rationale for imposing a fine, as well as the basis for determining its amount.

7.2 Whether to impose an administrative fine

Pursuant to Article 83(1), administrative fines “shall in each individual case be effective, proportionate and dissuasive”.

When deciding whether to impose an administrative fine, the supervisory authority must take the factors listed in Article 83(2)(a)–(k) GDPR into consideration in each individual case. In the following, the NO DPA will assess the case facts against these factors.

A purpose of the GDPR is to ensure a consistent and homogenous application of the GDPR

¹³¹ Section 43 of the Norwegian Public Administration Act, LOV-1967-02-10. See also e.g. HR-2014-01296-A para. 47.

¹³² See C-807/21, *Deutsche Wohnen SE v Staatsanwaltschaft Berlin*, in para. 78 with reference to Article 83 GDPR. See also Section 46 of the Norwegian Public Administration Act.

and a high level of data protection throughout all of the Member States, including the application of administrative fines.¹³³

For the purpose of achieving a consistent approach to the imposition of the administrative fines, the Article 29 Working Party adopted guidelines concerning the application of the criteria in Article 83(2) GDPR in 2017 (the “Administrative Fines Guidelines”), which the EDPB endorsed in 2018.¹³⁴ Article 70(1)(k) specifically lists that for the purpose of ensuring a consistent application of the GDPR, the EDPB shall draw up guidelines for supervisory authorities concerning the setting of administrative fines pursuant to Article 83.

The Administrative Fines Guidelines state that:

Like all corrective measures in general, administrative fines should adequately respond to the nature, gravity and consequences of the breach, and supervisory authorities must assess all the facts of the case in a manner that is consistent and objectively justified. The assessment of what is effective, proportional and dissuasive in each case will have to also reflect the objective pursued by the corrective measure chosen, that is either to reestablish compliance with the rules, or to punish unlawful behavior (or both).¹³⁵

The EDPB has adopted Guidelines 4/2022 on the calculation of administrative fines under the GDPR that complement the previously adopted guidelines.¹³⁶ These guidelines aim to harmonize the methodology the supervisory authorities use when calculating the amount of administrative fines pursuant to Article 83 GDPR.¹³⁷

The following sub-sections outline how the NO DPA has given “due regard” to the criteria in Article 83(2) GDPR and in regard with the methodology in the EDPB guidelines.¹³⁸

7.2.1 (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

Xandr has breached Articles 6(1) and 9(1) GDPR, which are basic requirements for processing personal data pursuant to the GDPR. The requirements they prescribe must be fulfilled for processing to even take place. Hence, the violation in this case is of fundamental nature going to the core of data protection rights of individuals.

¹³³ GDPR Recitals 10 and 150.

¹³⁴ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018.

¹³⁵ *Ibid*, p. 6.

¹³⁶ EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1.

¹³⁷ In 24-154313ASD-BORG/02, it says in unofficial translation: “*The Court of Appeal finds that the method for determining the administrative fine set out in the guidelines, as well as calculating the amount of the fine, should be given considerable weight.*”, p. 27.

¹³⁸ EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1.

As established above in Section 6.8, Xandr did not obtain valid consents from the Grindr users, neither directly from them nor when relying on the consents collected by Grindr, for the processing of personal data in accordance with Article 6(1)(a) GDPR, pursuant to Article 4(11) and Article 7.

Consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. This control is ever more important when special category data are in scope, in light of their private and sensitive nature. Xandr's failure to fulfil the requirements for a valid consent resulted in data subjects having limited or no control over the use and dissemination of their personal data. These circumstances meant that data subjects' control and choice over their personal data became illusory.

Xandr unlawfully processed personal data for purposes of behavioral advertisement.¹³⁹ At the time of investigation, Xandr's list of third-party providers included more than 4000 companies.¹⁴⁰ This list included bidders, real time data providers, and other third parties. The fact that Xandr shared the personal data that it collected unlawfully with an unknown number of companies, and that it would not be possible for data subjects to know precisely which companies that received their data, adds to the gravity of the infringement.

Xandr's collection and sharing of personal data involves tracking and profiling. Xandr itself states that it would identify whether the device visiting the Grindr app was assigned to any interest segments that Xandr made available to the advertiser clients. The Article 29 Working Party describes some of the challenges concerning profiling in their profiling guidelines:

*The process of profiling is often invisible to the data subject. It works by creating derived or inferred data about individuals – 'new' personal data that has not been provided directly by the data subjects themselves. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes.*¹⁴¹

The EDPB also summarizes some of the risks to fundamental rights that are involved in profiling and targeting based on personal data in paragraph 8-17 of its Guidelines 8/2020 on the targeting of social media users. One of the risks the EDPB describes is the potential manipulation of users:

A second category of risk relates to potential possible manipulation of users. Targeting mechanisms are, by definition, used in order to influence the behaviour and

¹³⁹ Behavioural advertising can be defined as advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests, see Article 29 Working Party, Opinion 2/2010 on online behavioural advertising (WP 171), p. 4.

¹⁴⁰ See NCC Report, p. 133 which referenced AppNexus' (now Xandr) list over "Third Party Providers" on its previous website. Xandr's current list of Third-Party Providers can be accessed here: <https://learn.microsoft.com/en-us/xandr/policies-regulations/third-party-providers> [last accessed 19 March 2025].

¹⁴¹ Article 29 Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01), p. 9.

*choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens engaged in civic life. Certain targeting approaches may however go so far as to undermine individual autonomy and freedom (e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns).*¹⁴²

The AdTech ecosystem is complex to understand for data subjects, and as stated by the EDPB, “a lack of transparency regarding the role of the different actors and the processing operations involved may undermine, complicate or hinder the exercise of data subject rights.”¹⁴³ This also adds to the gravity of the infringements.

The data subjects did not themselves initiate the particular processing operations in question. As discussed in Section 5.4 of the decision against Grindr, they presumably wanted to access the services provided in the Grindr app, and they did not necessarily intend to share their personal data to Xandr and Xandr’s 4000 advertising partners for commercial purposes. To illustrate, in the NO DPA’s privacy survey of 2024, 39 % of respondents were very negative to personal data being used to target them with advertisement, and further 28 % of the respondents were somewhat negative.¹⁴⁴ In a survey by YouGov commissioned by the NCC, 30 % of the respondents were very negative towards receiving ads based on their personal data, and further 22 % of the respondents were somewhat negative.¹⁴⁵

When considering the gravity of the infringements, the NO DPA also take into consideration that the processing in question is linked to Xandr’s core business activities to enable advertising transactions. The more central the processing is to the controller’s core activities, the more severe irregularities in this processing will be.¹⁴⁶

The number of data subjects concretely but also potentially affected is one of the relevant conditions when considering whether to impose an administrative fine.¹⁴⁷ According to the WP29 guidelines endorsed by the EDPB, the number of data subjects involved should be assessed, in order to identify whether this was an isolated event or symptomatic of a more systemic breach or lack of adequate routines in place.¹⁴⁸

For the purpose of the administrative fine, the NO DPA only take into consideration affected users in Norway. Thousands of Grindr users were subject to the unlawful sharing by Grindr to

¹⁴² EDPB Guidelines 8/2020 on the targeting of social media users, Version 2.0, para. 12.

¹⁴³ *Ibid*, para. 10.

¹⁴⁴ <https://www.datatilsynet.no/contentassets/4cc3a1d522254004a44641e46b2459f5/personvernundersokelsen-2024.pdf> p. 33, [last accessed 19 March 2025].

¹⁴⁵ <https://storage02.forbrukerradet.no/media/2021/06/202106-befolkningsundersokelse-holdninger-til-overvåkingsbasert-markedsføring.pdf>, [last accessed 19 March 2025].

¹⁴⁶ EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1, section 4.2.1, para. 53 b) iii).

¹⁴⁷ EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1, section 4.2.1, para. 53 b) iv).

¹⁴⁸ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018 p. 10.

other third parties.¹⁴⁹ The NO DPA does not know how many bid requests related to Grindr users Xandr received or shared during the investigation period. Thus, the NO DPA does not know the exact number of data subjects affected by Xandr's processing. Xandr states that it has searched its systems and has not identified any of the personal data it processed as part of providing its services to Grindr, since this data would have been deleted in accordance with Xandr's data retention policies applicable to data received in advertising transactions. Furthermore, Xandr submits that it did not receive requests from MoPub to display ad space on the Grindr app relating to Grindr users in Norway every month of the investigation period.¹⁵⁰

Since the NO DPA is unable to establish the facts concerning the number of affected users *in casu*, the NO DPA will not place any weight on this consideration. The NO DPA notes however, that the number of data subjects affected is just one of several elements in the assessment of whether to impose an administrative fine.

The type of data collected and shared unlawfully also illustrates the gravity of the infringements. Special categories of personal data, such as data concerning sexual orientation, merit specific protection under the GDPR. The affected data subjects wanted to join a dating and social networking app, with the opportunity to connect with others in the LGBTQ+ community nearby. The collection and sharing of the data without the data subjects' valid consent has breached the data subjects' trust. Misuse of the data concerning sexual orientation could put the data subject's fundamental rights and freedoms at risk, such as the right to privacy and non-discrimination.

The NO DPA will also consider the duration of the infringements. The duration of an infringement may be illustrative of, for example, willful conduct on the data controller's part, failure to take appropriate preventive measures, or inability to put in place the required technical and organizational measures.¹⁵¹

The NO DPA's findings suggest that Xandr lacked a legal valid basis for its processing during the investigation period, i.e. the time period between 20 July 2018 and 7 April 2020. By this time, the GDPR had been in force in Norway for almost two years. The duration of the infringement is an aggravating factor.

Based on the above, the NO DPA considers the infringements of high seriousness. The nature and gravity of the infringements, together with their duration constitute aggravating factors that all weigh in favour of imposing an administrative fine.

7.2.2 (b) the intentional or negligent character of the infringement

¹⁴⁹ 23-160384TVI-TOSL/04 p. 30.

¹⁵⁰ Reply to order to provide information 6 December 2024.

¹⁵¹ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018 pp. 10-11.

As noted under Section 7.1, the establishment of intention or negligence is a condition for imposing an administrative fine pursuant to Article 83(2)(b) GDPR, and Article 83(3) GDPR.¹⁵²

The GDPR itself does not identify the factors that need to be present in order for an infringement to be classified as either “intentional” or “negligent”. The Article 29 Working Party considered this in its Administrative Fines Guidelines as follows:

*In general, ‘intent’ includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas ‘unintentional’ means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.*¹⁵³

Pursuant to the requirement of due care, businesses and the responsible individuals acting on its behalf, need to examine legal requirements that apply to their field and implement these. Negligence exists where a person acts in contravention of the requirement of due care in an area of life and where the person may be held to blame in view of their personal circumstances.¹⁵⁴ The NO DPA notes that the duty of care is normally considered to be strict for enterprises conducting economic activities.¹⁵⁵ The NO DPA finds that the same strict standard for the duty of care must be applied in this case.

The Norwegian Supreme Court has ruled that it is not required that an identified individual has acted culpably on behalf of the company, and that anonymous and cumulative infringements committed by individuals who act on behalf of the company can be regarded as fulfilling the requirement of culpability, as long as the minimum requirement of negligence is in place.¹⁵⁶

Furthermore, the CJEU has affirmed that where the controller is a legal person, it is not necessary for there to have been action by or even knowledge on the part of the management body of that legal person for Article 83 GDPR to apply.¹⁵⁷

¹⁵² Court of Appeals 24-154313ASD-BORG/02, pp. 29-30, CJEU judgements in cases C-807/21 Deutsche Wohnen SE v Staatsanwaltschaft Berlin, para 73 and C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos v Valstybinė duomenų apsaugos inspekcija, para. 73.

¹⁵³ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018, p. 11.

¹⁵⁴ See the Norwegian Penal Code 20 May 2005 no. 28: *Any person who acts in contravention of the requirements of due care in an area of life, and who may be held to blame in view of his or her personal circumstances, is negligent. The negligence is gross if the act is highly reproachable and there are grounds for significant blame.* A [link](#) is provided to an unofficial translation of the law to English. The Norwegian law version prevails.

¹⁵⁵ See [Prop. 81 L \(2021–2022\) Section 5.5](#). Link is in Norwegian.

¹⁵⁶ HR-2022-1271-A para. 36-50.

¹⁵⁷ CJEU Judgement Case C-807/21 Deutsche Wohnen SE v Staatsanwaltschaft Berlin, para 77, with further reference to: See, by analogy, judgments of 7 June 1983, Musique Diffusion française and Others v Commission, 100/80 to 103/80, EU:C:1983:158, paragraph 97, and of 16 February 2017, Tudapetrol Mineralölerzeugnisse Nils Hansen v Commission, C-94/15 P, EU:C:2017:124, paragraph 28 and the case-law cited).

The Administrative Fines Guidelines proceed to detail how supervisory authorities should determine whether willfulness or negligence was present in a particular case:

*The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.*¹⁵⁸

As established in Section 6.8 and 6.9, the NO DPA has found that there is clear and convincing evidence that Xandr infringed Articles 6(1)(a) and 9(1) GDPR.

In determining whether an infringement was negligent, the NO DPA must determine whether the objective elements of conduct demonstrate that the controller ought to have been aware in the circumstances that it was falling short of the duty owed at the time under consideration.

Xandr is a leading advertiser technology company processing personal data on a large scale, and the processing of personal data constitutes the core part of its business. In light of Xandr's position in the AdTech industry and RTB environment, Xandr must be expected to be acquainted and compliant with central data protection requirements, such as having valid legal basis for their processing.

Xandr has stated in their response to the advance notification that Xandr was not aware of the processing of special categories personal data and that there is no reason to conclude that Xandr should have known this.¹⁵⁹ Furthermore, Xandr has stated that it would have been unfeasible for Xandr to determine whether the customer's legal basis for processing was valid.¹⁶⁰

As a joint controller, however, Xandr is responsible for complying with the GDPR, including pursuant to the accountability principle under Article 5(2) and Article 24 GDPR, which describes the controller's responsibility to implement appropriate technical and organizational measures. Here, the NO DPA notes that Xandr was already aware that it was a joint controller at least for parts of the processing. Therefore, it should have taken measures to ensure that it could lawfully process those personal data so integral to its business objectives, lawfulness being one of the most fundamental requirements in the GDPR.

Xandr devised a system in which it effectively outsourced the necessary assessments. Xandr asserts that pursuant to its contractual relationship with Grindr, it was Grindr's sole duty to verify the nature of the data and ensure valid consents. Such a position cannot be accepted. As a controller, Xandr carries a responsibility that cannot be shifted onto others. It was negligent of Xandr to not make any assessments as regards the lawfulness of the processing.

As Xandr did not itself have any direct interaction with the data subjects and thus can be considered to be 'further down the chain', in the NO DPA's opinion, it had all the more reason to check and ensure lawfulness.

¹⁵⁸ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018, p. 12.

¹⁵⁹ Response to the advance notification 2 June 2025 p. 1

¹⁶⁰ Response to the advance notification 2 June 2025 p. 2.

At the time, there was also guidance available from the Article 29 Working Party, endorsed by the EDPB, on the relevant consent requirements. The guidance would have aided Xandr to identify that Grindr's consent mechanism and the consent obtained did not comply with the requirements of the GDPR.¹⁶¹ Thus, the NO DPA considers that Xandr did not take the measures that could reasonably be expected of a controller to verify and ensure that a valid legal basis existed for its own processing, and this was at least negligent.

The Court of Appeal in the Grindr case further illustrates the importance of the controller understanding the circumstances in which consent is obtained. The court considered that, the sensitivity of the data in question and the importance of complying with the GDPR's consent requirements, a lack of knowledge regarding what information is shared and how the consent mechanism is designed, would in any case constitute gross negligence.¹⁶²

Consequently, Xandr's argument that the measures were adopted without intent to breach the GDPR must therefore be rejected. First, lack of intent does not, per se, exclude liability; second, the evidence demonstrates that the infringing conduct was at least negligent and thus culpable pursuant to Article 83(2)(b) GDPR.

In light of Xandr's role and their core business, the low threshold for establishing negligence for large commercial actors and the fact that the infringements concern some of the most central provisions in the GDPR, the NO DPA concludes that there is a clear preponderance of probability that the infringements of Article 6(1) and Article 9(1) were at least negligent under the circumstances in the present case.

7.2.3 (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects

The NO DPA considers that this factor is not relevant in the present case.

7.2.4 (d) the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32

According to the Administrative Fines Guidelines, the question that the NO DPA must answer is to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on them by the GDPR.¹⁶³

As observed above, Xandr was a joint controller in this case, and joint controllership does not necessarily entail equal responsibility. The obligation to ensure valid consent did not lie with Xandr alone, and consents were in practice collected by Grindr.

¹⁶¹ Article 29 Working Party, Opinion 15/2011 on the definition of consent (WP187), adopted on 13 July 2021.

¹⁶² 24-154313ASD-BORG/02, pp. 30-31.

¹⁶³ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018, p. 13.

Nevertheless, both parties had an obligation to ensure valid legal basis. Moreover, Xandr has not demonstrated to the NO DPA that it had integrated appropriate, or in fact any, measures to ensure that the consents collected by Grindr were valid. Simply referring to a contractual obligation on the part of Grindr to collect valid consents is not, in the NO DPA's opinion, an adequate measure that would contribute towards adherence to the GDPR requirements and protect the rights of the data subjects. Furthermore, the processing activity in question is linked to core activities of Xandr, and Xandr is expected to allocate a corresponding amount of attention and resources to its data protection responsibilities. The nature of the processing and the risks associated with it shows the importance of integrating appropriate measures to ensure that data was not collected and shared unlawfully, and this is an aggravating factor.

7.2.5 (e) any relevant previous infringements by the controller or processor

The NO DPA is not aware of any previous infringements.

7.2.6 (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

Xandr has cooperated with the NO DPA by providing information and answering most of the NO DPA's questions in its responses to the orders to provide information. This is in itself neither an aggravating nor a mitigating circumstance in the present case.¹⁶⁴

Additionally, Xandr voluntarily attended the 27 February Meeting in order to help the NO DPA establish the facts of the case, which goes beyond the cooperation that is required by law. However, the NO DPA could have legally compelled Xandr to provide the same information, and the meeting was necessary as some of Xandr's written statements were less informative. The NO DPA considers Xandr attending this meeting as slightly mitigating.

7.2.7 (g) the categories of personal data affected by the infringement

As discussed under (a) and 6.5 above, Xandr collected special categories of personal data unlawfully. Data concerning sexual orientation merit special protection under the GDPR, as disclosure of such data could put the data subject's rights and freedoms at risk, such as the right to privacy and non-discrimination. The NO DPA considers categories of personal data affected by the infringement as an aggravating factor.

¹⁶⁴ According to the Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018 p. 14, letter (f) could be a mitigating factor in some cases, however it would not be appropriate to give regard to cooperation that is already required by law. This is confirmed in 24-154313ASD-BORG/02, p. 32 where it states in unofficial translation: *"Having regard to the fact that the undertaking is under an obligation to respond to inquiries, and that it also has a self-interest in doing so, no weight can in any event be attached to such cooperation."*

7.2.8 (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement

The NO DPA considers that this factor is not relevant in the present case.

7.2.9 (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures

This factor is not applicable in the present case, as no measures referred to in Article 58(2) have previously been ordered against Xandr with regards to the same subject-matter.

7.2.10 (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

This factor is not applicable in the present case, as Xandr does not appear do adhere to any approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42.

7.2.11 (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement

Xandr holds that it was not aware of regulatory guidance that stated (and certainly it was not market practice to consider) that the mere fact that an individual was a user of Grindr or similar apps could in itself constitute special category data under Article 9(1) GDPR. As established above in Section 6.7, the NO DPA holds that Xandr has infringed clear and precise legal requirements in Article 9 GDPR, which should clearly have been foreseeable for Xandr.

According to the Administrative Fines Guidelines,¹⁶⁵ profit from infringements is a strong indication that a fine should be imposed:

Information about profit obtained as a result of a breach may be particularly important for the supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. As such, the fact that the controller had profited from the infringement of the Regulation may constitute a strong indication that a fine should be imposed.

The NO DPA finds it aggravating that Xandr must have gained financial benefits from the infringements, since the collection and sharing of personal data would enable Xandr to

¹⁶⁵ Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253), EDPB Endorsement 1/2018 p. 16.

facilitate advertising transactions and thus make profit.¹⁶⁶ If the consent had been informed, specific and freely given, and Grindr users had been provided with a real choice, it is likely that at least some users would not have agreed to the processing. Therefore, the NO DPA considers that there is clear preponderance of evidence that this infringement has led to a financial benefit for Xandr. Hence, in accordance with Article 83(2)(k) GDPR, this should be considered an aggravating factor.

Xandr has stated that the NO DPA has applied legal standards and reached conclusions in this case that neither Xandr nor any other legal company in its position objectively could have expected at the time the investigation began.¹⁶⁷ The NO DPA considers this statement to refer to the industry practice, and as stated by the Court of Appeal, industry practice during the relevant period cannot be considered a mitigating factor as it would undermine the deterrent effect of an administrative fine.¹⁶⁸ Moreover, the Court of Appeal in the Grindr case finds the fact that many companies in the industry breach the law reinforces the need for an administrative fine with a deterrent effect.¹⁶⁹

As to the amount of the fine, Xandr has stated that the NO DPA should reduce the fine further to account for its delay in handling the case.¹⁷⁰ Xandr has further stated:

“[E]limination of—or at a minimum a further decrease in the amount of—the fine is particularly warranted in this case given the impact that the NO DPA’s delays have had on Xandr’s ability to defend itself”.¹⁷¹

The practice of the Norwegian Privacy Appeals Board¹⁷² indicates that lengthy case handling time is an element to be considered under Article 83(2)(k) GDPR. Therefore, the NO DPA regards this a mitigating factor. The NO DPA does not however agree with Xandr’s claim that the delays have undermined Xandr’s ability to defend itself. As previously stated, Xandr were aware of the investigation and thus cannot in good faith under the investigation period delete the underlying data pursuant to its data retention policies.

7.2.12 Conclusion on whether to impose an administrative fine

In sum the NO DPA found aggravating factors in Article 83(2)(a)(d)(g)(k), mitigating factors in Article 83(2)(f)(k) and neutral factors in Article 83(2)(c)(e)(h)(i)(j). The argumentation above shows that an administrative fine is proportionate in the present case. In the NO DPA’s view, the imposition of an administrative fine is warranted to produce a genuine deterrent effect and dissuade Xandr – and other companies in general – from committing similar

¹⁶⁶ 24-154313ASD-BORG/02, p. 33. The Court of Appeal in the Grindr case found financial benefit an aggravating factor

¹⁶⁷ Response to the advance notification 2 June 2025 p. 1.

¹⁶⁸ 24-154313ASD-BORG/02, p. 31.

¹⁶⁹ 24-154313ASD-BORG/02, p. 31.

¹⁷⁰ Response to the advance notification 2 June 2025 p. 32.

¹⁷¹ Response to the advance notification 2 June 2025 p. 34.

¹⁷² The Privacy Appeals Board has revised their practise regarding reduction for long case handling time after the NO DPA sent the advance notification. See PVN 2025-30 p. 11.

infringements in the future. Indeed, enforcement efforts must generate sufficient pressure to make non-compliance economically unattractive in practice.¹⁷³

7.3 Deciding the amount of the administrative fine

It should be noted that the setting of a fine is not an arithmetically precise exercise,¹⁷⁴ and supervisory authorities have a certain margin of discretion in this respect.¹⁷⁵ They should nonetheless specify the factors that influenced the exercise of their discretion when setting a fine.¹⁷⁶

Article 83(1) GDPR establishes the following when deciding the amount of an administrative fine:

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

Article 83(2) further provides that when deciding on the amount of the administrative fine in each individual case, due regard shall be given to the factors listed in Article 83(2)(a)–(k) GDPR.

Recital 148 of the GDPR emphasizes that administrative fines should be imposed “in order to strengthen the enforcement of the rules of this Regulation”.

Recital 150 GDPR states:

Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes.

Pursuant to case law of the CJEU, the term “undertaking” must be understood as an economic unit, even if that economic unit consists of several legal persons.¹⁷⁷ Different companies belonging to the same group forming an economic unit is therefore considered an “undertaking” within the meaning of Articles 101 and 102 Treaty on the Functioning of the European Union (TFEU).¹⁷⁸

¹⁷³ See Opinion of Advocate General in Case C-304/02 *Commission v. France*, para. 39.

¹⁷⁴ See, *inter alia*, CJEU judgement in Case T-425/18 *Altice Europe NV v Commission*, in para. 362 and Case T-11/06 *Romana Tabacchi v Commission*, in para. 266.

¹⁷⁵ See, *inter alia*, CJEU judgement in Case T-192/06 *Caffaro Srl v Commission*, in para. 38.

¹⁷⁶ EDPB Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, in para. 75.

¹⁷⁷ See CJEU Judgement in Case C-516/15 P *Akzo Nobel and Others v Commission*, in para. 48, with further references. See also CJEU Judgement in Case C-807-21 *Deutsche Wohnen SE v Staatsanwaltschaft Berlin*, in para. 56.

¹⁷⁸ See EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1, p. 36.

Furthermore, the CJEU confirmed in the *ILVA* case that:

*(...) the term ‘undertaking’ in those provisions corresponds to the concept of ‘undertaking’, within the meaning of Articles 101 and 102 TFEU, with the result that, where a fine for infringement of the GDPR is imposed on a controller of personal data which is or forms part of an undertaking, the maximum amount of the fine is to be determined on the basis of a percentage of the undertaking’s total worldwide annual turnover in the preceding business year. The concept of ‘undertaking’ must also be taken into account in order to assess the actual or material economic capacity of the recipient of the fine and thus to ascertain whether the fine is at the same time effective, proportionate and dissuasive.*¹⁷⁹

In a different case, the EDPB has issued a binding decision with the instruction to the supervisory authority to take into consideration the total turnover of all the entities composing the single undertaking, i.e., the consolidated turnover of the group of companies headed by the parent company.¹⁸⁰

The EDPB explains that whether several entities form a single economic unit depends largely on whether the individual entity is free in its decision-making ability or whether a leading entity, namely the parent company, exercises decisive influence over the others.¹⁸¹ Moreover, the EDPB states that in the specific case where a parent company holds 100% of shares or almost 100% of shares in a subsidiary which has infringed the GDPR and therefore is able to exercise decisive influence over the conduct of its subsidiary, a presumption arises that the parent company does in fact exercise this decisive influence over the conduct of its subsidiary (so-called Akzo presumption). It is sufficient that the subsidiary is directly or indirectly wholly or almost wholly owned by the parent company in order to presume – as a rule of practical experience – that the parent exercises a decisive influence.¹⁸²

Xandr is now owned by Microsoft, a multinational technology conglomerate headquartered in the United States. Therefore, in this case, the administrative fine should be calculated – at least as a starting point - on the basis of a percentage of Microsoft’s annual turnover.¹⁸³

However, Microsoft did not own Xandr during the investigation period. Thus, Microsoft was not in a legal or factual position to exercise decisive influence over the conduct of its now subsidiary at that time. It is therefore pertinent to assess whether these circumstances merit a different conclusion.

The concept of “undertaking” is taken from competition law, and therefore, jurisprudence from that field of law may be relevant. In this regard, the CJEU judgment in case C-408/12 P *YKK*

¹⁷⁹ See CJEU Judgement in Case C-382/23 *ILVA A/S*, in para. 36.

¹⁸⁰ EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022, para 356.

¹⁸¹ See also EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1, in para 122.

¹⁸² *Ibid*, in para 124.

¹⁸³ *Ibid*, in para 124.

offers some guidance. One of the questions for consideration in that case was how to calculate the maximum possible fine for a company that had violated competition law. The perpetrating company had been acquired by a different company and became part of a larger undertaking during the infringement period. The dispute concerned whether the fine for the violation taking place before the acquisition should be calculated on the basis of the turnover of the individual perpetrating company or the turnover of the undertaking of which it later formed a part. The CJEU concluded with the former.¹⁸⁴

Consequently, the NO DPA considers that in the specific circumstances at hand, it would not be appropriate or proportionate to base a fine on the turnover of Microsoft, nor would it be necessary to do so in order to ensure that the fine is effective and dissuasive. The NO DPA will therefore base the calculation of the administrative fine on Xandr's revenue, given the facts of this particular case.

The infringements found in this case qualify for administrative fines under Article 83(5) GDPR, pursuant to *litra* (a) of the provision. The maximum amount under Article 83(5) GDPR is EUR 20 000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, *whichever is higher*. As stated before, the NO DPA has found it necessary to impose on Xandr an administrative fine for the infringements of Articles 6(1) and 9(1) GDPR. Article 83(3) GDPR provides that in the event of multiple breaches, as in this case, the total amount of the fine may not exceed the amount set for the most serious breach.

In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, the turnover of Xandr must be taken into account. The NO DPA will take the turnover of Xandr as the maximum fine applicable in the present case.

Xandr generated total revenue of USD [REDACTED]¹⁸⁵ approximately NOK [REDACTED]¹⁸⁶ or approximately EUR [REDACTED]¹⁸⁷ When determining the maximum amount of the fine in accordance with Article 83(5), EUR 20 000 000 is higher than 4 % of Xandr's total worldwide annual turnover. Thus, the legal maximum amount pursuant to Article 83(5) GDPR is EUR 20 000 000, which converts to approximately NOK 215 800 000¹⁸⁸ and USD 23 064 596.¹⁸⁹

¹⁸⁴ CJEU Judgment in Case C-408/12 P, YKK Corporation and Others v European Commission, para. 68.

¹⁸⁵ Response to additional order to provide information 15 June 2026, that clarifies financial year for 2025 covers the period from 1 July 2024 to 30 June 2025.

¹⁸⁶ Based on the USD to NOK daily exchange rate on 15 September 2026 of 9,35, quoted by Norges Bank: [Exchange rates \(norges-bank.no\)](https://www.norges-bank.no/exchange-rates) [last visited 16 September 2026].

¹⁸⁷ Based on the EUR to NOK daily exchange rate on 15 September 2026 of 10,79, quoted by Norges Bank: [Exchange rates \(norges-bank.no\)](https://www.norges-bank.no/exchange-rates) [last visited 16 September 2026].

¹⁸⁸ Based on the EUR to NOK daily exchange rate on 15 September 2026 of 10,79, quoted by Norges Bank: [Exchange rates \(norges-bank.no\)](https://www.norges-bank.no/exchange-rates) [last visited 16 September 2026].

¹⁸⁹ Based on the USD to NOK daily exchange rate on 15 September 2026 of 9,35, quoted by Norges Bank: [Exchange rates \(norges-bank.no\)](https://www.norges-bank.no/exchange-rates) [last visited 16 September 2026].

The NO DPA refers to the assessments above in Section 7.2 on the factors of Article 83(2)(a)-(k) GDPR. In sum the NO DPA found aggravating factors in Article 83(2)(a)(d)(g)(k), mitigating factors in Article 83(2)(f)(k) and neutral factors in Article 83(2)(c)(e)(h)(i)(j). In calculating the fine the NO DPA considers that considerable weight should be attributed to the nature, gravity and the duration of the infringements as concluded under letter (a).

This case concerns core elements of the GDPR, Xandr is a big, leading company in the AdTech industry and it is apparent that Xandr has made profit of an illegal system. However, there are as mentioned above some factors in the present case that merits a downward adjustment to the starting amount.

In accordance with the practice prevailing at the time of the advance notification, the length of the case handling time was regarded a mitigating factor. Accordingly, the amount of the fine has been reduced in this case.¹⁹⁰

Xandr disagrees with the use of revenue for the fiscal year of 2025, since it has taken the NO DPA over a year after the advance notification was sent to issue the present decision.¹⁹¹ In CJEU case law in competition law, which also applies to GDPR fines, the relevant point in time is when the fining decision is issued by the supervisory authority – not when the infringement took place, nor when a court gives its decision.¹⁹²

In light of all the relevant criteria of Article 83(2)(a)-(k) described above in Section 7.2 and the factors which implies downward adjustment to the starting amount as described above, the NO DPA imposes a fine of NOK 92 000 000 is effective, proportionate and dissuasive in the present case.

An amount of NOK 92 000 000 is [REDACTED] of Xandr annual turnover. This amounts to approximately EUR 8 500 000¹⁹³ and lies within the static range of 4 million EUR to 20 million EUR referred to in the EDPB's Guidelines 04/2022 for infringements with high level of seriousness.¹⁹⁴ The NO DPA emphasizes that the NO DPA has the discretion to utilise the full fining range from any amount up to and including the legal maximum.¹⁹⁵ The NO DPA finds this amount proportionate both to the severity of the infringements and to Xandr's financial situation, and it does not exceed what is necessary to achieve the objectives pursued by the GDPR in the present case.

¹⁹⁰ Although The Privacy Appeals Board has revised their practise regarding reduction for long case handling time after NO DPA sent the advance notification, NO DPA have decided to uphold what already was notified in this regard. See PVN 2025-30 p. 11.

¹⁹¹ Response to additional order to provide information 15 June 2026.

¹⁹² Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1, p. 38.

¹⁹³ Based on the EUR to NOK daily exchange rate on 15 September 2026 of 10,79, quoted by Norges Bank: [Exchange rates \(norges-bank.no\)](https://www.norges-bank.no/exchange-rates) [last visited 16 September 2026].

¹⁹⁴ EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1., p. 44.

¹⁹⁵ See EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR, Version 2.1., pp. 43-44.

8 Right of appeal

This decision may be appealed within **three weeks** of receipt of this letter, cf. Chapter VI of the Public Administration Act. In case of an appeal it should be sent to the NO DPA. If the NO DPA upholds the decision, the case will be sent forward to the Norwegian Privacy Appeals Board for consideration pursuant to Section 22 of the Norwegian Personal Data Act.

9 Access to documents

Pursuant to Sections 18 and 19 of the Public Administration Act, Xandr – as a party to this case – has the right to acquaint itself with the documents in the case.

Pursuant to Section 3 of the Norwegian Freedom of Information Act,¹⁹⁶ all case documents the NO DPA holds are, as a rule, subject to public access. If Xandr is of the opinion that any documents in this case should be partly or entirely exempted from public access based on legal derogations, please notify the NO DPA and provide an explanation for the claim.

Kind regards

Line Coll
Director General

Tobias Judin
Head of International

This letter has electronic approval and is therefore not signed

Copy to: FORBRUKERRÅDET

¹⁹⁶ Act relating to the right of access to documents held by public authorities and public undertakings 19 May 2006 no. 16 ([Freedom of Information Act](#)) (Lov om rett til innsyn i dokument i offentlig verksemd (offentleglova)). A link is provided to an unofficial translation of the law to English. The Norwegian law text prevails.