SCHJØDT

CONFIDENTIAL

DATATILSYNET
Postboks 458 Sentrum
0105 Oslo
Att: Bjørn Erik Thon and Anders Sæve Obrestad

Sent electronically only

Oslo, 8 March 2021
Doc.ref: 48315-601-8586733.1
Case responsible: Eva Jarbekk

REPLY TO ADVANCE NOTIFICATION IN CASE 20/02136-5

TABLE OF CONTENTS

1. INTRODUCTION AND SUMMARY OF MAIN LEGAL ARGUMENTS

We refer to your advance notification of 24 January 2021 (the "**Advance Notification**").

Below, we first set out a short summary of the legal views. Then we address background information on Grindr LLC ("**Grindr**" or the "**Company**"), Grindr's community work, and Grindr's ongoing commitment to transparency with its users and compliance with the General Data Protection Regulation ("**GDPR**"). We will also describe how Grindr endeavored (then and now) to be industry leading on privacy and data protection compliance, even though a small player in the exponentially larger ad tech industry.

We will thereafter address the legal arguments set out by the Norwegian Data Protection Authority, Datatilsynet ("**Datatilsynet**"), in the same sequence as in the Advance Notification.

It is important to note that the facts recorded by the Norwegian Consumer Council ("**NCC**"), and that Datatilsynet relies on, relate to a consent mechanism that Grindr stopped using in April 2020. In the Company's efforts to continuously enhance its overall privacy practices that support its compliance with global privacy requirements, including the GDPR, Grindr has indeed further refined its consent management process since then.

Grindr's proactive fine-tuning of its consent mechanisms started in June 2019 and did not stem from any particular complaint. Grindr was already launching its new consent mechanism by the time they received the letter from the Datatilsynet in 2020.

Nevertheless, as this, now-deprecated, consent mechanism seems to be relevant for this matter, it is this older mechanism that will be further described and referred to in this response.

After reviewing the facts of Grindr's GDPR compliance efforts, the surrounding circumstances of the ad tech industry in the early days of the GDPR, and the law cited in this brief, Grindr is confident that Datatilsynet will find Grindr to be a company committed to being of service to its users in compliance with the GDPR. If Datatilsynet continues to pursue a fine, Grindr believes the fine should be dramatically reduced as explained below.

1.1 Summary of main legal arguments

Grindr has legal basis for the processing in question

- Grindr is, and has always been, very clear on informing users of how personal data is used and has at all times had industry-leading disclosures about how personal data is used by the Grindr social networking platform (the "App"). Information has been given both before using the App and through multiple touch points, including without limitation in-App prompts, descriptive user interfaces, and a robust and transparent Privacy Policy, help center, and other online resources.
- The principle of legal certainty (No: "*legalitetsprinsippet*") under EEA law and Norwegian administrative law requires that in order to impose an administrative fine, there must be a clear legal basis and "*objective, non-discriminatory criteria which are known in advance to the undertakings concerned*". The requirements in Article 6 and 9, when applied to Grindr's previous consent mechanism, do not suffice as legal basis for imposing the notified administrative fine.
- Even under historical practice, Grindr obtained appropriate consent for the described processing according to the requirements in the GDPR itself. "Guidelines" from the EDPB cannot be the legal basis for administrative sanctions as set out by Datatilsynet.
- Users had ample possibilities to consent or object to the processing before such processing took place:

    1. At the beginning of the sign-up process in the App, users had to confirm having read Grindr's Terms and Conditions of Service ("**T&Cs**");

    2. To continue signing up for the App, users had to confirm adherence to the T&Cs;

    3. Users had to confirm having read Grindr's Privacy Policy (the "**Privacy Policy**") that was presented in full text to the user; and

    4. Users had to accept the processing set forth in the Privacy Policy.

    5. Users could choose not to share data with advertising partners. If users denied sharing data with advertising partners via the controls available in their device's mobile operating system, the App would still work equally well. In June 2019, Grindr began implementing the industry-leading OneTrust consent management platform to give users even greater

granularity and control from within the App with respect to their information sharing options.

6. Like in many free apps, users had the option of upgrading to a paid subscription without ads for a small, reasonable fee. Offering an ad-free, payable version of an app, as an alternative to a free version of an app financed by advertisements, is both a common and legal practice.

- If users did not approve of Grindr's processing of their personal data or the overall concept/service offerings of the App, users had the choice to select alternative apps. Grindr does not have a monopoly in its particular app category.

Grindr has not shared special categories of personal data with advertising partners

- Grindr did not share a user's sexual orientation with advertising partners.
- Grindr shared data points common in the industry such as Advertising ID (provided by the device's mobile operating system and under full user control) and information about the computing environment (operating system version, model, screen resolution, etc.); age, gender (e.g., male or female) and location. As of June 2020, Grindr stopped sharing even a user's obfuscated location information, age or gender with advertising partners.
- Grindr is one of the few places where the full spectrum of sexual orientations are represented and where users can interact with each other safely. Grindr is used by users of all sexual orientations, including those who belong to the LGBTQ+ community as well as users who identify as heterosexual. The fact that an individual has the App installed on their device does not reveal the specific sexual orientation of said user. Therefore, the presence of the App on one's device does not equate to a special category of personal data, in and of itself. This is supported by a German judgement.

On the size of the warned fine

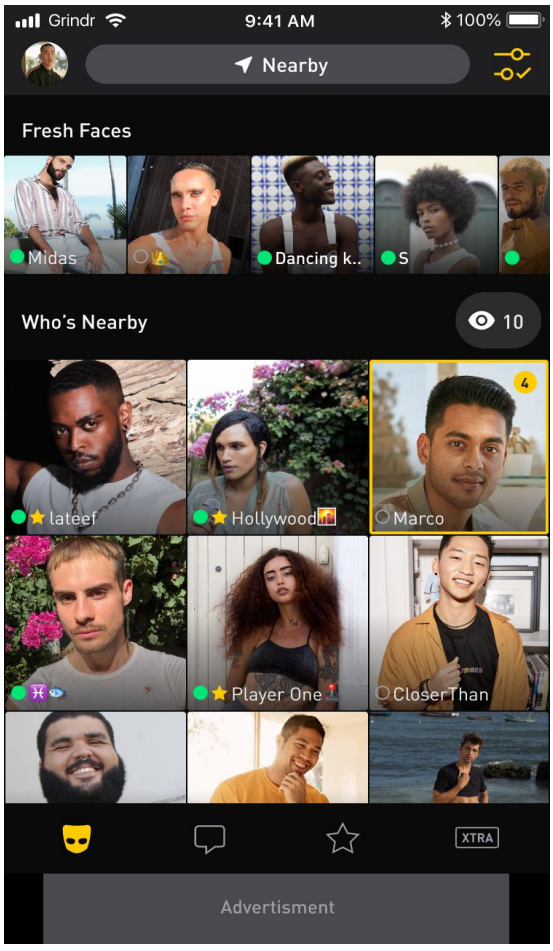
- Datatilsynet has not given adequate attention to the many measures taken by Grindr to fine-tune its mechanisms for obtaining consent. Grindr has always been proactive in securing the privacy of its users. Consent mechanisms have been in place since the launch of the App, and the consent mechanisms have been fine-tuned as industry consent practices and guidance have evolved, including through regulator feedback. The facts recorded by NCC, and that Datatilsynet relies on, relate to a consent mechanism that Grindr stopped using in April 2020. The privacy regulatory landscape, including interpretations of the GDPR (and more specifically, notions related to consent) have evolved and continue to evolve over time. Therefore, it is not proportionate to impose an administrative fine against Grindr, which has had appropriate consent mechanisms in place. Further, the size of the administrative fine indicated in the Advance Notification is certainly not proportionate to the alleged breach, nor would a fine be effective in protecting the privacy of the users, as Grindr had already further enhanced its consent mechanisms.
- A survey of recent administrative fines demonstrates that Datatilsynet's Advance Notification sets out the largest GDPR-related fine, not only in the Nordic

countries, but throughout the European Union as well relative to Grindr's size. Datatilsynet's anticipated fine is meant to address how Grindr was processing personal data of all EEA users, but the fine is not proportionate. The fine would disproportionately punish Grindr for not adhering to certain EU guidance on the finer details in how consent shall be obtained, but the guidance does not have the force of law. (And as noted, Grindr has since fine-tuned its consent mechanism that satisfies such guidance.) Therefore, the proposed fine is neither proportionate nor justified by the asserted gravity, duration, scope, or nature of the alleged breach.

- Datatilsynet's warning of the largest administrative fine that the Nordics have ever applied appears to be motivated by a desire to protect the LGBTQ+ community. However, the record-setting fine against one small player in a much larger ad tech ecosystem would have a disproportionately punitive impact on Grindr and the LGBTQ+ community that the company supports. Industry leading companies that provide services concerning heterosexuals are typically larger (in some cases exponentially so) than those serving minority communities. Thus, regulators must ensure that any penalties below the statutory cap do not disproportionately punish smaller companies, particularly ones like Grindr that demonstrate a commitment to the principles of the GDPR and work extensively to improve acceptance and a safe and open environment for the LGBTQ+ community and those supporting it.

1.2 Grindr is a community with important values

1.2.1 A diverse and active community



Grindr's social networking platform safely connects the lesbian, gay, bisexual, transgender, queer and others ("**LGBTQ+**") community both online and offline. As a pioneer LGBTQ+ social networking app, Grindr provides a unique and needed space for a historically marginalized community largely alienated from non-queer culture, including mainstream social networking and dating apps or websites.

Since its launch, Grindr has grown to represent and reflect a modern LGBTQ+ lifestyle with greater interconnectivity and that is inclusive of all sexual orientations. Grindr aims to be the preeminent platform to connect its users with the LGBTQ+ community and enable them to discover, share, and navigate their world. Grindr also provides users with an online blog and merchandise store for users to have additional ways to engage with the community.

Although Grindr is well-known in the global LGBTQ+ community, Grindr has remained a small company with a fraction of the revenue and resources of its non-queer social networking competitors. By example, in 2018 (and today) Grindr had approximately 100 employees with headquarters in West Hollywood, California.

Datatilsynet suggests, incorrectly, that a Grindr user is "*presumably gay,*" ignoring the much broader community that Grindr serves.

1.2.2 Grindr does not collect users' sexual orientation

Grindr has designed and maintains the App to be an open platform for all users of every sexual orientation and gender expression. There is no litmus test, no barrier to entry, and no preconceived requirement of a specific sexual orientation that a Grindr user must satisfy to access the App. The App does not even offer a profile field to specify one's sexual orientation.

Grindr users may be of any sexual orientation, including gay, bisexual, straight, pansexual, or questioning, just to name a few. Users may be cis men, trans men, cis women, trans women, or non-binary, among other gender identities.[1] Therefore, one Grindr user may be a cis gay man looking to connect with other cis gay men, while another user may be a straight male looking to connect with trans women. Heterosexual individuals may also be on the App out of curiosity or to find a wider expression of themselves and those they wish to connect with.

It is wrong to assume that a person having downloaded Grindr is a gay man. Downloading and using the App does not reveal your sexual orientation, it only reveals that you are interested in being on the Grindr platform and connecting with other users of the App.

Overall, the App is open to any individual who wants to download it, create an account, and comply with the T&Cs.[2] To create an account, a user must provide only an email address and password as an account identifier and a date of birth. Grindr does not require or collect a true name, phone number, government ID number, or physical address – nor is sexual

[1] The term "cis" refers to people whose gender identity matches their gender assigned at birth.

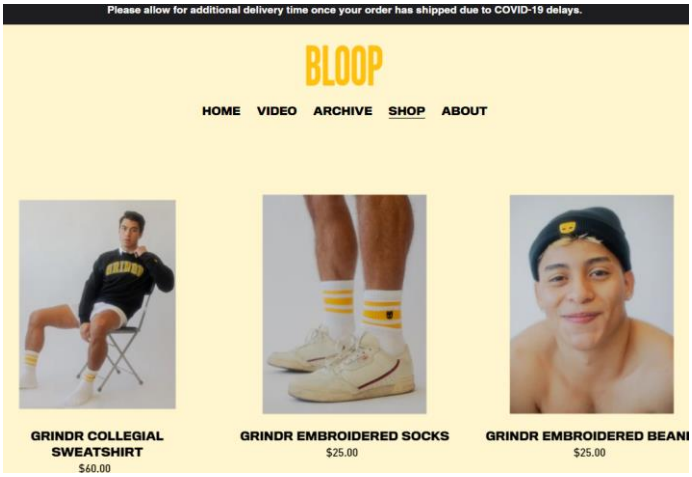
[2] Grindr does exclude users under the age of 18 (or users under the age of 21 in places where 18 is not the age of majority) and users previously banned from the App for violating Grindr's T&Cs. Apart from such exclusions, Grindr strives to maintain an open platform.

orientation or gender required. In signing up for the service, the user must agree to both Grindr's T&Cs and Privacy Policy.

1.2.3 Grindr serves the community

In addition to the App, Grindr maintains a website at www.grindr.com that provides users with additional information to support user well-being and other ways users can connect to the community. The website provides easy access to Grindr's T&Cs, Privacy Policy, and the Grindr help center with additional customer support, privacy, security, trust and safety, and other community resources.

Grindr also makes available various online safety resources, such as the holistic security guide,[3] sexual health resource center (available in more than 70 languages), and community guidelines to support self-care within the Grindr community. The Grindr website also offers users a blog that provides information on Grindr initiatives and policies, as well as an online shop, where users can purchase Grindr merchandise.[4]



As a demonstration of Grindr's commitment to the privacy, security, safety, and public health of its users, the Company established Grindr for Equality ("**G4E**"), the Company's global social impact initiative, whose mission is to work "*toward a world that is safe, just, and inclusive for people of all sexual orientations and gender identities.*"[5] As just one example, G4E partnered with an organization in India to develop and launch the first-ever online resource so that people in India could find their nearest HIV testing center.

These and other efforts illustrate how Grindr serves the global community, including LGBTQ+ people and friends of the community.

1.2.4 Grindr's focus on privacy and security

Serving a diverse community, Grindr is highly focused on protecting the interests of its users and the LGBTQ+ community at large. Grindr truly understands the risks of disseminating certain information related to the members of the LGBTQ+ community and has remained

[3] See, e.g., https://www.grindr.com/g4e/G4E-HolisticSecurityGuide-English.pdf (also available in other languages).
[4] See https://shop.grindrbloop.com/.
[5] See Grindr For Equality, Grindr, https://www.grindr.com/g4e/ (last visited Feb. 11, 2021).

focused on ensuring its features and services are developed with privacy and security controls.

Historically and today, Grindr has been committed to transparency and to obtaining the consent of its users for processing activities that are based upon the data subject's consent. Despite being a small company among much larger competitors, Grindr has often been a "first mover" in the industry in adopting privacy-forward tools like "just-in-time" notifications to its users and other privacy-forward designs (including those discussed below).

For example, starting in 2017, Grindr began providing users with the full text of Grindr's Privacy Policy and eliciting acceptance of that policy before a user created a Grindr account on the App and before users provided Grindr with any personal data. Grindr's Privacy Policy clearly and thoroughly discloses that Grindr collects personal data, shares personal data with third parties, and explains the risks of sharing location information via a location-based app.

In addition to providing users' with a full copy of Grindr's Privacy Policy in the App, the description of the App in app stores contained clearly distinguishable and intelligible information on advertising and a link to the Privacy Policy. As the Privacy Policy is available online, the information was easily available to the users also before downloading the App.

Throughout Grindr's history, the user voluntarily decides what, if any, information to include in their profile.[6] Optional profile information may include a public profile picture or other information the user may elect to provide, including a range of optional public profile attributes such as height, weight, and age. The App settings also offer a number of additional privacy options, including controls that allow the user to decide whether they want to show their relative distance from other users (an ancillary option that does not impact that user's experience).

Because each user decides what, if any, information to include or not to include in their Grindr profile at any time, the information contained in any given profile can vary widely both for a single profile over time and across profiles. All information displayed via a user's profile is widely accessible by all other Grindr users. As disclosed in Grindr's T&Cs, Grindr does not review or verify the information a user may provide when creating an account or completing a profile.

1.2.5 Grindr's previous consent mechanism

When a user first signed up for a Grindr account, they were provided with multiple disclosures regarding the sharing of their data with third advertising partners and opportunities to opt-in to the personal data collection and sharing that is central to the App experience.

[6] The App has no barrier to entry and is thus "*public*".

(i) the operating system with advertising preference selections;[7]

The Google Android and the Apple iOS platforms are designed to permit the user to make advertising preference selections that will apply to all apps on their device. In this regard, the Privacy Policy informs users that their mobile device platforms offer these types of native preference selections and explains that the operating system settings are designed to give users granular control over impact on the type of advertising that the user receives and the type of information shared with advertising partners.

If the user withdraws their consent for sharing information for advertising purposes by adjusting their device settings, advertising partners will only have access to basic technical information required to deliver the ad to the user's device (such as app operating system, device type, etc.), but Grindr will not share users' personal data with advertising partners.

(ii) the description of the App in the online store, as this contained information on advertising and a link to the Privacy Policy;

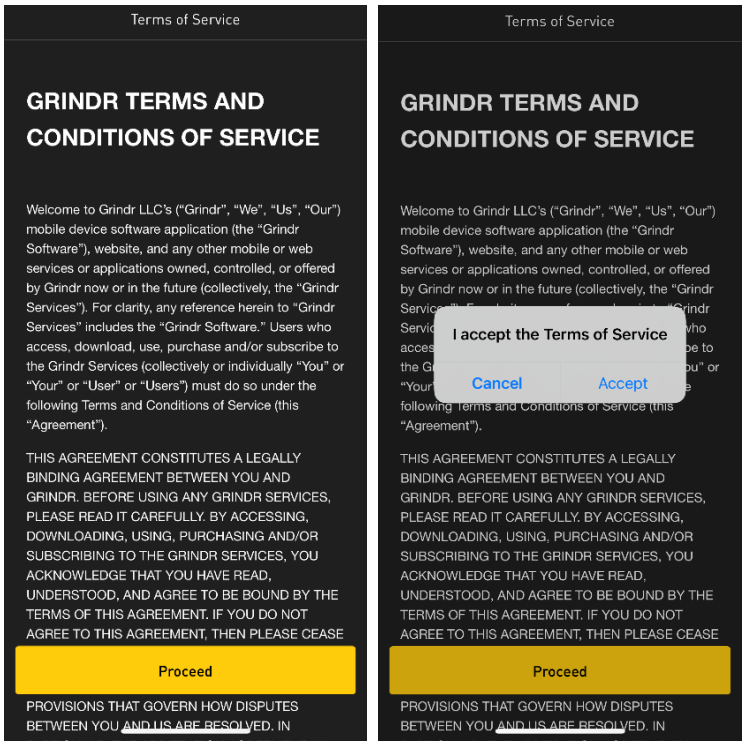
Grindr's notice in the Google Play Store and Apple App Store at the time of NCC's investigations included the following key information:

> *"[..] Grindr XTRA subscription features include: • No banner ads • See 6x the profiles, up to 600 at once • View only people who are online now • View only profiles with a photo • Unlimited blocks and favorites • Access to all premium filters • Chat easily with saved phrases • Send multiple photos at once Grindr has someone for everyone. [...] If you are experiencing any issues, you can get support by contacting us through https://help.grindr.com/hc/ Terms of Service: http://www.grindr.com/terms-of-service/ Privacy Policy: http://www.grindr.com/privacy-policy/ Grindr and Grindr XTRA are for adults 18 years and older only."*

Once the user accepted this notice (which even includes language on advertising and a link to the Privacy Policy) and downloaded the App, the user was given the option to consent to the processing of personal data for advertising purposes.

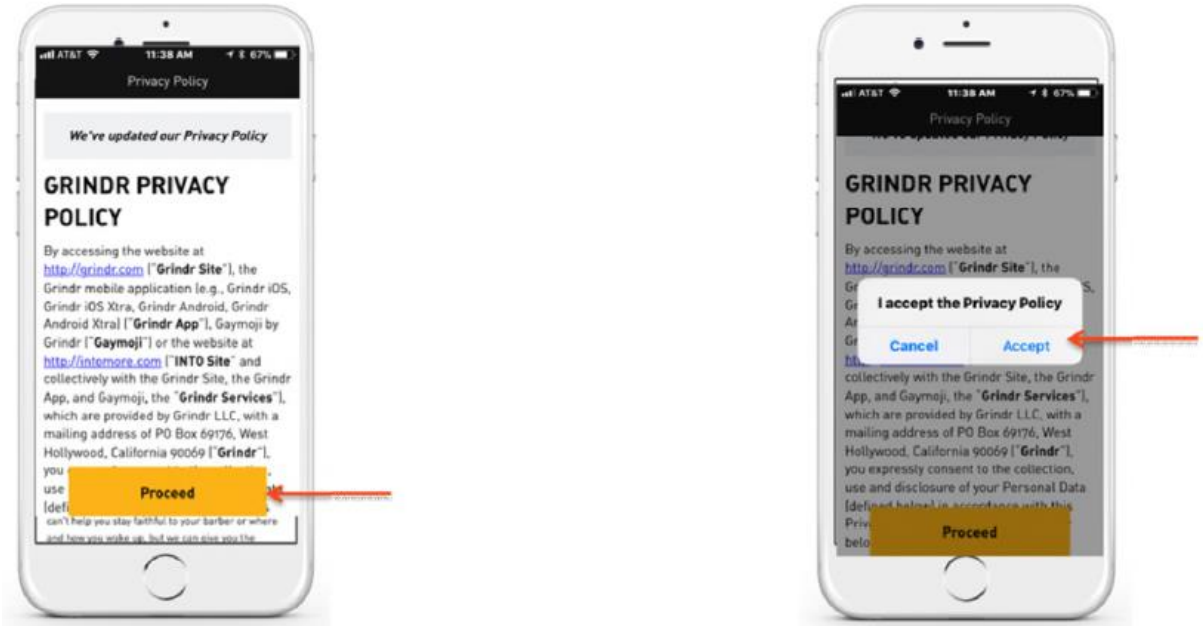
(iii) through the T&Cs, which contained a link to the Privacy Policy, for which users must take the affirmative action the click "Proceed" in order to reach the consent page;

[7] Although an opt-out solution provided by the device's operating system was not itself an independent elicitation of consent, the totality of the information presented by Grindr to the users clearly show that the consent was valid under Article 6.



(iv) through separately consenting to the T&Cs by clicking "*Accept*";

(v) through the Privacy Policy, for which users must take the affirmative action the click "*Proceed*" in order to reach the consent page;



(vi) through the separate ask to opt-in to processing activities that require consent by clicking that they "*accept*" such specific practices described in the Privacy Policy.

This process evidences that Grindr's sharing of data with advertising partners was very visible to the user, striking the appropriate balance with the user experience and complying with evolving laws, regulations, and guidelines from EU and local authorities at that time.

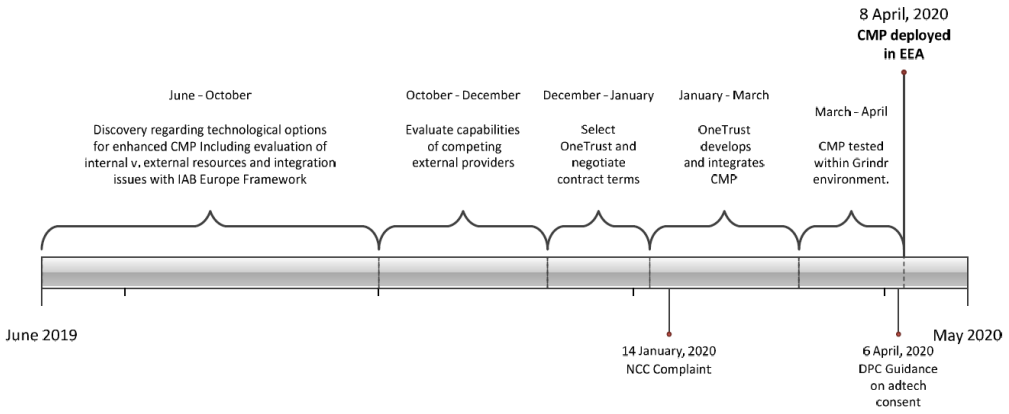
After displaying the full Privacy Policy, containing clear and plain information about advertising, users were asked to confirm that they were finished reviewing the text by clicking an icon to "*proceed*". Users were then separately asked to opt-in to processing activities that require consent by clicking that they "*accept*" the practices described in the Privacy Policy. The Privacy Policy is available for review anytime within the App's Settings->Privacy Policy menu.

At the time, and to this day, many well-regarded companies such as Tinder and Match, just to name a few, present the ***link*** to their privacy policy in grey, not the entire text of the privacy policy itself.

Grindr, together with its legal advisors, periodically reviews standards and practices within the social networking industry. Grindr's historic approach to transparency and consent exceeded the industry's privacy practices, and continues to do so today.

1.2.6 Grindr's current consent mechanism

In June 2019, at Grindr's own initiative as part of its ongoing commitment to fine-tune its privacy practices, and well before the issuance of the NCC Complaint, Grindr launched work streams to provide users with additional disclosures and greater granularity through a new CMP. After evaluating internal capabilities and external alternatives regarding Grindr's consent mechanism, Grindr negotiated and then entered into a contract with OneTrust, an industry-leading CMP. Although Grindr was one of the early adopters of OneTrust at the app level, OneTrust's CMP has become an industry leading tool that supports publishers' compliance with various regulations, including the CCPA, GDPR, ePrivacy, IAB Europe TCF v2.1, DAA AdChoices, and many others. Grindr invested extensive engineering resources to deploy the OneTrust CMP as part of its ongoing commitment to the Company's ever-evolving privacy practices. The following timeline summarizes the development and deployment of the current CMP:

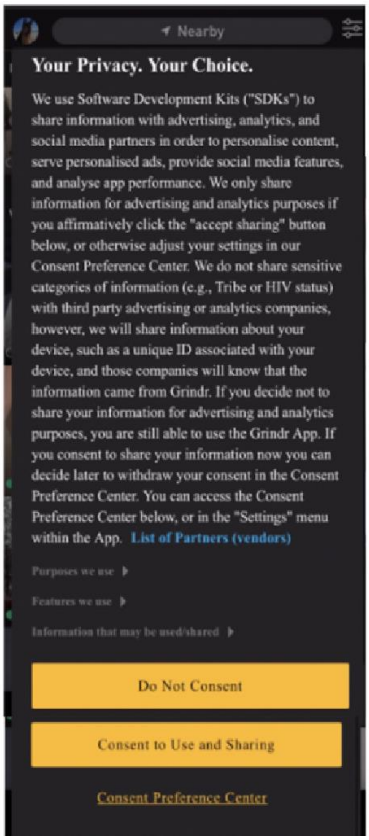


The current CMP was initiated well before the issuance of the NCC complaints in January 2020 and Datatilsynet's Order To Provide Information of 24 February 2020. With the new

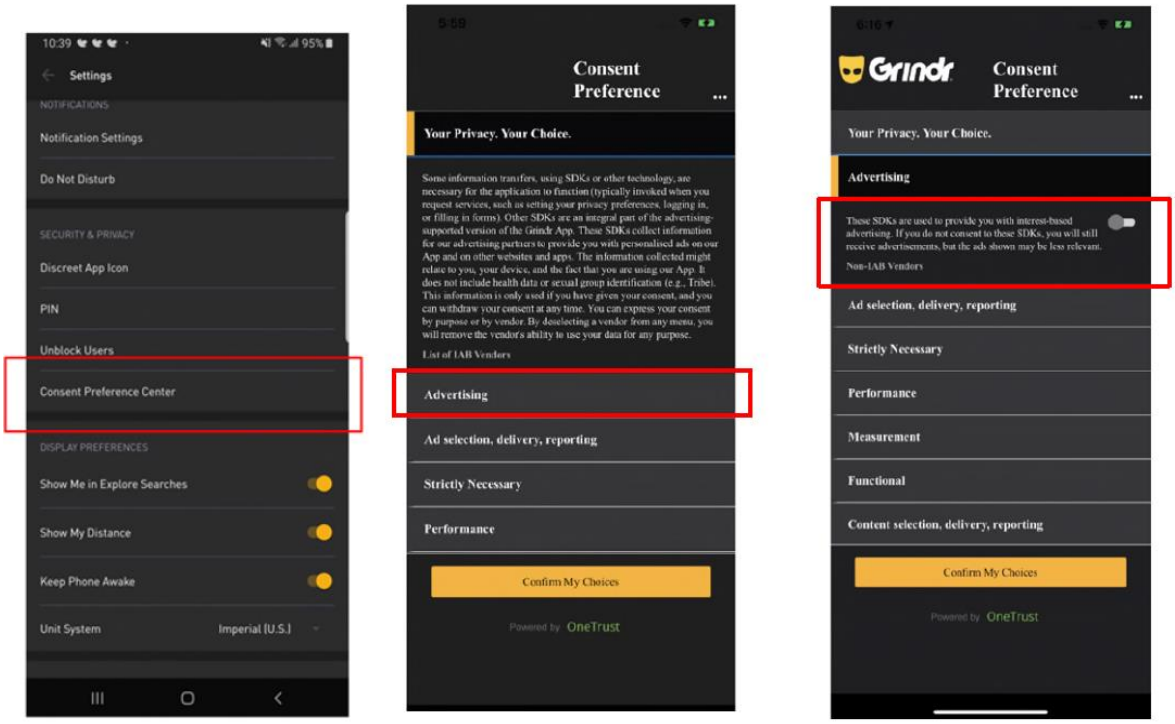
CMP, users are provided with a layered set of choices and information regarding the sharing of personal data through software development kits ("**SDKs**") and for advertising purposes.

Through the current CMP, users are presented with granular controls regarding their privacy settings and processing activities that would satisfy even EDPB's interpretation of consent. As seen in the screenshots below, prior to the collection of data, users are presented with a consent banner which allows them to confirm the default no consent/opt-out status by clicking "*Do Not Consent*", opt-in to non-required SDKs by clicking "*Consent to Use and Sharing*" or seek more information by clicking "*Consent Preference Center*".

User's consent is not presumed, or set to a default opt-in position (the default position used is "*no consent*"), nor are the users directed, pushed, influenced, or "*nudged*" to provide their consent. The "*Do Not Consent*" option is provided in the same font, color, and size as the option to "*Consent to Use and Sharing*." Indeed, the "*Do Not Consent*" option is provided with greater prominence than the consent option as it is presented as the first option to the data subject. The second screenshot depicts what a user is presented when they select "*Consent Preference Center*" in the App.



The screenshots below illustrate Grindr's Consent Preference Center, which EEA users can access at any time from the "*Settings*" menu from within the App. Through the Consent Preference Center, a user has access to additional information about the purpose of the separate SDK types, such as "*Advertising*" and may choose to opt-in or opt-out on a per SDK category basis.



In addition to following best practices of ensuring that the options presented to users are not designed to encourage consent, users that decline to consent are still permitted to use the App in the same manner as users that accept the sharing of data.

In addition, in December 2020 as part of Grindr's never-ending commitment to enhancing its privacy practices, the Company launched its new layered format of its Privacy Policy, providing the same thorough disclosures, first in a succinct 4.5 page primary layer that describes the essentials of Grindr's information collection and sharing practices and giving users the ability to easily navigate and learn more detailed information about the nuances of Grindr's privacy practices. As before, the Privacy Policy is presented to the user for review in its entirety, the user must click proceed, and then elect to opt-in to accept the policy and the processing activities.

1.2.7 TCF and the evolving concept of consent among Industry and Regulators

When looking at a company's historical practices, as Datatilsynet is doing here, it is important to remember that the understandings regarding the nuances of the GDPR have evolved since it was announced in 2016 and entered into effect in 2018. Implementation of the GDPR has been an ongoing journey for companies, governments, and regulators alike. Some five years since its passage, there are still many nuances that need to be clarified in the interpretation of the GDPR. This is also seen by the fact that regulators themselves issue new guidelines and review old guidelines.[8] Thousands of articles have been written about the lack of clarity in many elements of the GDPR, and some of the most discussed are the details and nuances surrounding the definition of consent under Article 4.

[8] In less than 2 years, the European Data Protection Board issued more than 20 sets of Guidelines (exceeding a total of 500 pages) interpreting the GDPR, not including the 16 endorsements of older Working Party 29 Guidelines.

Early on, and to this day, the online advertising industry recognized it was going to take far-reaching collaboration across all facets of the ad tech ecosystem to address the perception of the needs defined under the GDPR. Leaving aside the discussions of what "*legitimate interest*" processing may be used for as a legal basis, the IAB Europe[9] quickly began work on a technical standard and operational approach that would allow publishers to collect consent and pass these details into the ad ecosystem so that all further processing occurred in a legally compliant manner. Nearly a hundred companies participated in the development of version 1.1 of the Transparency and Consent Framework (the "**TCF**"), which was released just prior to May 2018.

It took time for the industry to implement the new TCF standard, including to connect the dots of data custody to ensure that consent details travelled through the entire ad delivery chain – from the publisher all the way through to ad delivery. Grindr's initial consent mechanism strived to follow industry practice on implementing version 1.1 of the TCF.

So while companies had two years between the GDPR's passage to it becoming effective, even weeks before May 2018, it was still unclear whether the ad tech industry as a whole would support TCF or, if it was supported, how it would be fully implemented. Thus, small companies with a fraction of the engineering or other resources were left to make best efforts towards compliance. Grindr's best efforts included the industry leading practice of providing users with clear and transparent description of its practices in its Privacy Policy, presenting the entire text of that policy to its users, and eliciting explicit, opt-in consent to that policy and Grindr's practices.

Not only is the setup and implementation of the GDPR itself complex, it is only one layer of the onion with respect to legal compliance under the GDPR. In February 2019 the UK ICO started an investigation into the real-time bidding environment in online advertising. The UK ICO published its report in June 2019, and set forth a six month timeline for the industry to include their recommendations.[10] Along with the largest EU publishers and internet giants like Google, the TCF working group - now numbering in the hundreds of companies - started the development of version 2.0 of the industry standard. Although Grindr is not a party to the TCF working group, many of Grindr's advertising partners are.

In late August 2019, the IAB EU announced the release of version 2.0 for public comment and feedback. Questions abounded, and the UK ICO held a fact finding forum in November 2019. This helped address many, but not all, of the core open questions as the industry moved forward with starting the work to build out version 2.0 and transition from version 1.1. By this time, Grindr had already begun work transitioning to a third party CMP solution with OneTrust, as further described in section 1.2.6 above. The initial implementation of OneTrust was under version 1.1 and all of Grindr's EEA users gave their consent – or re-consent – according to this standard. Following the release of TCF version 2 and OneTrust

[9] IAB Europe is the European association for the digital marketing and advertising ecosystem. The IAB Europe Transparency and Consent Framework version 1.1 was launched on 25 April 2018, after extensive industry consultation with members of IAB Europe and IAB Tech Lab, and the broader digital advertising industry. "The IAB Europe TCF is the only GDPR consent solution built by and for the industry, giving it a true industry-standard approach." Available at https://iabeurope.eu/transparency-consent-framework/, visited 12 February 2021, and https://iabeurope.eu/about-us/, visited 23 February 2021.

[10] The UK Information Commissioner's Office, *Update report into adtech and real time bidding*, 20 June 2019, page 4 and 24.

building support for this new standard into their CMP solution in 2020, Grindr implemented this version in Q3 2020 and, again, Grindr's EEA users (re)consented under this new version.

The UK ICO continued to find some issues with the TCF version 2.0 approach, so a subsequent version 2.1 of the standard was released to address these remaining issues, which Grindr now supports in its present consent flows.

Throughout these iterations, many of the ad tech companies operating in the EU devised "*blinding methods*" to obfuscate which app the ad call is coming from. The obfuscation included both downstream partners and the advertising partners' own internal systems.

In the EU, this blinding method results in ads that are not contextually aware of the App and therefore will show more generic ads for gaming and retail apps. As the App is blinded on entry to the ad tech platform it also removes the capability for the device to be profiled as a Grindr user.

Grindr realizes that even now the consensus around privacy practices will continue to evolve, and there are a series of significant technical changes to the platforms that will evolve in parallel, including new tooling and approaches adopted by web browsers and mobile operating systems.[11] Grindr continues to monitor the situation and adapt its approach to consent via OneTrust as regulators and industry groups work together to build consensus and add coverage for emerging questions or concerns.

1.3 Data shared with advertising partners at the time of the alleged infringement

From the Advance Notification, one may get the impression that Grindr has shared user sexual orientation data with advertising partners. This is simply not accurate.

The only categories of personal data shared with advertising partners during the period of the alleged infringement were:

1. Advertising ID provided by the mobile operating system (and under full user control), IP Address, and information about the computing environment (operating system version, model, screen resolution, etc.) (Collected by the SDK, not pushed by Grindr);
2. Self-Reported Age (in whole years);[12]
3. Gender;[13] and

[11] For example, Apple's newest iOS 14 provides users with greater control over third party data collection and over the relative precision of location information shared with app developers.

[12] At account creation, users are prompted to enter their date of birth to validate that they are a legal adult. Grindr does not verify if the self-reported age is accurate and only stores the user's age in whole years. A user can later change their age in their profile to anything between 18-99.

[13] In the Grindr App, users have a wide variety of option to express their gender such as man, woman, cis man, cis woman, trans man, trans woman, non-binary, non-conforming, queer, crossdresser, or custom. Users could change their gender identity in their profile at any time. Importantly, Grindr would only provide gender in an ad call if it matched either "male" or "female" - the other options were not shared with advertising partners.

4. Location (Collected by the SDK and only if the user has both allowed location services on their device and has provided express consent to the Grindr App to access their location).

Datatilsynet points to one single advertising partner, OpenX that pulled the description of the App from the online store and passed this along with ad calls. These *were not keywords generated or shared by Grindr* to OpenX.

Datatilsynet seems to base its decision on that Grindr is sharing the keywords "*gay, bi, trans and queer*" with advertising partners, but these keywords are not part of the information that Grindr shares. Datatilsynet apparently references the Mnemonic report that displays the keywords that were part of the report's technical study of an OpenX request parameter that apparently was generated *by the OpenX SDK*.[14]

The words "*gay, bi, trans and queer*" that were in the OpenX ad call did not describe any individual user's sexual orientation. Rather, the ad requested from the SDK was appended with keywords that were associated with the App. No information on sexual orientation was ever shared.

Grindr itself did not and does not share the keywords "gay, bi, trans and queer" with advertising partners.

We note that with the current CMP, the only information that is shared is basic data to carry out the functionality of the ad to function (Advertising ID, devise OS, etc.).[15]

1.4 Excerpts from the privacy notice

Much of the Advance Notification centers on Datatilsynet's argument that Grindr did not obtain sufficient consent from its users. Before addressing the substance of those arguments, it is important to outline just how much transparency and disclosure Grindr provided to its users and the extensive efforts Grindr undertook to explain to users what they were consenting to, how they could withdraw that consent, and how their personal data was used.

It is essential to note that every Grindr user acknowledges that they had 1) read the Privacy Policy, including the excerpts below and 2) accepted the Privacy Policy in a separate screen where it was as easy to click "*accept*" as it was to click "*cancel*".

Datatilsynet has used some excerpts from Grindr's Privacy Policy in the Advance Notification, but there are many more elements that are relevant to this matter, some of which are set out below:

Grindr encouraged its users to carefully read the Privacy Policy:

[14] By way of background, when an ad is to be displayed, the App will make a call to the ad SDK, and the SDK collects information from the mobile operating system and passes the information to the SDK partner's own servers. The ad SDK will "service the ad" front her partner's advertising partners.

[15] Age and gender are no longer shared with advertising partners.

As a global LGTBQ social networking application, the Grindr App allows you to share sensitive information about yourself, including your sexual orientation and precise location, with us and other Grindr users. ***This Privacy and Cookie Policy also explains how you can control your personal data****. We recommend you read this Privacy and Cookie Policy, and our Terms and Conditions, carefully.* ***You can also use the links below to jump to specific information concerning our privacy practices.***

Grindr explained how users control the location information they share with Grindr:

Personal Data We Receive When You Use Grindr Services

Location and Distance Information. […] ***Should you choose not to allow the Grindr App to access your Location, certain features (such as displaying nearby user profiles or features that include Live Location Sharing) of the Grindr Services will not function properly. You may also revoke this permission and disable the location services on your device.***

Grindr explained that data is shared with advertising partners and that advertising partners collect data:

Personal Data We Receive From Third Parties

Third-Party Tracking. ***Our advertisers and certain service providers also use their own cookies or other tracking technologies*** *(such as software development kits or "SDKs") which may collect information about you within the Grindr Services.*

Grindr explained how data is used and which legal basis that use is based on:

How And Why We Use Your Personal Data

In order to provide the Grindr Services and facilitate connections with the community, ***we use your Personal Data for the purposes described below****. Please note that even if we are not relying on consent to use your Personal Data, we may ask you for permission to access your device for Personal Data such as photos and location.* ***Under E.U. and U.K. data protection laws, we may only use your data when we have a lawful basis to do so. The table below provides an overview of the legal bases on which we rely. Where the legal basis is consent, you can withdraw your consent at any time (typically by controlling what data you provide in your Grindr community profile). Where the legal basis is legitimate interests, you have a right to object to our use of your data. We explain in the relevant sections in this Privacy Policy how you can withdraw consent or opt-out of certain data uses.***

21. Share your Personal Data with our advertising partners.	***Personal Data we collect from you, including: Hardware and Software Information; Profile Information[16] (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.***	***Consent***
22. Provide or show advertising on the Grindr Services based on the Personal Data you provide or that we collect through the Grindr Services.	***Personal Data we collect form you, including: Hardware and Software Information; Profile Information[17] (excluding HIV Status, Last Tested Date, and Tribe); Location and Distance Information; Cookies, Log Files and Other Tracking Technologies. Additional Personal Data that we receive about you, including: Payment Information and User Activity.***	***Consent***
23. Process your Personal Data to provide personalized advertising.	***Personal Data we collect from you, including: Hardware and Software Information; Profile Information[18] (excluding HIV Status, Last Tested Date, and Tribe); Location and Distance Information; Cookies, Log Files and Other Tracking Technologies.***	***Consent***

[16] Only age (in years, not birth date) and gender.

[17] Only age (in years, not birth date) and gender. Grindr no longer shares that information with advertising partners.

[18] Only age (in years, not birth date) and gender. Grindr no longer shares that information with advertising partners.

Grindr explained how data is shared:

How We Share Your Personal Data
We share Personal Data in the following situations: • *Distance Information. […]* ***Please note, you may choose to hide your Distance Information; however, the Grindr App will continue to sort and display your profile based on your relative distance from other users. Accordingly, even if you choose to hide your Distance Information, others may nevertheless be able to determine your Location. You can disable location services on an iPhone by going to settings, privacy, location services, Grindr and on Android, by going to settings, location, Grindr, permissions, location.*** • *Third-Party Advertising Companies.* ***We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Location Information, and same of your demographic information with our advertising partners. These third parties may also collect information directly from you as described in this Privacy and Cookie Policy through tracking technologies such as cookies. The privacy policies of these third-party companies apply to their collection, use and disclosure of your Personal Data. One of these advertising partners is MoPub that helps Grindr deliver personalized advertising. You can follow the links to MoPub's privacy notice and partner page. See the YOUR CHOICES section of this Privacy and Cookie Policy for information on your ability to apt-out of interest- based advertising.*** *Note that we do not share information about your Tribe, your HIV status [or your Last Tested Date] with any advertising companies.* ***For more information on third-party tracking technology, please visit Cookie Information below****. […]*

Grindr explained how users may control the processing of data:

Your Choices
You can make the following choices regarding your Personal Data: • *[….]****If you do not want third parties to collect information about your use of the Grindr Services, or your affiliation to Grindr, or to tailor any of the advertising that you see, you can apt out from same third party behavioral advertising at the Digital Advertising Alliance in the US, the Digital Advertising Alliance of Canada in Canada, or the European Digital Advertising Alliance in Europe. Please note that opting-out of behavioral advertising does not mean that you will not receive advertising while using the Grindr Services. It will, however, exclude you from interest-based advertising conducted through participating networks, as provided by their policies and choice mechanisms.***

Grindr explained how users may withdraw consent:

Your Rights
Subject to certain conditions, you may ask us to: • *[….]* • ***Withdraw consent that you have previously given us. You may make this request at any time. Note that revocation of your consent will only apply to future processing activities and will not apply retroactively.*** • *[…]*

Grindr explained how users may control cookies:

How can you control cookies?
[…] ***You also may be able to configure your browser settings to use the Grindr Services without the same cookie functionality. You can delete cookies manually or set your browser to automatically delete cookies on a pre-determined schedule. For example, in the Internet Explorer menu bar, select: Tools -> Internet Options -> Browsing History -> Delete to view manual and automatic options.*** **To** ***learn about how to manage cookies on popular browsers, please visit the links below: Apple Safari, Google Chrome, Microsoft Edge, Microsoft Internet Explorer, Mozilla Firefox*** **You** ***may also be able to reset device identifiers through settings on your mobile device. The procedure for managing device identifiers if different for each device. You can check the specific steps in the help or settings menu of your particular device.*** • *Interest-based Advertising.* ***You can opt out of seeing online interest-based advertising through the Digital Advertising Alliance in the US, the Digital Advertising Alliance of Canada in Canada, or the European Digital Advertising Alliance in Europe. Please note that opting-out of behavioral advertising does not mean that you will not receive advertising while using the Grindr Services. It will, however, exclude you from interest-based advertising conducted through participating networks, as provided by their policies and choice mechanisms. You may also reset your advertising identifier on your device, or use the AppChoices app, or turn off location tracking. We do not currently recognize automated browser signals regarding tracking mechanisms, which many include "Do Not Track" instructions.*** • *Google TM Analytics Cookies. We use Google Analytics, a Google service that uses cookies and other data collection technologies, to collect information about your use*

> *of the Grindr Services.* ***You can opt out of Google Analytics tracking by clicking here or by downloading the Google Analytics opt-out browser add-on here.***
>
> - *Flash Cookies. We may also use Flash cookies (also known as "persistent identification elements" or "local shared objects") on certain websites. Because Flash cookies cannot be controlled through your browser settings,* ***you may click here to adjust your preferences.*** *You can also identify Flash cookies running on your computer by visiting the Flash Player folder. Flash cookies, or LSO files, are typically stored with a ".SOL" extension. Please note that if you block cookies, s**o**me functions on the Grindr Services may be unavailable, and we may not be able to present you with personally-tailored content.*
>
> *How we share.* ***You agree and consent that the information and data outlined above may be shared with third parties as described throughout this document.***

Consequently, there is no doubt that Grindr has made a comprehensive effort to inform its users of how personal data is used, that the use is based on consent where necessary/appropriate, and that consent could be withdrawn without any detriment at any time. Users could also opt-out from their device if they do not allow Grindr to share their Advertising ID.

2. COMMENTS TO DATATILSYNET'S ASSESSMENT OF THE CASE

2.1 Principles of legal certainty and sources of law

In order to impose intrusive administrative sanctions, such as an administrative fine, the principle of legal certainty must be satisfied.[19]

As stated by the EFTA Court in its judgement in Case E-9/11, the principle of legal certainty is *"a general principle of EEA law (see, inter alia, Case E-1/04 Fokus Bank [2004] EFTA Ct. Rep. 11, paragraph 37)*".[20] The EFTA Court further states that "*while the principle of legal certainty does not preclude the conferral of discretionary powers on the competent authorities*", such powers "*must be based, as a general rule, on objective, non-discriminatory criteria which are known in advance to the undertakings concerned*".[21] Under the GDPR, recital 41 explicitly states that legal basis under national law "*should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights*". The principle of legal certainty in the European Convention on Human Rights applies as an administrative fine is deemed to be a penalty under Article 6.[22]

The principle of legal certainty is also established in Norwegian administrative law, and requires a clear legal basis to impose intrusive administrative sanctions, such as an

[19] No: "Legalitetsprinsippet".
[20] Case E-9/11 page 29 paragraph 99.
[21] Case E-9/11 page 30 paragraph 100.
[22] Rt. 2012 page 1556.

administrative fine.[23] The principle is relative; the requirement to the legal basis depends on the nature and intrusiveness of the sanction.[24]

The administrative fine that Datatilsynet intends to impose against Grindr would be one of the highest administrative fines imposed for breach of the GDPR within the EEA, relatively. Reference is made to the overview in Appendix 1.

Due to the highly intrusive character of the administrative fine proposed, the requirement to the legal basis under the principle of legal certainty is raised, and Datatilsynet must give due regard to the principle. We do not see that this has been done. We note that Datatilsynet's reasoning for the amount of the proposed administrative fine is on one page and does not show any aggravating factors justifying the intrusiveness of the historic administrative fine or the deviations from established practice within the EEA.

Additionally, in the Advance Notification, Datatilsynet interprets the GDPR in light of the European Data Protection Board Guidelines 05/2020 on consent and 8/2020 on the targeting of social media users, and Kuner, Bygrave and Docksey, *The EU General Data Protection Regulation (GDPR), A Commentary*, 2020. In this context it is important to note that the EDPB's guidelines have limited value as source of law, even though it may provide guidance as an expression of administrative practice by EU data protection authorities **("DPAs")**, and that one does not use interpretations or guidelines published after the relevant facts.[25]

---

[23] See the following cases from the Privacy Appeals Board: PVN-2020-13, PVN-2017-3, PVN-2013-9, PVN-2013-20, PVN-2013-5, PVN-2013-8, PVN-2013-10, PVN-2013-11 and PVN-2013-12. The questions for the Privacy Appeals Board in these cases were not regarding the issuing of an administrative fine, but if a certain paragraph could be used for issuing an instruction. However, if the ambiguousness of a paragraph is the reason for one not being able to issue an instruction, the same level of ambiguousness in another paragraph cannot be used for imposing an administrative fine.

[24] Rt. 1995 s. 530 page 573.

[25] PVN-2020-14: Norwegian: "*Nemnda legger til grunn at Personvernrådets veileder, i likhet med Artikkel 29-gruppens veileder, har begrenset verdi som rettskilde, men gir nyttig veiledning som uttrykk for forvaltningspraksis hos tilsynene i EU og EØS."PVN-2019-02: Norwegian: (...) Erfaringsmaterialet som ligger til grunn for retningslinjene er med andre ord nokså begrenset. Samlet sett tilsier dette varsomhet med å legge altfor stor vekt på retningslinjene. Artikkel 29-gruppen har også selv forutsatt at listen over kriterier «will evolve over time, building on the experience of DPAs». Etter nemndas oppfatning er det altså ikke grunnlag for å mene at retningslinjene har stor juridisk vekt. Nemnda finner her grunn til å vise til at heller ikke EU-domstolen bygger interesseavveiningen i G.C. & Others v NCIL på Artikkel 29-gruppens retningslinjer. Domstolen nøyer seg i avsnitt 66 med å konstatere at det skal foretas en interesseavveining og gir en nokså løselig anvisning på hvilke momenter som skal inngå i denne avveiningen: (...) Nemnda ser det likevel slik at retningslinjene fra Artikkel 29-gruppen spiller en viss rolle i den interesseavveiningen som skal foretas. De kan likevel bare vektlegges så langt de har relevans for den aktuelle saken, og en nærmest mekanisk anvendelse av alle 13 kriteriene ved avgjørelsen av saker om sletting av søketreff innebærer en risiko for at man taper den overordnede interesseavveiningen av syne. (...)"*

English office translation: *The Privacy Appeals Board in PVN-2020-14: "The Board assumes that the Data Protection Board's guide, like the Article 29 Working Party's guide, has limited value as a source of law, but provides useful guidance as an expression of administrative practice in EU and EEA." The Privacy Appeals Board in PVN-2019-02: "(...) The empirical material on which the guidelines are based is in other words rather limited. Overall, this indicates that caution should be used in placing too much emphasis on the guidelines. The Article 29 Working Party has also assumed that the list of criteria "will evolve over time, building on the experience of DPAs". In the Board's opinion, there is thus no basis for believing that the guidelines have great legal weight. The Board finds reason here to point out that the European Court of Justice does not base the balancing of interests in G.C. & Others v NCIL on the Article 29 Working Party's guidelines. In paragraph 66, the Court confines itself to stating that a balancing of interests must be carried out and provides a fairly loose instruction as to which elements are to be included in this balancing: (...) The Board nevertheless finds that the guidelines from the Article 29 Working Party play a certain role in the balancing of interests to be carried out. However, the guidelines can only be emphasized as far as they are relevant to the case in question, and an almost mechanical application of all 13 criteria when making decisions in cases on deletion of search results entails a risk of losing sight of the overall balancing of interests. (...)*"

The above entails that, as a threshold matter, Datatilsynet must point at an infringement of an unequivocal legal requirement in order to impose a sanction of the warned size. As we will revert to, we do not find that the wording of the articles in question have the necessary amount of clarity, and hence Grindr may not be fined as suggested by Datatilsynet.

2.2 Grindr's consent mechanism was compliant with Article 6

2.2.1 Introduction

Datatilsynet is wrong when stating that Grindr has failed to obtain consent for sharing personal data for advertising purposes.

Grindr has clearly implemented consent procedures, and the legal question is only if the finer requirements of EDPB's guidelines on consent, which are not legally binding, were satisfied during the period of time of the alleged infringement.

Grindr is a small player in a large ad environment. Privacy practices and requirements evolve. As Datatilsynet is undoubtedly aware, even Apple has recently evolved on this topic, switching to an opt-in model in its new OS 14. Grindr's previous CMP and privacy practices must be assessed in light of the then-current norms and privacy practices in the ad tech environment, including the data subject's privacy choices made at the operating system level. Grindr's layered consent mechanism ensures privacy measures in compliance with GDPR requirements, and Grindr's practices have evolved in recent years to provide even greater control from within the App (as well as at the device level).

Grindr's Privacy Policy is highly transparent, it uses clear and plain language about the categories of data and the purposes of the sharing. In addition, the relevant legal basis for the different processing activities are listed in a clear and distinguishable manner.

It is important to note that the user needs to make independent choices (opt-ins) at the operating system level, e.g., whether to give location information to Grindr. Therefore, the processing does not start automatically when the user pushes "*I accept the Privacy Policy*".

To conclude, the use of the free version of the App not only requires the user's acceptance of the Privacy Policy in the App but relies on choices made in the operating system as well.

2.2.2 Grindr's collection of consent according to Article 6(1)(a)

As explained in section 1.2.5, Grindr's previous consent mechanism incorporated the following process:

(A) Grindr provided users with its full Privacy Policy as part of creating an account.

(B) After displaying the full Privacy Policy, users were asked to confirm that they are finished reviewing the text by clicking an icon to "*proceed*", unbundled from acceptance to any other legal document.

(C) Users were then separately asked to opt in to processing activities that require consent by clicking that they "*accept*" such specific practices described in the Privacy Policy.

Grindr thus collected a double-consent requiring two positive actions. A first affirmative action to proceed upon receiving the Privacy Policy, and a second affirmative action to consent to each privacy practice that requires consent.

This process complies with Article 6(1)(a) and the TCF of IAB Europe.

Further, as explained in section 1.2.5, besides the double-consent, the user had several opportunities not only to get acquainted with the different processing activities, including the ones related to data sharing with advertising partners as described in the Privacy Policy, but also to opt-out in the mobile device's operating system, see reference to the text from the Privacy Policy below:

> *"Should you choose not to allow the Grindr App to access your Location, certain features (such as displaying nearby user profiles or features that include Live Location Sharing) of the Grindr Services will not function properly. You may also revoke this permission and disable the location services on your device."*

In addition, the Privacy Policy, in its section "What We Collect", presents types of data, how the data is collected and, specifically, the different *purposes* of collecting the data. The data collected and associated purposes are provided clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

Grindr asked users to read and accept easily accessible information about sharing personal data for advertising purposes.

In this way, Grindr did appropriately satisfy its obligations of eliciting consent.

2.2.3 Freely given

Grindr's previous CMP complied with Article 4(11) – "*freely given*".

The data subject was presented with easily accessible information about sharing of some specific categories of data for advertising purposes. This information was clearly distinguishable from the other processing activities listed in the privacy policy and presented in a clear and plain language. The Privacy Policy was not bundled with the T&Cs.

The user was not "*nudged*" to proceed without familiarizing themselves with the provided information – they were explicitly urged to read through the given information.

<u>Granularity</u>

Datatilsynet states that "*consent requests were bundled with other processing operations and other purposes*" and that "*consents to sharing personal data with advertising partners were not given 'freely'*".

Datatilsynet refers to the "legal requirement of granularity"[26] as a condition for considering that consent is freely given.

[26] See Advance Notification, p 25 "The legal assessment of "freely given", inter alia the requirement of granularity",

In its Advance Notification, Datatilsynet refers to paragraphs 55 and 60 of the EDPB guidelines on consent. Those guidelines state:

> *"Article 6(1)(a) confirms that the consent of the data subject must be given in relation to "one or more specific" purposes and that a data subject has a choice in relation to each of them. The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time, it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent. In sum, to comply with the element of 'specific' the controller must apply:*
>
> > *i) Purpose specification as a safeguard against function creep,*
> > *ii) Granularity in consent requests, and*
> > *iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters."*
>
> *"Consent mechanisms must not only be granular to meet the requirement of 'free', but also to meet the element of 'specific'. This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes."*

Datatilsynet is of the view that the controller needs to provide a separate opt-in for each purpose, stating:

> *"The EDPB has also stated that a controller who seeks consent for various different purposes should provide a separate "opt-in" for each purpose, to allow users to give specific consent for specific purposes, i.e. granularity in consent requests. As discussed under Section 5.1.1, we have concluded that Grindr did not provide separate "opt-in" for each purpose."*

The tasks of the EDPB are set out in Article 70. The EDPB shall inter alia "issue guidelines, recommendations and best practices in order to encourage consistent application"[27]. The EDPB mentions on its website[28]:

> *"We issue general guidance to promote a common understanding of European data protection laws, both across the European Union and around the world.*
>
> *We clarify data protection provisions, advise the European Commission and provide the general public and stakeholders with our interpretation of their rights and obligations.*
>
> *We can issue guidelines, recommendations and best practices about the GDPR and the Law Enforcement Directive, as well as other documents*".

[27] Article 70(1)(e)
[28] https://edpb.europa.eu/our-work-tools/general-guidance_en

Consent is defined in Article 4(11). The conditions for obtaining valid consent are set out in Article 7. However, the "legal requirement of granularity" referred to in the Advance Notification is not even mentioned in the GDPR. Granularity is neither a legal requirement nor one of the conditions for obtaining a consent under the GDPR. Granularity is just the result of the EDPB's own interpretation of the requirements for a valid consent.

For this reason, the implementation of these recommendations, which are the result of the EDPB's own interpretation of the GDPR, is not required by law. The non-adherence by a controller to a specific EDPB recommendation constructed around the EDPB's own interpretation of the GDPR should not be understood as a breach of the GDPR.

While Grindr recognizes the positive value of such guidelines, Grindr is of the view that neither the EDPB guidelines nor the guidelines issued by any other data protection authority create legal rights or legal obligations for anyone. EDPB Guidelines should be considered as 'soft law', just like any other opinions, recommendations and the like of administrative agencies.[29] Soft law is a well-known concept in European law and has extensively been described in legal doctrine.[30] *S*uch guidelines are solely intended to guide the practices of different market players but are "non-binding", as pointed out by Advocate-General Szpunar in his opinion in the Planet 49 case.[31] Guidelines can increase legal certainty as the regulator clarifies how it interprets the legislation. However, such soft law is not binding for the interpretation of GDPR, as explicitly stated in the Treaty on the Functioning of the European Union Article 288, and clearly implied in the EEA Agreement Article 7.

We also refer to The Privacy Appeals Board in its decision PVN-2020-14, which states that: "*The Board assumes that the Data Protection Board's guideline, like the Article 29 Working Party's guideline, has limited value as a source of law, but provides useful guidance as an expression of administrative practice in EU and EEA."*

Specifically, such guidelines cannot be used as a basis for Datatilsynet's conclusion that consents to sharing personal data with advertising partners were not given 'freely'. Further, such guidelines cannot be used as a basis for imposing an administrative fine of the warned size.

Furthermore, under the GDPR, it is possible to obtain consent to a set of processing activities as long as the data subject receives the specific information to each of the purposes of the data processing in advance. There are relevant court decisions in this regard.

The Highest Administrative Court of France (the "**Conseil d'Etat**"), stated in its decision partially annulling the guidelines of CNIL on cookies and similar technologies[32] that "*the users' consent must relate to each of the purposes pursued by the data processing and any subsequent new purpose, compatible with the initial purpose(s), is subject to the collection of its own consent".*

[29] Groos, D. , & van Veen, E., "Anonymised Data and the Rule of Law", *European Data Protection Law Review*, Volume 6, Issue 4 (2020), pp. 503. See also Lynskey, O. "The Europeanisation of data protection law", in Cambridge Yearbook of European Legal Studies, (2016), 252-286.

[30] See for example Chalmers, D., Davies, G., Monti, G., European Union law, Cambridge University Press, 2019, 116-119.

[31] Opinion of Advocate General Szpunar, 21 March 2019, Case C-673/17, §81.

[32]Conseil d'État, Décision 434684, lecture du 19 juin 2020, ECLI:FR:CECHR:2020:434684.20200619

However, the Court recognized that *"compliance with such requirements implies at the very least that, in the event the collection of consent was carried out for a set of purposes, it would be preceded by information specific to each of the purposes"* (our office translation).[33] The Court did not refer to any obligation to implement separate opt-ins for a consent to be valid.

Grindr's previous consent mechanism is aligned with the decision of the Conseil d'Etat, as the information related to each of the purposes requiring consent was presented to the user before the consent request. This confirms that the user's consent to the processing was freely given.

In addition, the guidelines on cookies from CNIL, recommends asking for consent independently for each distinct purpose. However, CNIL considers that this recommendation "*does not preclude the possibility of requesting the users to consent to a set of purposes, subject to presenting all the purposes pursued in advance to the users*" (our office translation).[34]

For all the above, the fact that Grindr had not implemented the EDPB recommendation of providing separate opt-ins for each purpose during the period of the alleged infringement does not constitute a violation of the GDPR.

In the Privacy Policy at the time of NCC's investigations, Grindr presented the processing purposes as bullet points and separated from each other. Grindr's consent requests were bundled in a legally permissible way, and the obtained consents were freely given.

In the prior Privacy Policy, and in the current version, Grindr provides a clear, detailed description of the processing purposes and legal basis. Information related to each of the purposes requiring consent was presented to the user before the consent request. This confirms that the user's consent to the processing was freely given.

<u>Conditionality</u>
Datatilsynet maintains that *"gaining access to the Grindr services within the free version of the app seemed dependent on consenting to sharing personal data for marketing purposes. This implies breach of the element of conditionality.*"

Grindr offers its users a genuine choice between the free version of the App, which requires consent for the use of personal data for advertising purposes, and a paid version of the App. This is perfectly aligned with EDBP Guidelines on consent:

---

[33]Conseil d'État, Décision 434684, paragraph 18 "le consentement de l'utilisateur doit porter sur chacune des finalités poursuivies par le traitement de données et que toute nouvelle finalité ultérieure, compatible avec la ou les finalités initiales, assignée au traitement de données est soumise au recueil d'un consentement propre. Le respect d'une telle exigence implique à tout le moins, dans l'hypothèse où le recueil du consentement serait effectué de manière globale, qu'il soit précédé d'une information spécifique à chacune des finalités.

[34] Commission Nationale de l'Informatique et des Libertés, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs », paragraphs 25 et 26: 25. "25. Afin de s'assurer du caractère libre du consentement donné, la Commission recommande de demander aux utilisateurs leur consentement de façon indépendante et spécifique pour chaque finalité distincte. 26. Toutefois, la Commission estime que cela ne fait pas obstacle à la possibilité de proposer aux utilisateurs de consentir de manière globale à un ensemble de finalités, sous réserve de présenter, au préalable, aux utilisateurs l'ensemble des finalités poursuivies."

> *"The controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand. As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent"*[35].

Grindr questions whether Datatilsynet is of the opinion that free versions of apps cannot have sharing of personal data for advertising purposes. Grindr also questions whether Datatilsynet will issue administrative fines of equivalent size to other apps with a free version with ads and a paid version without directed ads.

Grindr's offering of two versions of the App constitutes a genuine choice. This has been explicitly endorsed by the EDPB guidelines on consent.

Further, as clearly set out by both the EU and by Datatilsynet in a number of reports, legislative instruments and proposals, personal data may be used to pay for digital services. This is illustrated by the following examples:

> *"Consumers currently pay for digital services either via monetary means or with their personal data, time or attention."*[36]

> *"Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. (...) The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. (...) For example (...) where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service (...) It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes."*[37]

> *"It may be claimed that the use of various internet-based services – for example social media – represents a form of mutual contract in which the individual gains access to and can use the service in exchange for being exposed to advertising. As an extension of this, it may be argued that the processing of personal data in order to adapt the*

[35] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, paragraph 37.

[36] European Parliament Think Tank, *Update the Unfair Contract Terms directive for digital services,* 9 February 2021, section 2.1.4.

[37] *Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services*, recital 24.

> *marketing to the individual is a necessary part of the contract. The individual then pays for the service indirectly with their personal data".*[38]
>
> *"Making access to a website dependent on consent to the use of cookies for additional purposes as an alternative to a paywall will be allowed if the user is able to choose between that offer and an equivalent offer by the same provider that does not involve consenting to cookies."*[39]

Grindr allows users to choose between a free version and a paid version. The information about the two alternatives was provided in a clear, plain, and intelligible manner. The user had multiple opportunities to withdraw consent to the sharing of data with advertising partners, either within the App, by upgrading to the paid version, and beyond the App, by adjusting the device settings. Hence, the use of the App is not conditional on consenting to the sharing of personal data with advertising partners.

A data subject selecting the free version of the App will not experience detriment to the user experience. The data subject agrees to share data for advertising purposes; first on their mobile device/operating system, then in the app store when installing the App, and thereafter in the App itself through the user's unambiguous acceptance of the Privacy Policy which describes processing activities that require consent.

Nevertheless, Datatilsynet maintains that *"providing data subjects with information on how they could 'opt-out' on their own device is not in line with the principle of accountability in Article 5(2) GDPR. (...) Grindr failed to control and take responsibility for their own data sharing, and the 'opt-out' mechanism is not necessarily effective.*"

As mentioned above, any user may withdraw their consent beyond the App (i.e. on the mobile device/operating system). Those consent mechanisms are device/operating system specific.

The withdrawal of consent at the operating system level ensures that users can continue using the free version of the App with contextual ads served by third partners. If a data subject withdraws their consent at the operating system level, their advertising ID is either cleared and/or comes paired with the users opt-out, and the advertising partner would then serve the user only contextual or run of network ads - not based on previous behavior.[40]

Datatilsynet has failed to establish how the provision of the Grindr services was dependent on consenting to processing operations beyond what was strictly necessary for the performance of the service. Grindr users' previous consents were given "*freely*".

---

[38] Datatilsynet, *The Great Data Race. How commercial utilisation of personal data challenges privacy*, November 2015, page 31.
[39] Council of the EU, press release: *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules*, published 10 February 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/, last visited 26 February 2021.
[40] Run of network means an ad that is neither behaviour or contextually targeted.

Refusal or withdrawal of consent without detriment

Datatilsynet states that as "*refusal or* withdrawing *consent to sharing personal data with advertising partners would lead to extra costs for Grindr's users, Grindr's users could not refuse or withdraw consent without detriment*."

This statement is manifestly false.

Firstly, Grindr provided an alternative to users who refuse to give their consent - a paid version of the App, where the cost was so low it cannot be categorized as detrimental. See also paragraph 37 of the Guidelines for consent, as discussed under conditionality. The paid version of the App is easily accessible from within the same App.

As with most free apps, the free version of the App is based on the user providing certain data to Grindr and its advertising partners to facilitate showing ads. If users denied sharing data with advertising partners via the controls available in their device's mobile operating system, the App would still work equally well. For those users that withdraw their consent, the advertising partner would then only have basic info about the user to show the ad (device type, OS version, etc.).

The offering of an equivalent service for payment is in line with the GDPR. The issue of "additional costs" has been discussed by the European data protection authorities and even added as a condition in the first version of the Guidelines. Indeed, in its 2017 Guidelines on Consent, the WP29 required that both services are '*genuinely equivalent, including no further costs*'.[41] This requirement that the equivalent alternative service offered by the controller should not entail additional costs was however deleted from the updated guidelines adopted in 2018[42] which has also been upheld in the 2020 EDPB Guidelines.[43] This view is supported by legal doctrine[44]

Datatilsynet's statements in its report "*The Great Data Race*" regarding "*take it or leave it*" designs[45] are not relevant for the App. Datatilsynet states:

> "*If saying 'no' is to the disadvantage of the individual, this may represent a form of pressure that is incompatible with the requirement. If for example the real alternative to consent is to not use the service in question, then this is problematic. Such «take it or leave it»-designs are a major challenge*."
>
> "'*Take-it-or-leave-it' -approaches must be avoided. Publishers must give all users access to their services, including those who do not consent to their information being collected and used for personally customized content and advertising*."

[41] WP29 2017, p. 10

[42] WP29 2018, p.9: "*As long as there is a possibility to have the contract performed or the contracted service delivered by this controller without consenting to the other or additional data use in question, this means there is no longer a conditional service. However, both services need to be genuinely equivalent*."

[43] EDPB Guidelines 05/2020 on consent under Regulation 2016/679p. 11.

[44] E. Kosta in Kuner, Bygrave and Docksey *The EU General Data Protection Regulation (GDPR), A Commentary*, 2020, page 352.

[45] Datatilsynet, *The Great Data Race, How commercial utilisation of personal data challenges privacy*, November 2015, page 32 and page 46.

Grindr does not utilize a "*take it or leave it*" approach. All users have access to the service, including those who do not consent to receiving ads.

Secondly, users who withdraw their consent to sharing personal data with advertising partners could still use the free version of the App without detriment.

Users of the free version of the App who would like to withdraw their consent would just need to follow the steps mentioned in the Privacy Policy or make the necessary changes at the device level/in their operating system.

Thirdly, none of the functionalities of the App would be altered.

Datatilsynet contradicts itself and the EDPB when not recognizing a paid version of the App as a valid alternative for users of the free version of the App who do not want to give their consent to the processing of their data for the purposes of receiving ads.

As stated above, Datatilsynet as well as other EU regulators through reports, legislative instruments, and proposals all make clear that personal data may be used to pay for digital services.[46]

Datatilsynet's Advance Notification fails to establish how a user who has withdrawn his consent would suffer any detriment.

2.2.4 Specific

Datatilsynet states that "*Grindr's statement of purpose describes a processing operation, and not the purpose behind the processing operation. The wording of the stated purpose is ambiguous, vague and general, in other words the purpose is not specified*."

The EDPB has taken the position that consent should be specific such that consent requests should be "granular" in nature and there should be a "*clear separation of information relating to obtaining consent for data processing activities from information about other matters*."[47]

Grindr's Privacy Policy states, under the heading "*Where We Share*" and subheading "*Third Party Advertising Companies*", that:

> *"We share your hashed Device ID, your device's advertising identifier, a portion of your Profile Information, Distance Information, and some of your demographic information with our advertising partners. These third parties may also collect*

[46] Datatilsynet, *The Great Data Race. How commercial utilisation of personal data challenges privacy*, November 2015, page 31, European Parliament Think Tank, *Update the Unfair Contract Terms directive for digital services,* 9 February 2021, section 2.1.4, General Secretariat of the Council, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP,* 10 February 2021, page 25 paragraph (2aaaa) (available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf), and Council of the EU, press release: *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules*, 10 February 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/, last visited 26 February 2021.

[47] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, v 1.0, 4 May 2020, page 13, paragraph 55, iii.

> *information directly from you as described in this Privacy Policy through technology such as cookies. The Privacy Policy of these third party companies applies to their collection, use and disclosure of your information. One of these advertising partners is MoPub that helps Grindr deliver personalized advertising. You can follow the links to MoPub's privacy notice and partner page. See the YOUR CHOICES section of this policy for information on your ability to opt-out of interest based advertising. Note that we do not sell your personal user information to third parties for advertising purposes. Also note that we do not share information about your Tribe, or about your HIV status, with any advertising companies."*

Grindr's wording "*deliver personalized advertising*" is a clearly formulated and limited purpose, not a processing operation, as alleged by Datatilsynet. The language is plain and specific, including examples of what is not shared.

Hence, through its previous consent mechanism, Grindr stated a specific purpose behind a processing operation. Furthermore, Grindr obtained consent to its processing separate and apart from other matters, i.e. separate from the consent to the T&Cs.

Datatilsynet has failed to show in the Advance Notification that Grindr has not complied with the principle of purpose limitation in Article 5(1)(b) and the requirement of "*specific*" consents in Article 4(11).

2.2.5 Informed

Datatilsynet maintains that:

> "*information that is relevant for the particular consent request should be highlighted in the request and not solely appear amongst all other information in a long privacy policy. (...) [W]e conclude that the data subjects were not equipped to make informed decisions and understand what they were agreeing to. This means that Grindr did not comply with the requirement of 'informed'*."

Recital 42 of the GDPR explains that in order for consent to be "informed", the data subject must "*be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended*."[48]

Additionally, Article 7(3) requires that the data subject be informed of their right to withdraw consent at any time.[49]

As described in section 1.2.5, Grindr's previous consent mechanism provided users with the complete Privacy Policy for review. The Privacy Policy provided the necessary information related to the purposes of the processing of personal data and informed the users their right to withdraw consent at any time.

[48] GDPR, recital 42.
[49] GDPR, Article 7(3).

Grindr took great lengths to ensure the Privacy Policy was well organized, important sections highlighted and clearly distinguishable, easy to discover, and independent of anything else in the Privacy Policy.

By way of example, the user may also click the link "*Where we share*", which links to "*Third Party Advertising Companies*" that includes further information in a clear and plain language. The information is also concise, and easily accessible pursuant to Article 12(1). In addition, the Privacy Policy has "*privacy by design*" features, which guides the user to relevant and clear, intelligible information,

In addition, Grindr had made the necessary efforts to ensure that the information related to the sharing of data with third party advertising companies was also available in two separate places prior to downloading the App and consenting to T&Cs and the Privacy Policy.

First, the information was available in Grindr's online Privacy Policy, which is available to anyone who wants to know more about how Grindr processes personal data through the App.

Second, such information was also available in the description of the App in app stores, which contained specific information on advertising and a link to the Privacy Policy published on Grindr's webpage.

Datatilsynet has failed to show why the steps mentioned above and in section 1.2.5 do not meet the requirements for an informed consent.

Grindr in all respects complied with the requirement of "*informed*".

2.2.6 Unambiguous

Datatilsynet states that "*Grindr cannot demonstrate that data subjects consented to the particular processing under Article 7(1). Data subjects had to consent to the Privacy Policy in its entirety. (...) [P]rocessing for advertising purposes is quite different from processing data necessary in order for the app to function*."

Datatilsynet's statement is wrong, and it seems that Datatilsynet repeats its approach under "granularity" instead of applying the correct test.

The GDPR is clear that "[c]*onsent should be given by a clear affirmative act establishing [an] unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement*."[50]

Grindr's previous consent mechanism contained a double-consent to the Privacy Policy.

Through the double-consent mechanism, which required a clear, affirmative and positive action, Grindr was able to register the user's unambiguous consent. The consent mechanism

[50] GDPR, recital 32.

was designed in a way that would not register user consent where a user might unintentionally, or mistakenly clicked on a box because:

1. The user must click two different boxes.
2. The boxes were located in two different locations on the screen (avoiding an accidental second click).
3. None of the boxes where pre-ticked box,

Accordingly, a mistaken registration of consent is extremely unlikely.

Solicitation of consent is not "*nudged*" or encouraged; the most prominent option presented to the users is not to accept the Privacy Policy. Grindr is also explicit on how to withdraw consent in the Privacy Policy.

In line with EDPB's guidelines on consent, Grindr has developed a consent flow with clear affirmative actions that complies with the GDPR. Grindr's double-consent mechanism was clear to users, avoided unambiguity, and ensured that the action by which consent was given was distinguished from other actions, which is an essential element in the EDPB guidelines on consent.

Grindr has demonstrated that users consented to the particular processing under Article 7(1).

2.2.7 Concluding remarks

Grindr's previous consent mechanism complied with Article 6(1).

Grindr obtained the consent of its EEA users for the specific purpose of sharing the categories of personal data listed in section 1.3 with Grindr's advertising partners, and Datatilsynet's suggestion to the contrary is simply wrong.

Grindr has demonstrated that users consented to the particular processing under Article 7(1). Grindr has complied with the principle of purpose limitation in Article 5(1)(b) and the requirement of "*specific*" consents in Article 4(11). Consent to processing for advertising purposes was not bundled with acceptance of the T&Cs. The double-consent mechanism is not opt-out, as alleged by Datatilsynet.

Grindr has also shown that users were given enough information during the user journey to make an informed consent related to the sharing of some categories of data for advertising purposes; in the mobile device's operating system, in the app store, in the Privacy Policy and through separate consent to certain processing activities. In addition, consent to the T&Cs and consent to the Privacy Policy were separately accepted through two different double-consent processes.

In addition, such consent was freely given, as it was not bundled with other purposes.

Furthermore, users had the opportunity to withdraw consent to personalized ads in their device/at the operating system level or by using the paid version of the App.

Finally, it is important to mention that the sharing of data with advertising partners is only possible if the three below conditions were met:

1. The user has made certain opt-in choices in their device/at the operating system level;
2. The user has consented to the T&Cs; and
3. The user has consented to the processing activities mentioned in Privacy Policy in the App.

In this way, users consented to the particular processing under Article 7(1).

Datatilsynet's arguments to issue a fine for the violation of Article 6 are solely grounded on EDPB's interpretation of consent from the EDPB guidelines, which are not legally binding.

2.3 Grindr has not shared special categories of personal data under Article 9

Datatilsynet's initial assessment rests on the presumption that if a data subject is a Grindr user, it qualifies as data "*concerning*" the user's "*sexual orientation*" according to Article 9(1).

Datatilsynet suggests that a Grindr user is "presumably gay" to argue that the sharing of personal data with advertising partners falls under Article 9 of the GDPR by default.

It is simply wrong to assume that Grindr's users are "*presumably gay*" or that being a Grindr user means that the user "*belongs to a sexual minority*".

A Grindr user could be homosexual, bisexual, transsexual, pansexual, heterosexual, bi-curious, or any other sexual orientation. In fact, the App is open for all sexual orientations, including those who are unsure about their own sexual orientation. Grindr continues to be an open platform that will evolve as people's expression of themselves evolve, perhaps in ways that transcend the fundamental construct of sexual orientation.

Nevertheless, Datatilsynet concludes that "*the processing falls within the scope of Article 9*", that Grindr has failed to demonstrate that one or more of the exceptions in Article 9(2) were applicable and thus has violated the prohibition laid down in Article 9.

As mentioned in the response of 22 May 2020, although Grindr does not collect a user's sexual orientation, Grindr recognizes that a user's sexual orientation is a "*special category*" under Article 9.

In the ordinary course of using the App, users may choose to disclose their sexual orientation in the free text fields of their profile ("About Me"), or they may discuss their orientation privately via chats between users. Grindr would process (i.e. in the meaning *store* information in the App) "*special categories*" by allowing users to inform other users about their sexual orientation. However, this information would never be shared with advertising partners.

As stated in section 1.3, during the period in question, Grindr only shared standard categories of information with advertising partners such as advertising ID, provided by the mobile operating system (and under full user control), IP Address, and information about

the computing environment (operating system version, model, screen resolution, etc.) (collected by the SDK); self-reported age (in whole years); gender; and location (Collected by the SDK) - only if the user has both allowed Location services on their device and has provided express consent to the Grindr App to access their location.

None of the above categories of personal data shared with advertising partners fall under the scope of Article 9 of the GDPR. Keywords used to market the app ("*gay, bi, trans and queer*") could not disclose any user's sexual orientation. The fact that one ad tech partner's SDK previously appended those keywords in certain ad calls did not elevate all of Grindr's user information to "special category" data under Article 9.

Grindr never shared the user's sexual orientation or any other categories of personal data considered as special categories under the GDPR of personal data with its advertising partners. Therefore, Datatilsynet cannot establish any violation of Article 9 of the GDPR.

2.3.1 The processing does not fall within the scope of Article 9

Datatilsynet suggests that Grindr has disclosed "*special categories*" of personal data to third party advertising partners without a valid exemption from the prohibition in Article 9(1).

A user's mere use of the App does not indicate their sexual orientation. Grindr does not process its users' data in order to draw inferences about their sexual orientation, and Grindr does not track or classify users according to their sexual orientation.

Specifically, Grindr does not *share* information about sexual orientation with advertising partners.

Datatilsynet suggests that Grindr has disclosed "*special categories*" of personal data to third party advertising partners without a valid exemption from the prohibition in Article 9(1).

In general, Grindr would be surprised if any ad companies can or would profile based on "*special categories*" of personal data. The fact is that Grindr's advertising partners – in the event they would ever theoretically receive sensitive personal data – must "*blind*" themselves to any sensitive personal data pursuant to GDPR Article 25 ("*data protection by design and by default*"). Further, participants in the ad tech ecosystem would likely only receive a "blinded" app-ID[51] and not the corresponding app name.
EDPB confirms in its guidelines on processing of personal data through video devices that the mere disclosure of the data is not sufficient to trigger the applicability of Article 9(1), as long as the purpose of such processing is not to deduce special categories of data.[52]

Grindr does not endeavor to deduce any special categories of data through the information that it collects, and certainly does not share special category information with advertising partners.

[51] It is a common practice in the EU for ad networks to nullify the app name and use a random App ID in the ad call so that downstream bidders are "blind" to the actual name of the app where the ad is to be served.

[52] European Data Protection Board, *Guidelines 3/2019 on processing of personal data through video devices - version adopted after public consultation,* 29 January 2020, page 17 paragraph 62-64 (available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en).

This approach has been confirmed by the Administrative Court of Berlin in the Ebab case[53].

In this case, the Administrative Court of Berlin confirmed that not every indirect indication related to special categories of data is sufficient to justify the application of Article 9, even if the information about the particularly sensitive circumstances can also be derived indirectly from the overall context.

In the Ebab case, the *"#1 travel community for gay and friends"*, the Court concluded that the indication that a person uses the Ebab platform only increases the statistical probability of the conclusion that the user is homosexual. The Court confirmed that "*this conclusion is not compelling, since the platform generally does not assume a sexuality"* on its users.

In addition, the Administrative Court of Berlin took into consideration the self-presentation of the platform, according to which it offers "*private accommodations by gay or gay-friendly hosts*", and the slogan *"your possibility to travel 100% gay! - travel community for gays, Lesbians & Friends*", and concluded that not all the hosts are necessarily homosexual but some of them would describe themselves as "*gay-friendly*" or "*friends*".

In contrast, Datatilsynet's Advance Notification states that *"Information about someone merely being a Grindr user may be a special category of personal data"*. This argument is not aligned with the German Court decision on the Ebab case, where the German Court stated that *"as long as there are doubts, the application of the special provisions for processing sensitive data must be denied."*

In light of the above, it is irrelevant how Grindr markets itself, how newspapers describe Grindr, or how the public perceives of Grindr when assessing whether Grindr's sharing of ordinary, industry-standard information with advertising partners would fall under the scope of Article 9(1).

Considering recent case-law, the EDPB guidelines, we believe that Datatilsynet is wrong when it suggests that because Grindr users are "presumably gay", the sharing of any personal data with advertising partners falls under the scope of Article 9 because:

[53] Verwaltungsgericht Berlin (Administrative Court Berlin), Order of 27 March 2017, VG 6 L 250.17, BeckRS2017, 106722

1. Grindr has never disclosed or shared "*special categories*" of personal data such as sexual orientation with advertising partners;
2. Grindr only shared standard data elements such as the Advertising ID provided by the mobile operating system (and under full user control) and information about the computing environment (operating system version, model, screen resolution, etc.), age (in whole years), gender, and location;
3. The purpose of the processing is not to deduce information on the sexual orientation of the user;
4. If, in a hypothetical scenario, an advertising partner ever received sensitive personal data, they would "*blind*" themselves to any sensitive personal data pursuant to GDPR Article 25 ("*data protection by design and by default*"). Further, the real-time bidding would receive app-ID only; and
5. Grindr's contracts with its advertising partners have contractual commitments to comply with applicable laws, and some even have express commitments that prevent Grindr from disclosing "*special categories*" of personal data, as illustrated by the following example:
    - *"Neither party shall provide the other with any special categories of Personal Data."* (Grindr:Smaato contract)

Contrary to Datatilsynet's view, the mere use of the App does not indicate the user's sexual orientation, and the personal data Grindr shared with advertising partners does not fall within the scope of Article 9.

2.3.2 The unintended consequences of Datatilsynet's interpretation

All data related to Grindr cannot be considered as "*concerning sexual orientation*" under Article 9(1). Such an interpretation may lead to significant unintended consequences.

As discussed above, the Grindr community includes users across the full spectrum of sexual orientations. Thus, Datatilsynet assumption that all Grindr users are "*presumably gay*" or "*belong to a sexual minority*" is simply mistaken.

Datatilsynet's reasoning may create unintended consequences, as it would impose a higher threshold for apps which serve the LGBTQ+ community when collecting and sharing data for advertising purposes than for the rest of other players in the market than for other social network or dating apps, which process the same categories of data for the same purposes.

In addition, Datatilsynet's approach would create far-reaching obligations for any organization that serves a special interest community. In the LGBTQ+ space, travel agencies specializing in LGBTQ+ travel, "gay friendly" hotels, organizers of LGBTQ+ events, or any organization that markets to or provides any product or service for the LGBTQ+ community would be subject to a heightened threshold of Article 9.

For example, it would place any information collected by any website (whether such website is directed at heterosexual users or homosexual users) under the scope of Article 9, as well as any information collected on websites that target users concerning racial or ethnic origin (e.g., websites for individuals of Irish, Polish, or African descent), political opinion (e.g.,

websites targeted to conservative or liberal leaning individuals), or philosophic belief (e.g., websites that appeal to individuals with shared philosophic leaning).

We refer to Kuner et. al. which states that:

> *"(...) information about an individual obtained in everyday situations should not be considered sensitive data unless there is an intention to use it based on one of the particular elements of sensitivity obtained in the law (...)."*[54]

> *"(...) for example, the Islamic name of an individual which is listed in a company's customer directory should not be considered to be sensitive data unless and until there is the intent to use it for its ethnic or religious character, such as if the company decides to start an advertising campaign directed at individuals of Islamic background."*

Thus, Datatilsynet's presumption that if a data subject is a Grindr user, that in itself qualifies as data "*concerning*" the user's "*sexual orientation*" according to Article 9(1), is wrong and may have unintended consequences, including disproportionately burdening a community that has historically been subject to disproportionate and unfair discrimination.

At the most, the user's association with the App indicates an interest in interacting with other users with the same interests; it would not entail sharing the user's sexual orientation with third parties.

2.3.3 Grindr's arrangements with advertising partners could not "put the data subject's fundamental rights and freedoms at risk"

Datatilsynet alleges that Grindr's arrangements with its advertising partners implies "spreading" information about the data subjects' sexual orientation, "*even without revealing their specific sexual orientation*", and that such "spreading" of information could "put the data subject's fundamental rights and freedoms at risk."

Datatilsynet concludes that "*the purpose behind Article 9 also shows that Grindr has disclosed data 'concerning' the data subject's 'sexual orientation'*."

The fact is that Grindr previously shared the industry-standard categories of data, listed in section 1.3, with advertising partners for the purposes of displaying ads, as other apps regularly do. Notwithstanding the negative impact on Grindr's advertising revenue, the Company stopped sharing even this limited personal data with advertising partners.

Grindr and its advertising partners have contractual, organizational, physical, and logical measures in place that are particularly designed to prevent unauthorized access, security incidents, hacking, or other unwanted activity.

The fact that a data subject is a Grindr user is not likely to lead to prejudice or discrimination against the data subject in the real world. Using Grindr is no different from using Tinder or similar dating apps and online discussion forums where online trolls may be present but can

[54] Kuner et. al. page 374

be reported and dealt with quickly. As discussed in sections 1.2.7 and 2.3.1, many of the advertising partners that Grindr uses would have "*blinded*" the app name. The only link between Grindr and the physical world is those situations where two Grindr users agree to meet in-person. Grindr provides users with Trust & Safety instructions to guide them through approaches to help reduce risks to both parties. Grindr is not aware of a circumstance in which a Grindr user was barred access from a product, service or other offering in a discriminatory fashion based on their use of the Grindr App.

However, although there are places where sexual minorities are at risk of being discriminated against, this is not a type of discrimination that is evident in the digital world.

In light of this, Datatilsynet's comment regarding risks for "*data subject's fundamental rights and freedoms*" is unsubstantiated and undocumented.

Datatilsynet has failed to show that Grindr's processing activities (i.e. *sharing* the categories of personal data mentioned in section 1.3 with advertising partners) fall within the scope of Article 9.

Thus, a positive conclusion by Datatilsynet under Article 9(1) would be contrary to the principle of legal certainty.

Grindr does not process its users' data in order to draw inferences about their sexual orientation, and Grindr does not classify users according to their sexual orientation.

2.3.4 In any case, the processing falls within the exceptions in Article 9(2)

Even in the imaginary scenario that associating Grindr's name, in conjunction with keywords related to the App, with user data is somehow within the scope of Article 9(1), Grindr would have sufficient basis for processing of Grindr's user data under Article 9(2)(a).

Pursuant to Article 9(2)(a) a controller may process personal data concerning a data subject's sexual orientation if "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes*".

As explained in section 2.2.7 Grindr has obtained valid consents under Article 6(1)(a). Further, as illustrated above in sections 2.2.2, 2.2.6 and 2.2.7, the consents have been double confirmed, *i.e.* the data subjects have been presented with the entire text of the Privacy Policy, required to take first click "proceed," and then indicate their consent to the practices set forth in the Privacy Policy by clicking "I accept the Privacy Policy."

Grindr's Privacy Policy clearly and explicitly explains that information in their profile will become public: "*Remember that if you choose to include information in your Grindr community profile, that information will become public to other Grindr users. As a result, you should carefully consider what Personal Data to include in your profile*."

In light of this, it is clear that Grindr has obtained explicit consent to share user data associated with Grindr's name with third parties for advertising purposes, cf. Article 9(2)(a).

In any event, Article 9(2)(e) provides sufficient legal basis for Grindr's processing within the scope of Article 9(1). Pursuant to Article 9(2)(e) a controller may process personal data concerning sexual orientation in Article 9(1) if the "*processing relates to personal data which are manifestly made public by the data subject*".

The App is open for everyone, there are no barriers to use the App. The data shared in the App is public for all users of the App. Unlike other social networking apps, Grindr does not function with gates around certain user data made accessible only to certain classes of users or only after two users indicate mutual interest. Nearly all user data supplied to Grindr is made public to other Grindr users through the App via Grindr's proprietary cascade.

The fact that a Grindr profile could be exposed to Grindr's approximately 4 million daily active users indicates that the profile must be deemed public. By comparison, an article in the Norwegian main newspaper *Aftenposten* may be exposed to *Aftenposten's* 1.3 million average daily users. In light of this, creation of a Grindr profile must be deemed as "*manifestly*" making the individual's use of Grindr public.

In the assessment of Article 9(2)(e), Datatilsynet refers to five elements set out in the EDPB guidelines on targeting of social media users.[55] We note that this guideline is from September 2020, five months after the relevant time period for this case. Datatilsynet cannot refer to this guideline as a source of law for determining the legality of Grindr's consent mechanism up until April 2020 because (i) the EDPB guidelines are "soft law", and (ii) the principle of legal certainty.

Under any circumstance, the EDPB notes the following:

> *"the presence of a single element may not always be sufficient to establish that the data have been 'manifestly' made public by the data subject. In practice, a combination of these or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public."*

The ICO has identified the following factors that should be addressed when considering reliance on Article 9(2)(e).[56] As illustrated below, each factor supports the ability of Grindr to rely upon the exception:

- "Is the special category data already in the public domain – can a member of the public realistically access it in practice?"

Grindr is open to all individuals, and the personal data shared there is freely available to all who use the App (available for free to all users).

---

[55] European Data Protection Board, *Guidelines 8/2020 on the targeting of social media users*, Version 1.0, Adopted on 2 September 2020, section 8.2

[56] UK ICO, Guide to the General Data Protection Regulation (GDPR), Lawful basis for processing, Special category data. Available at: www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/. Even though the UK ICO is no longer part of the EEA, it is still relevant as a source of interpretation.

- "Who made the data public – was it the individual themselves or was it someone else? In what context was it made public – for example was it due to them giving an interview, standing for public office, or writing a book, blog or social media post?"

Data is collected directly from the data subject who decides what, if any, data about themselves to make public.

- "Did the individual deliberately take the steps which made this special category data public, or was it accidental or unintentional? Did they make a clear decision? Is the individual likely to have understood that their action means that their special category data is in the public domain?"

Grindr users deliberately and affirmatively take steps to make their data public. Grindr's Privacy Policy makes clear that by creating a Grindr user profile, that information becomes "public." Users understand that the core function of the App is to share information about oneself and discover other users through the information that they share about themselves in order to make new connections with a potentially indeterminate number of other Grindr users. Thus, users understand that whatever they share on their public profile will indeed be publicly available to all other users.

The recent GDPR commentary from Oxford University Press (2020) by Kuner, Bygrave and Docksey is illustrative as it states on page 378 that "*making public*" should encompass making personal data available on online social network platforms. On the same page, the term "*manifestly*" is interpreted as requiring "*an affirmative action by the data subject, and that he or she realized that this would be the result*".

In light of this, it is clear that the creation of a Grindr profile is an "*affirmative*" action to make the knowledge of the profile public. Further, when creating a Grindr profile, it is clear that the data subject understands that the Grindr profile will be public to all other Grindr users.

Consequently, Grindr informs the users that the information they explicitly share through their profile will be publicly available to the community.

Datatilsynet argues that:

> *"[a]lthough Grindr makes the data subject's profile available for other Grindr users, the free version of the app only displays a limited number of users at a time. Only users within a certain range from the user's actual or chosen location are visible to them. This also shows that a Grindr user who uploads a profile image may not necessarily have intended to make the information 'public', but only available to a limited number of relevant users."*

The facts Datatilsynet is basing this argument on is incorrect.

First, irrespective of whether a user is a free or paid user, his or her profile will be potentially visible to any Grindr users including (i) free users, (ii) paid users who have access to unlimited profiles, or (iii) users who use the Explore feature to find users in other regions.

Second, even free users can expand their connection with users farther away by applying one of the profile filter options available within the App or by changing their location. Third, whenever the user or other users update their location, the cascade of profiles is immediately updated allowing the user to see additional profiles.

Hence, a profile will not only be visible to a limited number of other users "*within a certain range from the user's actual or chosen location*", and a Grindr user cannot rightfully have intended to make its profile available to only "*a limited number of relevant users.*"

To the contrary, signing up for a Grindr account by consenting to the T&Cs and Privacy Policy, the user must be deemed to have taken an affirmative action to make the Grindr profile public, and the data subject must have realized that its profile would be visible to the millions of other users from all over the world. In fact, the ability to interact with a potentially limitless number of Grindr users is one of the central features of the App.

Lastly, earlier interpretation of Article 8(2)(e) of the previous Directive 95/46/EC is also relevant for understanding GDPR Article 9(2). The Norwegian preparatory work in Ot.prp.nr. 92 (1998-99) stated that the wording "*data which are manifestly made public by the data subject*" shall include making one's personal data available on the web.

The fact that an individual has a Grindr profile must be understood as manifestly made public by the data subject under Article 9(2)(e).

In the event that associating Grindr's name with user data is within the scope of Article 9(1), both Article 9(2)(a) and Article 9(2)(e) provide sufficient basis for Grindr's processing.

2.4 On the proposed administrative fine

2.4.1 Introduction – it lacks legal basis and is not proportional

Datatilsynet has spent a very long time in preparing their case, and has only once asked Grindr for information. NCC complained to Datatilsynet in January 2020 and Datatilsynet asked for information from Grindr 24 February 2020, which was rendered 22 May 2020. It is first nine months later, in February 2021, that Grindr receives any further communication from Datatilsynet.

As there is no clear and convincing evidence that Grindr has in fact breached Article 6(1)(a) nor Article 9, there is no legal basis for imposing an administrative fine in accordance with Article 83(1), cf. Rt. 2012 p.1556.

Grindr is of the opinion that the administrative fine that Datatilsynet intends to impose on [redacted] lacks sufficient legal basis for several reasons.

Firstly, Datatilsynet did not give regard to all the relevant factors set out in Article 83(2). In section 2.4.3 we explain why these factors, in this case, fail to make an administrative fine

[redacted]

against Grindr "*effective, proportionate and dissuasive*", cf. Article 83(1). The principle of legal certainty under EEA law and Norwegian administrative law requires a clear legal basis and "*objective, non-discriminatory criteria which are known in advance to the undertakings concerned*" to impose an administrative fine.[58] [59] Such clear legal basis and known "*objective, non-discriminatory criteria*" do not exist in this case. Thus, there is no legal basis for imposing an administrative fine under Article 83.

Secondly, the amount of Datatilsynet's proposed administrative fine is in any case disproportionate. The administrative fine notified by Datatilsynet will be one of the highest administrative fines imposed for breach of the GDPR within the EEA, relatively. It is not proportionate to the alleged breach, cf. Article 83(1), and deviates from established practice contrary to the concept of equivalence and the consistency mechanism, ref. WP253 agreed to be used as a common approach by EDPB,[60] and the principle of equal treatment under Norwegian administrative law. In section 2.4.4, we further explain why the administrative fine that Datatilsynet intends to impose in any case is disproportionate.

Thirdly, we note that Datatilsynet's reasoning for the amount Datatilsynet intends to impose, is on less than one page. As the size of the administrative fine Datatilsynet intends to impose is substantial and highly intrusive, and clearly deviates from established practice within both the EEA and Norway, the requirement to the reasoning for the administrative fine is raised. In light of this, the short reasoning appears insufficient in light of the deviation from practice established by the data protection authorities in the EEA, leaving the amount of the fine intended to be imposed appearing arbitrary and discriminatory.

2.4.2 General principles when assessing administrative fines

The competence to impose a fine under GDPR Article 83 is under the data protection authorities' discretion. However, a mere finding of breach of Article 6(1) and/or Article 9(2) does not necessarily mean that the data protection authority should impose an administrative fine. An administrative fine imposed by a data protection authority pursuant to Article 83 "*shall in each individual case be effective, proportionate and dissuasive*", cf. Article 83(1). When considering whether a fine will be "*effective, proportionate and dissuasive*", the data protection authority shall consider the factors listed in Article 83(2)(a)-(k) on an individual basis. However, "*a more precise determination of effectiveness, proportionality or dissuasiveness will be generated by emerging practice within supervisory authorities*".[61] Hence, when determining the amount that will constitute an "*effective, proportionate and dissuasive*" fine in an individual case, a data protection authority must take into account the practices of the other data protection authorities within the EEA.

---

[58] Case E-9/11 page 30, paragraph 100.

[59] PVN-2020-13, PVN-2017-3, PVN-2013-9, PVN-2013-20, PVN-2013-5, PVN-2013-8, PVN-2013-10, PVN-2013-11 og PVN-2013-12. The questions in these cases were not on the issuing of a fine, but if a certain provision could be used for issuing an instruction. However, if the ambiguity of a paragraph is the reason for one not being able to issue an instruction, the same level of ambiguity in another paragraph cannot be used for imposing a fine.

[60] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 3 October 2017, page 4 and 5, and Kuner, Bygrave and Docksey *The EU General Data Protection Regulation (GDPR), A Commentary*, 2020, page 1189.

[61] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 3 October 2017, page 6.

The administrative fine that Datatilsynet intends to impose in this case will be one of the highest administrative fines imposed for breach of the GDPR, relatively. By comparison, we note that the administrative fine that Datatilsynet intends to impose will be the highest fine ever imposed for breach of the GDPR within the Nordics, both relative and absolute. The alleged breach in this case is not significantly more grave than other breaches sanctioned by Datatilsynet and other data protection authorities. In light of this, it is clear that the administrative fine Datatilsynet intends to impose in this case is not proportionate to the alleged breach, cf. Article 83(1), and deviates from established practice contrary to the concept of equivalence.[62] Equal and consistent practice is particularly important when imposing a fine for "*processing operations that substantially affect a significant number of data subjects in several Member States*", cf. recital 135. Grindr's previous CMP and the alleged breach affected all Grindr users within the EEA.

Further, the administrative fine imposed by Datatilsynet interferes with the principle of legal certainty under EEA law and the principles of legal certainty and equality under Norwegian administrative law.

In the event that Grindr has breached Article 6(1) and/or Article 9, Grindr is of the opinion that the content of these provisions is unclear.

The principle of legal certainty under EEA law and Norwegian administrative law requires a clear legal basis and "*objective, non-discriminatory criteria which are known in advance to the undertakings concerned*" in order to impose intrusive administrative sanctions, such as an administrative fine.[63] The rationale of the principle is to ensure predictability with respect to what constitutes a breach and when a negative sanction can be imposed.

Under the GDPR, recital 41 explicitly states that legal basis under national law "*should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights*". The principle of legal certainty in the European Convention on Human Rights applies, as an administrative fine is deemed to be a penalty under Article 6.[64]

Pursuant to the Norwegian Personal Data Act section 26, Datatilsynet may impose administrative fines in accordance with GDPR Article 83 at its sole discretion. However, Datatilsynet must exercise its discretion in a uniform manner, and the exercise of discretion shall not appear arbitrary. The administrative fines previously imposed by Datatilsynet are substantially lower, both relatively and absolutely, than the administrative fine Datatilsynet intends to impose in this matter. In light of this, the administrative fine Datatilsynet intends to impose appears arbitrary.

---

[62] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 3 October 2017, page 5.

[63] Case E-9/11 page 30 paragraph 100, and PVN-2020-13, PVN-2017-3, PVN-2013-9, PVN-2013-20, PVN-2013-5, PVN-2013-8, PVN-2013-10, PVN-2013-11 og PVN-2013-12. The questions in these cases were not on the issuing on a fine, but if a certain paragraph could be used for issuing an instruction. However, if the ambiguousness of a paragraph is the reason for one not being able to issue an instruction, the same level of ambiguousness in another paragraph cannot be used for imposing a fine.

[64] Rt. 2012 page 1556.

2.4.3 Imposing an administrative fine is not appropriate

An administrative fine shall be "*effective, proportionate and dissuasive*" in each individual case, cf. Article 83(1).

Grindr's consent mechanism has been fine-tuned on its own initiative. As such, these initiatives would also count as mitigating efforts according to Article 83(2)(c), therefore, imposing an administrative fine is not necessary to dissuade Grindr to cease the alleged breaches of Article 6(1) and/or Article 9(2).

When deciding whether to impose an administrative fine, the factors listed below in (a) to (k) shall be given due regard, cf. Article 83(2).

EDPB mentions in Guidelines on the application and setting of administrative fines[65]:

> "*Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine. This does not recommend a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case, as provided by article 83.*
>
> *The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice.*
>
> *This section provides guidance for the supervisory authorities of how to interpret the individual facts of the case in the light of the criteria in article 83 (2).*"

Grindr believes that Datatilsynet has not made an assessment of an individual case but decided to issue an administrative fine on the basis of the findings of the NCC report and on a specific interpretation of Article 6 and Article 9 of the GDPR.

For the purposes of our response, Grindr will follow EDPB's interpretation of the assessment criteria

(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

First of all, the categories of personal data concerned are, as described in section 1.3: advertising ID provided by the mobile operating system (and under full user control), IP Address, and information about the computing environment (operating system version, model, screen resolution, etc.) (collected by the SDK); Self-Reported Age (in whole years)[66];

[65] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP253

[66] At account creation, users are prompted to enter their date of birth to validate that they are a legal adult. Grindr does not verify if the self-reported age is accurate and only stores the user's age in whole years. A user can later change their age in their profile to anything between 18-99.

gender[67]; and location (collected by the SDK) - only if the user has both allowed location services on their device and has provided express consent to the Grindr App to access their location.

Secondly, the recipients of such data were Grindr's advertising partners with whom Grindr had adequate contractual mechanisms in place. Furthermore, those contracts would explicitly prevent Grindr from disclosing "special categories" of personal data.

Thirdly, the legal basis for the sharing of data was user's consent, which had been obtained as described in section 2.2 (and section 2.3.4).

Lastly, the scope of the infringement of Article 9 is incorrectly determined by Datatilsynet, and the alleged infringement is not as grave as implied by Datatilsynet.

In light of the above, Grindr will provide a detailed explanation to Datatilsynet regarding the interpretation of the individual facts of the case in the light of the criteria in article 83 (2) (a).

Regarding the nature, gravity and duration of the alleged infringement,

The alleged infringement would not be related to Grindr's inability to put in place the adequate required technical and organizational measures to implement a GDPR compliant consent mechanism but to a specific interpretation of the requirements for obtaining consent.

The duration of the alleged infringement is limited in time.

Such infringement would have been mitigated with the implementation of the new consent mechanism in April 2020.

Datatilsynet fails to provide reasonable legal arguments to justify the gravity of the infringement.

Regarding the nature, scope or purpose of the processing, under Article 83(2)(a),

Datatilsynet has made the following argument:

> *"Furthermore, the data subjects did not initiate the particular processing operations in question. As discussed in Section 5.1, they presumably wanted to access the services provided in the app, and they did not necessarily intend to share their personal data to several third party advertisers. They were instead subject to Grindr's and third parties' commercial interests, with the potential of their personal data being disseminated, sold or further processed without a valid consent and without clear information about this further processing."*

[67] In the Grindr App, users have a wide variety of option to express their gender such as man, woman, cis man, cis woman, trans man, trans woman, non-binary, non-conforming, queer, crossresser, or custom. Users could change their gender identity in their profile at any time. Importantly, Grindr would only provide gender in an ad call if it matched either "male" or "female" - the other options were not shared with advertising partners.

Grindr provided the users with extensive information on Grindr's data processing activities at different stages, as described in sections 1.2.5 and 2.2. The information related to the sharing of purportedly special categories of data with advertising partners had been made available to the users before requesting their consent through the consent mechanism described in section 2.3.4.

The user initiates the particular processing in question when consenting to the processing by clicking the two consent boxes.

Regarding the number of data subjects affected and the level of damage suffered by them

Grindr notes that Datatilsynet refers to the number of affected users in the whole EEA. It is thus clear that Datatilsynet with this Advance Notification seeks to sanction Grindr's alleged breach against all users in the EEA, ref. the principle set out in recital 149.

Although a large number of users within the EEA were using Grindr during the period of time of the alleged infringement, to our knowledge, only one data subject filed a complaint to the NCC.[68] This shows and implies a low level of damage suffered by the affected users.

Datatilsynet further asserts that "*the lack of control over further processing caused a risk of incompatible use*" and that "[t]*he large scale data flow for tracking and profiling for providing behavioral advertisement could inter alia lead to manipulation of data subjects*", adding to the gravity of the alleged infringements.

This statement is not correct. Every user of the free version of the App has been in full control over the processing and had different options to stop the processing by (i) opting out following the process described in the Privacy Policy, (ii) by disabling the necessary features in his or her own device or (iii) by upgrading to the paid version.

Datatilsynet also asserts that:

> "*Grindr has processed personal data illegally when it disclosed personal data about its users with a number of recipients. These recipients may have subsequently disclosed the data to other recipients. Grindr disclosed the data to Twitter MoPub's SDK, and Twitter MoPub lists more than 160 partners. This means that over 160 partners could access personal data from Grindr without a legal basis. We consider that the scope of the infringements adds to the gravity of them.*"

This statement is not correct. Grindr had a legal basis for sharing the relevant personal data through opt-in consent.

Datatilsynet asserts that "*misuse of data concerning sexual orientation could lead to discrimination against the data subject*", and that the fact that Grindr has shared "*user's exact GPS location*" alongside these the alleged special category of data, "*adds to the gravity of the infringements*".

[68] Datatilsynet, *Advance Notification*, page 2, section 3, second paragraph.

Grindr disagrees on this, and the argument is unduly hypothetical and factually inapposite. As discussed above in section 2.3.3, although there are places where sexual minorities are at risk of being discriminated, this is not a type of discrimination that is evident in the digital world. The fact that a data subject is a Grindr user, is not likely to lead to prejudice or discrimination against the data subject in the digital world.

Although there is a link between the digital world and the physical world by Grindr users agreeing online to meet in the physical world, these users will decide time and place, and thus minimize the risk of discrimination on the street by strangers.

In light of this, Datatilsynet's comment regarding risks for "*data subject's fundamental rights and freedoms*" is unsubstantiated. Further, the users also had a possibility of opting out of sharing their location, ref. the text from the Privacy Policy below:

> *"Should you choose not to allow the Grindr App to access your Location, certain features (such as displaying nearby user profiles or features that include Live Location Sharing) of the Grindr Services will not function properly. You may also revoke this permission and disable the location services on your device."*

(b) the intentional or negligent character of the infringement

Datatilsynet asserts that:

> *"the in-app settings did not allow the user to proceed in the app without accepting the entire privacy policy, including the processing in question. This could indicate that Grindr intentionally made it impossible for the user to access the app without accepting behavioural advertising."*

Moreover, Datatilsynet asserts that:

> *"It seems clear that Grindr intended to use its previous consent mechanism and maintains that the consents were valid and in accordance with the GDPR. Our assessment shows that the consent mechanism clearly did not meet the applicable GDPR requirements. In our view, the inadequacy of the consent mechanism should have been clear to Grindr.*

Grindr would like to point out that it does not intend to use *its previous consent mechanism.* Grindr had implemented a consent mechanism powered by OneTrust in April 2020, nine months before Datatilsynet issued the Advance Notification.

Datatilsynet justifies its position solely on the EDPB's interpretation of consent. We note that Datatilsynet and the courts are bound by the GDPR, but not by the guidelines of the EDPB and hence these guidelines are not legally binding. It is absolutely not clear why Grindr's previous consent mechanism was not lawful

Grindr believes there has not been an intentional or negligent breach of the GDPR.

The fact that Grindr's approach towards privacy compliance has been ahead of industry standards and the Company makes continued efforts to make its data processing practices even more transparent, illustrates that there is a clear will to comply with the GDPR.

Datatilsynet should consider that Grindr has been ahead of the industry standard and industry guidelines, such as the IAB Europe Transparency and Consent Framework and the Irish Data Protection Authority's Guidance published 6 April 2020 ("**DPC Guidance**").[69]

IAB Europe TCF is made by the European association for the digital marketing and advertising ecosystem, and is the only GDPR consent solution built by and for the industry, giving it a true industry-standard approach.[70]

In the DPC Guidance, the Irish Data Protection Authority recognized the confusion in the industry regarding laws that regulate SDKs and the necessary balance between evolving advertising technology standards and providing industry time to adjust to that evolution.

The Irish Data Protection Authority stated that consent management platforms, provided by third party vendors or developed internally, could help record, document, and manage data subject consent-selections. In order to balance the need to evolve adtech consent standards with the practical recognition regarding current industry standards and practices, the DPC stated that it would "*allow a period of six months from the publication of this guidance for controllers to bring their products, including mobile apps, into compliance after which enforcement action will commence*."[71]

Grindr began exploring a new CMP in June 2019, and entered into an agreement with OneTrust for development of a Grindr European CMP in January 2020, for the same purposes as recommended in DPC Guidance published ten months later. Grindr implemented the platform two days after the DPC Guidance was issued, well before the end of the six months period granted in the DPC Guidance. The new CMP meets the recommendations in the DPC Guidance, and is otherwise compliant with Article 6(1) and Article 9 and other recent guidance on the use of cookies and other advertising related data sharing technologies. This illustrates that Grindr was well ahead of industry guidelines and standards with respect to ensuring valid consents.

In contrast to the DPC Guidance, Datatilsynet gives no regard to Grindr's implementation of its current CMP. However, the fact that the Irish Data Protection Authority deemed it necessary to provide controllers and processors with a six months grace period from its April 2020 DPC Guidance illustrates that the state of the law with respect to Article 6(1) and Article 9(2) was unclear at that time.

For US technology companies, the Irish Data Protection Authority's guidance is especially relevant. Most of the big technology companies established within the EEA are established in Ireland, making the Irish DPA the lead Data Protection Authority for these companies.

---

[69] An Coimisiún um Chosaint Sonraí (Irish Data Protection Commission), Guidance Note: Cookies and other tracking technologies (6 April 2020).

[70] https://iabeurope.eu/transparency-consent-framework/, visited 12 February 2021.

[71] DPC Guidance at page 16.

As Grindr initiated the assessment of a new CMP prior to the publication of the DPC Guidance, Grindr has clearly been doing more than "*what it could be expected to do*".

Further, the case with the European Parliament and NOYB's complaint regarding use of cookies illustrates the complexity of the practical implementation of the GDPR.[72]

Reference is also made to the Danish decision on imposing an administrative fine of 12 February 2021.[73] Here, a furniture company was found to have stored personal data for a longer period than what was necessary for the purposes the personal data was processed for, in violation of GDPR Article 5(1)(e) and Article 6. The furniture company had not deleted the personal data on approximately 350 000 customers in an old IT system. Further, the furniture company had neither set out any deadlines nor routines for deletion of these data. In the consideration of the fine to be imposed, significant weight was given to the mitigating factor that the furniture company had conducted significant efforts to ensure that the company's many IT systems were compliant with the "*not uncomplicated*" provisions of the GDPR. As in the Danish case, Datatilsynet must give significant weight to the considerable efforts Grindr has taken in order to ensure its users' privacy beyond the requirements of the GDPR.

In light of this, it is evident that Grindr has continuously worked on and evaluated its own practice in light of the industry guidelines and standards to improve its consent mechanism.

In the event that Grindr has breached Article 6(1) and/or Article 9(2), Grindr is of the opinion that these provisions are not sufficiently clear to suffice as clear legal basis for imposing an administrative fine under Article 83(5), in light of the principle of legal certainty. The fact that the state of the law was unclear and vague at the time of the alleged breaches, and that this confusion was the reason for Grindr's alleged breaches of Article 6(1) and/or Article 9(2) imply that the nature and gravity of the infringement(s) shall be given regard as mitigating factors.

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

Datatilsynet asserts that Grindr's implementation of its current CMP is irrelevant in the present case, contrary to Article 83(2)(c).

Grindr understands that Datatilsynet considers that the alleged breach ended in April 2020 when Grindr implemented its current CMP.

Even if any user had suffered any damage due to the alleged breach of Article 6(1) and/or Article 9(2) under the previous CMP, Grindr mitigated such damage when it implemented the current CMP in April 2020.

[72]Complaint under Regulation 2018/1725, Article 63(1) and 67 by NOYB, case-no. C-035, available at https://noyb.eu/sites/default/files/2021-01/NOYB%20COMPLAINT%20C035_Redacted.pdf.
[73] Court case no. 13-3662/2020 against ILVA A/S dated 12 February 2021.

The current consent mechanism for EEA users is aligned with most recent guidance on the use of cookies and other advertising related data sharing technologies, including the guidance published by the Irish DPC.

Grindr invested heavily in the adoption and implementation of the OneTrust CMP (and was actually one of the early adopters of OneTrust for apps). While not binding as a matter of law, the CMP was implemented to give users industry-leading levels of granularity with respect to the processing activities for which consent is solicited, including without limitation providing names of the specific third parties with whom Grindr intends to share such information. As discussed in section 1.2.6, Grindr has adopted a layered approach to its Privacy Policy to enhance users' ability to quickly learn more about the Company's information collection and sharing practices. Users are provided with additional notice concerning Grindr's use of online tracking technologies, such as SDKs, to personalize advertising, to provide social media features, and to analyze Grindr traffic by providing information to third parties.

A data subject can selectively accept/reject certain types of sharing based upon the specific purpose for which the data will be shared (e.g., advertising, social media, etc.). Consent is not set to a default opt-in position. Rather, the default position is "*no consent*" and users are not directed, pushed, influenced, or "*nudged*" to provide consent. The "*Do Not Consent*" option is provided in the same font, color, and size as the option to "*Consent to Use and Sharing*." Indeed, the "*Do Not Consent*" option is provided with greater prominence than the consent option as it is presented as the first option to the data subject. It is clearly stated that use of the App will not be impacted by a decision not to provide consent for non-essential processing activities.

Moreover, after April 2020, Grindr launched a Third Party Disclosure website[74] with more detailed information on how user personal data is collected, used, disclosed, and retained, in compliance with the "layered" approach recommended by the Working Party, the EDPB, and various data protection authorities, allowing users that wish to obtain additional details to readily obtain such information.

The features identified by Datatilsynet in the Advance Notification have been fine-tuned, therefore mitigated, on Grindr's own initiative with the implementation of the new CMP. The process of onboarding the fine-tuned consent mechanism was initiated prior to the publication of the NCC report, and implemented well before the Advance Notification.

Consequently, the current consent mechanism includes features that would certainly satisfy even EDPB's interpretation of consent.

Grindr recognizes that privacy practices are constantly evolving, as reflected by the updated guidelines published by EDPB, reflecting the evolution of privacy practices and norms. For this reason, Grindr keeps an open dialogue with its community of users, regulators, and other industry players. Datatilsynet must consider Grindr's active position as frontrunner within its industry as a mitigating factor.

[74] The Third Party Disclosure website was deactivated when Grindr transitioned to a more layered privacy policy approach.

(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

Datatilsynet has stated that it is "*not aware of any data protection measures taken by Grindr to secure the information shared with advertising partners. On the contrary, it seems that Grindr lacked control of the data flow and recipients, as it shared personal data on its users through an SDK where Grindr has limited or no control over further processing.*"

Further, Datatilsynet raises the question "*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*".

Regarding the *"data protection measures taken to secure the information shared with advertising partners":*

First of all, in many cases, the user's use of the Grindr App is not provided to downstream participants in the ad ecosystem by blinding the app ID. This is a feature that was initially introduced into the ad ecosystem over a decade ago as large publishers didn't want others in the ad ecosystem to be able to profile their users. As they were a large channel for revenue the ad ecosystem was forced to create these blinding mechanisms to protect the data interests of the big publishers.
Having said this, Grindr had adopted a series of technical and organizational measures to ensure the security of the sharing of the data with the advertising partners as required by article 32. Such measures included:

1. The encryption of data: Grindr conducts regular audits to validate that ad calls are encrypted in transit to help prevent third parties from illicitly accessing user information.

2. The implementation of a robust security program that is led by an experienced team that includes security policies, training, and procedures that operationalize Security by Design. Security assessments are regularly conducted, including with respect to new app features and vendors to ensure appropriate controls are implemented (e.g., encryption, hashing, access controls, etc.), especially where personal data may be collected, used, or otherwise processed.

3. Conducting due diligence on our advertising partners and negotiating contracts to include robust commitments to adequately secure and lawfully process personal data.

4. The implementation of a full suite of privacy standard operating procedures, guidelines, and training to satisfy the privacy by design and by default principles.

5. With respect to relevant data protection routines/policies, cf. Article 24, Grindr's privacy and security policies are available to all Grindr employees and have been disseminated throughout the organization via regular employee communications, management meetings, and training.

In response to Datatilsynet's question regarding "*to what extent Grindr "did what it could be expected to do":*

The timing of the implementation of the current CMP, and the uncertainty in the industry at the time Grindr initiated investigations on a new CMP clearly shows that Grindr has implemented measures to ensure data protection by design ahead of the DPC Guidance and the practice of its competitors, and thus did more than what it could be expected to do. We also refer to the discussion under (b) above, showing Grindr's privacy initiative.

Datatilsynet also states that *"Grindr collected a lot of personal data from a lot of users, including data concerning sexual orientation".*

This statement is false. Grindr only shared the categories of data listed in section 1.3:

- Advertising ID provided by the mobile operating system (and under full user control), IP Address, and information about the computing environment (operating system version, model, screen resolution, etc.) (Collected by the SDK, not pushed by Grindr);
- Self-Reported Age (in whole years);[75]
- Gender;[76] and
- Location (collected by the SDK and only if the user has both allowed Location services on their device and has provided express consent to the Grindr App to access their location).

As stated above, several of the advertising partners that Grindr's uses even require "blinding" that the user is a Grindr user.

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

The fact that Grindr has not previously violated the GDPR must be taken into account as a mitigating factor. This is confirmed by the Danish decision on imposing an administrative fine of 12 February 2021, which is further explained above under (b).[77]

Grindr has been under scrutiny from the Spanish DPA (defined below) and the ICO. It is important to note that none of them have found any breach of data protection regulations.

In April 2017, following the publication of report drafted by SINTEF, a Norwegian research organization, stating that Grindr would be sharing data related to users' HIV status and location data with third parties unlawfully, the Spanish data protection authority, Agencia Española de Protección de Datos ("**Spanish DPA**") received complaints from three Spanish Consumer Associations against Grindr.

[75] At account creation, users are prompted to enter their date of birth to validate that they are a legal adult. Grindr does not verify if the self-reported age is accurate and only stores the user's age in whole years. A user can later change their age in their profile to anything between 18-99.

[76] In the Grindr app, users have a wide variety of option to express their gender such as man, woman, cis man, cis woman, trans man, trans woman, non-binary, non-conforming, queer, crossdresser, or custom. Users could change their gender identity in their profile at any time. Importantly, Grindr would only provide gender in an ad call if it matched either "male" or "female" - the other options were not shared with advertising partners.

[77] Court case no. 13-3662/2020 against ILVA A/S dated 12 February 2021.

The Spanish DPA started a preliminary inspection proceeding to investigate the alleged infringements. Grindr cooperated with the Spanish DPA and provided the necessary information upon the Spanish DPA's request, including a copy of the contract signed with those third parties, which contains a section on confidentiality and data protection.

On 6 September 2018, the Director of the Spanish DPA issued a resolution[78] ordering the dismissal of the case based on the results of the preliminary inspection proceedings and stated that it had not been proven that Grindr had incurred a violation of data protection regulations.

This resolution was challenged through an administrative appeal introduced by one Spanish Consumer Association. However, the Director of the Spanish DPA dismissed it. In a second resolution[79] related to Grindr, the Director of the Spanish DPA resolved that, on the basis of the preliminary proceedings, it could not be proved that there had been a violation of the data protection regulations.

We also refer to the ICO's request for information to Grindr dated 27 June 2018, Grindr's response dated 30 July 2018 and the ICO's decision "*that no further action is necessary at this stage*", dated 17 December 2018. The background for the case was that a number of users of Grindr contacted the ICO regarding sharing of personal data. Grindr responded that unrelated data fields (e.g., age) are not themselves special categories subject to the heightened requirements of Article 9. ICO's closing of the matter without further inquiry is tacit approval of Grindr's response that the GDPR does not treat every data field collected on a website, the use of which might infer a special category of information, as itself constituting a special category.[80]

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

Pursuant to Article 83(2)(f), the data protection authority shall give regard to "*the degree of cooperation with the supervisory authority*" when determining whether to impose an administrative fine and when deciding the amount of the fine. Despite this, Datatilsynet did not give regard to Grindr's cooperation as a mitigating factor, and asserted "*it would not be appropriate to give regard to cooperation that is already required by law*". However, it must be taken into account that Grindr has provided requested information, and fine-tuned Grindr's consent mechanisms.

Grindr has always cooperated with different EU data protection authorities, in particular with the British, the Spanish, and the Slovenian data protection authorities in the context of different proceedings. Some of these proceedings concerned the sharing of data with third parties and the processing of location data.

It is important to note that none of them have found any breach of data protection regulations.

[78] Expediente Nº: E/01823/2018 Resolución de Archivo de Actuaciones
[79] Expediente Nº: E/01823/2018 Resolución De Archivo De Actuaciones. Recurso De Reposición Nº RR/00643/2018
[80] ICO case reference number: RFA0742872

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

Datatilsynet asserts that *"Grindr has disclosed special categories of personal data illegally to third party advertising partners. 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 and cause grave harm. Combined with exact location data, Grindr puts the data subject at even greater risk." Datatilsynet further states that "processing of a data subject's location information can be a highly intrusive act, depending on the circumstances."*

Datatilsynet's affirmation is not correct. The categories of data shared are listed in section 1.3. Datatilsynet further claims that Grindr could put participants in an address confidentiality program at risk. However, as any other user, a participant in an address confidentiality program would be required to consent to the Privacy Policy, where sharing of location data with advertising partners is described. A participant in an address confidentiality program would not consent to such sharing of data. Datatilsynet's only example of how Grindr may put individuals at risk, by allegedly sharing special categories of personal data, is not realistic.

Grindr does not collect and does not share data concerning users' sexual orientation with advertising partners, as explained in section 2.3. In addition, the App is blinded on entry to the ad tech platform, which does not allow to assess what app the user is using.
Grindr refers below to the series of questions related to the categories of personal data affected by the infringement included in the assessment criteria from WP 253 Guidelines:

(a) Does the infringement concern processing of special categories of data set out in articles 9 or 10 of the Regulation?

Grindr has not shared any special categories of personal data, cf. Article 9.

As explained in section 2.3.1, the Administrative Court of Berlin confirmed in the Ebab case that not every indirect indication related to special categories of data is sufficient to justify the application of Article 9, even if the information about the particularly sensitive circumstances can also be derived indirectly from the overall context.[81]

In addition, the app ID is blind, which does not allow the advertising partner to identify the app from which the call is coming from.

(b) Is the data directly identifiable/ indirectly identifiable?

The data in question is not directly identifiable and requires a large effort, even to accomplish any indirect identification.

(c) Does the processing involve data whose dissemination would cause immediate damage/distress to the individual (which falls outside the category of article 9 or 10)?

No, the dissemination of such data could have not caused any damage or distress to the individual.

[81] Verwaltungsgericht Berlin (Administrative Court Berlin), Order of 27 March 2017, VG 6 L 250.17, BeckRS2017, 106722

In addition, considering the security measures in place, none of the categories of data disclosed to the advertising partners could be processed in a way that could lead to cause prejudice or discrimination against the data subject, neither in the digital nor in the physical world.

Datatilsynet's comment regarding risks for "data subject's fundamental rights and freedoms" is unsubstantiated.

(d) Is the data directly available without technical protections, or is it encrypted?

The data was encrypted in transit, meaning measures were taken to prevent third parties to access the data.

Datatilsynet should consider the answers provided above when assessing "*the categories of personal data affected by the infringement".*

(e) 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

Grindr considers this factor not to be applicable in this matter.

(f) 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

There has not previously been any measures referred to in Article 58(2) against Grindr with regard to the same subject matter. This must be given regard as a mitigating factor.

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

Grindr considers this factor irrelevant in the present case.

(h) 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

Datatilsynet states that "[t]*he legal assessment of 'freely given', inter alia the requirement of granularity and the opportunity to withdraw consent without detriment, has not evolved since the announcement of the regulation*" on 4 May 2016. Thus, Datatilsynet concludes that "*Grindr had two years to adapt to the GDPR requirements*".

As explained in section 2.2, Grindr's previous consent mechanism was aligned with the GDPR. Furthermore, the "legal requirement of granularity" is an interpretation from the EDPB on the requirements for obtaining a freely given consent. Neither today nor at the time of the alleged infringement, there was a legal requirement to implement separate opt-ins.

The Highest Administrative Court of France and CNIL have confirmed that it is possible to offer users a global consent to a set of purposes, subject to presenting all the purposes pursued in advance to the users.

The content of the GDPR requirements has been unclear from the start. Reference is made to the evolution of EDPB and guidelines from different national data protection authorities after May 2018, the TCF framework, and other similar frameworks and guidelines. In May 2018, it was not clear how the requirements to consent were to be interpreted, and the interpretations of these requirements have developed since. Thus, Grindr did not have two years to adapt to clear GDPR requirements.

Moreover, Datatilsynet argues that:

> "*Grindr also refers to guidance on consent provided by the Irish supervisory authority (DPC) from April 2020, where the DPC gives controllers six months to adapt before they start to take action against non-compliance.*
>
> *The guidance provided by the DPC is not a binding document for other supervisory authorities. It should also be noted that neither the GDPR nor Norwegian law allows for grace periods. In addition, other supervisory authorities are enforcing the consent requirements. Most notably in this regard is the French supervisory authority (CNIL), which has imposed a € 50 000 000 fine on Google for relying upon invalid consents. Furthermore, the DPC issued the guidance on 20 April 2020, so it is not likely that this guidance has given Grindr any legitimate expectation of avoiding enforcement actions by supervisory authorities before it was issued*."

It is correct that "*DPC is not a binding document for other supervisory authorities*" and "*that neither the GDPR nor Norwegian law allows for grace periods*". However, the fact that the Irish Data Protection Authority deemed it necessary to provide controllers and processors with a six months grace period, when publishing the DPC Guidance in April 2020, illustrates that the state of the law with respect to Article 6(1) and Article 9(2) was unclear at that time. We note that also CNIL rendered a grace period after updating their recommended cookie practice.[82] Datatilsynet has not given regard to these mitigating elements.

With respect to Datatilsynet's reference to the fine imposed against Google, we note that the fine constituted approximately 0.05% of Google's 109.7B$ global turnover in 2017. This also shows that the system of fines in the GDPR has a bias for large companies, as the fines will be disproportionate relative to the turnover, and thus more grave for smaller companies.

Further, Datatilsynet argues that it is "*aggravating that Grindr must have gained financial benefits from the infringements*."

[82] CNIL, Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL, 1 October 2020, *Des missions de contrôle sur l'application des nouvelles lignes directrices seront ensuite réalisées à la fin de la période d'adaptation annoncée par la CNIL, soit 6 mois après la publication de la recommandation et des lignes directrices".*

The basis of the alleged aggravating factor is related to Grindr's offering of the App without monetary payment from its users. Instead of requiring all users to buy a subscription, Grindr serves advertising to support providing free users with access to the Grindr platform.

This is in line with how many apps and internet content service providers are financing providing their services for no monetary payment from free users.[83]

It is clearly presumed by Datatilsynet and the EU Institutions - including in a number of reports[84], legislative instruments, and proposals - that personal data may be used to "*pay*" for digital services.[85] Even assuming that Datatilsynet determines to issue a fine in this matter.

Datatilsynet has not demonstrated how Grindr obtained a financial benefit resulting from any alleged infringement, particularly given that users were provided with actual notice of Grindr's information collection and sharing practices, including how they could adjust the information shared with advertising partners. [redacted]

In the event that Grindr is found to have breached Article 6(1) and/or Article 9, an administrative fine against Grindr is neither effective, proportionate, nor dissuasive given regard to the factors above.

2.4.4 The amount of the administrative fine is not appropriate

The amount of the proposed administrative fine is not proportional to the alleged infringement, cf. Article 83(1).

The factors in Article 83(2) discussed above in section 2.4.3 clearly indicate that an administrative fine should be nominal, not anywhere close to the maximum penalty under Article 83(5).

---

[83] As confirmed by Directive 2011/83/EU recital 24, and *EDPS Opinion 8/2018 on the legislative package 'A New Deal for Consumers',* 5 October 2018, page 3 and 17.

[84] European Parliament Think Tank, *Update the Unfair Contract Terms directive for digital services,* 9 February 2021, section 2.1, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, recital 24, Datatilsynet, *The Great Data Race. How commercial utilisation of personal data challenges privacy*, November 2015, page 31, Council of the EU, press release: *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules*, 10 February 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/, last visited 26 February 2021.

[85] Datatilsynet, *The Great Data Race. How commercial utilisation of personal data challenges privacy*, November 2015, page 31, and European Parliament Think Thank, *Update the Unfair Contract Terms directive for digital services,* 9 February 2021, section 2.1.4, and General Secretariat of the Council, *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP*, page 25 paragraph (2aaaa), 10 February 2021 (available at https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf) and Council of EU, press release: *Confidentiality of electronic communications: Council agrees its position on ePrivacy rules*, 10 February 2021, available at https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/, last visited 26 February 2021.

Datatilsynet's calculation of the proposed fine is wrong: [redacted] and approximately 50% of the maximum penalty under Article 83(5).[86]

Datatilsynet only presumes annual turnover for 2019 was "*at least*" USD 100 000 000. Here are the correct numbers:

	Norway			Europe			Global		
	2018	2019	2020	2018	2019	2020	2018	2019	2020
Total turnover from the App	[redacted]								
Revenues per user	[redacted]								

As evident from the table in Appendix 1, the notified fine is substantially higher (relatively), than other significant administrative fines imposed by other data protection authorities.

Datatilsynet has not accounted for sufficient aggravating factors justifying an administrative fine of this size. The substantial difference between the relative size of the administrative fines previously imposed and the administrative fine, intended to be imposed by Datatilsynet in this case, cannot be justified by the asserted gravity, duration, scope, or nature of Grindr's alleged breach.

Reference is also made to "*Vedtak om overtredelsesgebyr – Bergen kommune – melding om avvik i Viglio*", reference 20/02181-3, where Datatilsynet imposed a fine against Bergen municipality on 3 000 000 NOK for grave violations of Article 5 and 32. This is currently the highest administrative fine imposed by Datatilsynet. The violations of Article 5 and 32 constituted a risk to the health and lives of several children. The difference between the administrative fine imposed against Bergen municipality and the administrative fine Datatilsynet intends to impose against Grindr, constituting 97 000 000 NOK, cannot be justified by the asserted gravity, duration, scope, or nature of Grindr's alleged breach of Article 6. The same applies for the event that Grindr has breached Article 9. Thus, the administrative fine Datatilsynet intends to impose appears arbitrary.

Moreover, we note that imposing a fine based on a company's turnover, without taking into account the company's EBITDA, may have consequences that are disproportionate to the alleged breach for low margin companies. What matters for a company is the EBITDA, not the turnover.

[redacted]

Further, reference is made to the Danish Data Protection Authority's guideline on the size of administrative fines imposed pursuant to GDPR Article 83.[87] Being the first EEA guideline on how to set administrative fines according to the GDPR, it will have legal weight even though it is not a Norwegian legal source. Under the GDPR is "*equivalent sanctions for infringements*" an explicit goal, cf. recital 11 and 13, in addition to the consistency mechanism.[88] [89] Hence, as the guidelines issued by Danish authorities will be taken into account by Danish authorities when assessing administrative fines under Article 82 should these guidelines also be of relevance for Datatilsynet, to ensure an equivalent and consistent level of the administrative fines imposed.

When determining the amount of an administrative fine in accordance with this guideline, the Danish DPA shall first calculate the base amount in the case in questions. Then, this base amount shall be adjusted in accordance with the factors listed in Article 83(2)(a)-(k). Further, the amount shall be adjusted in accordance with the maximum amounts set out in Article 83, and may be adjusted in light of the controller's/processor's ability to pay the fine.[90]

For a breach of Article 6, the base amount according to the Danish Data Protection Authority's guidelines constitutes 10% of the maximum administrative fine imposable (20 000 000 EUR).[91] This equals 2 000 000 EUR and approximately 20 000 000 NOK. Datatilsynet has not presented any arguments that would justify a difference between 20 000 000 NOK and the 100 000 000 NOK Datatilsynet intends to impose. As described above, in section 2.4.3, the factors listed in Article 83(2)(a)-(k) shows that there are no aggravating circumstances. On the contrary, the mitigating factors in 83(2)(b), (c) and (f) implies that the administrative fine should be lower than the base amount. Thus, the administrative fine should be lower than 20 000 000 NOK. This clearly shows that the fine Datatilsynet intends to impose, on 100 000 000 NOK is disproportionate.

For a breach of Article 9, alone or in combination with Article 6, the base amount according to the Danish Data Protection Authority's guideline would be 20% of the maximum administrative fine (20 000 000 EUR).[92] This equals 4 000 000 EUR and approximately 40 000 000 NOK. Neither for such a case, has Datatilsynet presented any arguments that would justify the difference between 40 000 000 NOK and the 100 000 000 NOK. As described above, in section 2.4.3, the factors listed in Article 83(2)(a)-(k) shows that there are no aggravating circumstances. Thus, the amount of the administrative fine shall not be higher than the base amount for breaches of Article 9. This clearly shows that the fine Datatilsynet intends to impose, on 100 000 000 NOK is disproportionate also in the event that Grindr has breached Article 9 alone, or in combination with Article 6.

Lastly, the fact that Grindr has been negatively impacted by COVID-19 should be taken into account when determining the amount of the administrative fine, cf. Article 83(2)(k). Grindr

[87] The Danish DPA, *Bødevejledning, Udmåling af bøder til virksomheder*, January 2021.
[88] Kuner, Bygrave and Docksey, *The EU General Data Protection Regulation (GDPR), A Commentary*, 2020, page 1189.
[89] Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 3 October 2017, page 4 and 5.
[90] The Danish DPA, *Bødevejledning, Udmåling af bøder til virksomheder*, January 2021, page 4.
[91] The Danish DPA, *Bødevejledning, Udmåling af bøder til virksomheder*, January 2021, page 7.
[92] The Danish DPA, *Bødevejledning, Udmåling af bøder til virksomheder*, January 2021, page 7.

has been hit by the pandemic like all other companies. The impact of Covid-19 and the shift to purely virtual team presence has had the same effect on Grindr as many other tech companies - namely a reduction in the speed of product releases with a need for more time, money, and effort to organize, develop, and release its product roadmap.

In light of the above, it is clear that the amount of the administrative fine Datatilsynet intends to impose against Grindr is in any case too high, and not "*effective, proportionate and dissuasive*", cf. Article 83(1).

3. CLOSING REMARKS

In light of the abovementioned, we believe we have sufficiently proven that Grindr has not infringed article 6 or article 9 of the GDPR, hence should not be sanctioned.

Even in case Datatilsynet insists to sanction Grindr, by imposing a fine, we believe the intended fine of 100 000 000 NOK [redacted] is not proportionate, as required by article 83(1) GDPR. Imposing a fine for an alleged breach of the finer details in how EDPB recommend consent is obtained, is not proportionate and is not justified by the asserted gravity, duration, lack of damage suffering, scope or nature of the alleged breach.

Moreover, and as extensively explained above, such a fine would interfere with the principle of legal certainty under EEA law, the European Convention on Human Rights, and Norwegian administrative law.

In any case, we understand that in its fine calculation, Datatilsynet refers to the number of affected users in the whole EEA. It is thus clear that if sanctioned, Datatilsynet seeks to cover and sanction Grindr's alleged breach regarding all users in the EEA, ref. the principle of *non bis in idem*, as set out in recital 149 GDPR.

The size of the intended fine is not even aligned with the current practice of fine calculations by other data protection authorities in Europe. The intended fine [redacted] would indeed be the largest fine ever issued, not only in the Nordic countries, but throughout the European Economic Area.

We respect that the factual issues of this matter are complex. Grindr is happy to elaborate further on how personal data are used if Datatilsynet may find this useful. Any questions may be addressed to the undersigned.

Kind regards
ADVOKATFIRMAET SCHJØDT AS

Eva Jarbekk
Partner

EVA.JARBEKK@SCHJODT.COM

Appendix 1: Overview of comparable EU fines

APPENDIX 1
OVERVIEW OF COMPARABLE EU FINES

The information below is based upon publicly available data and may contain inaccuracies.

Controller/ processor	Fine (EUR)	Art.	% of revenue
1. **Google Inc (21 January 2019, France)**	50 000 000	Art. 5, 6, 12, 13 and 14.	109.7B$ in turnover in 2017 (approximately 96B euros). **The fine constitutes 0.05% of this.**
2. **TIM – Telecom Provider (1 February 2020, Italy)**	27 800 000	Art. 5, 6, 17, 21 and 32.	TIM S.p.A. had ~ 14B euros in turnover in 2018. **The fine constitutes 0.2% of this.**
3. **British Airways (16 October 2020, UK)**	22 046 000 (not taken into account the latest reduction due to COVID)	Art 5 and 32.	**The fine was less than 0.2% of global turnover before the latest reduction due to COVID-19.**
4. **Marriot International, Inc (30 October 2020, UK)**	20 450 000	Art. 32.	**The fine is less than 0.6% BA's global turnover.** This fine was imposed for infringements for which the fine can be 10 000 000 EUR or 2% of total worldwide annual turnover, cf. Article 83(4).
5. **Wind Tre S.p.A (telephone operators) (13 July 2020, Italy)**	16 700 000	Art. 5, 6, 12, 24 and 25.	**The issued fine constitutes 0.32% of the annual turnover,** and 8% of the maximum legal sanction.
6. **Caixbank S.A (Bank) (12 January 2021, Spain)**	6 000 000	Art. 6, 13 and 14.	"*Operating Margin*" of 2,035M euros. According to the information contained in the Central Mercantile Registry, the "*Subscribed Capital*" amounts to 5,981,438,031.00 euros. **The fine constitutes 0.1% of "Subscribed Capital".** 386,622 M euros of total assets.
7. **Carrefour France and Carrefour Banque (Part of the Carrefour Group (Retail) (18 November 2020, France)**	3 050 000 (2 250 000 + 800 000)	Art. 5, 12, 13, 14, 15, 17, 21, 32 and 33.	<u>Carrefour France</u> The fine on 2 250 000 euros constituted 16 % of annual turnover (approximately 14 M euros), but CNIL took into account the annual turnover of the rest of the Carrefour group. In 2019, the Carrefour group achieved sales of around 80B euros. **The fine constitutes 0.0028% of this.** <u>Carrefour Banque:</u> Net annual income of 308M euros. **The fine on 800 000 constitutes 2.6 % of this.**
8. **Twitter International Company (Ireland)**	450 000	Art. 33 (1) and 33 (5).	Twitter Inc. $3,46B in turnover 2019. **The fine is 0,014 % of this.** This fine was imposed for infringements for which the fine can be 10 000 000 EUR or 2% of total worldwide annual turnover, cf. Article 83(4).
9. **H&M Hennes & Mauritz Online Shop A.B. & Co. KG**	35 258 708	Art. 5 and 6.	Global turnover approximately 22B euros. **The fine is 0.16% of this.**