

**EIP**

# The European Data Protection Board (EDPB) publishes its decision on Meta's legal basis for its use of personalised adverts

## Summary

On 12 January 2023, the EDPB published its decision (which was actually made on 5 December 2022) (the “**Decision**”) on the dispute between the Irish Data Protection Commissioner (**IDPC**) and a number of its equivalent supervisory authorities in other member states relating to complaints made to the Austrian and Belgium supervisory authorities. The dispute was in respect of an alleged breach by Meta of the General Data Protection Regulation (**GDPR**) as a result of Meta's use of personalised adverts in Instagram's and Facebook's social media processing activities. In particular, it was alleged that Meta did not have a valid legal basis for such processing. Meta argued that “a contract was entered into” between it and users and that “processing of users' data in connection with the delivery of its Facebook and Instagram services was necessary for the performance of that contract”, which included the provision of “personalised services and behavioural advertising” The IDPC in a draft decision issued on 23 December 2021 had ruled that whilst Meta's practices and terms lacked transparency (as required by GDPR) the legal basis relied upon was valid. This decision was objected to by a number of other supervisory authorities in July 2022 and the matter was referred to the EDPB to investigate on 11 August 2022. In the Decision, the EDPB ruled that, inter alia, Meta's legal basis for processing such data was invalid and required the IDPC to alter its decision, ordering Meta to change its data-targeting model to comply with the GDPR in

the next three months and increased the aggregate fine from Euros 59m to Euros 390m.

p2

## **Background**

Under the GDPR (and UK GDPR) all processing of personal data is required to have a legal basis (as set out in the GDPR) in order to be lawful and there must be communication of such information to individual users. Meta's processing of its users personal data on the Facebook and Instagram platforms was, according to Meta, justified on the basis it is necessary for the performance of the contract it had with each user to provide it with the services of each platform as set out in Article 6(1)(b) of GDPR. The terms of service for each platform contained clauses permitting the use of such data for various purposes including in order to provide a personalised service, to connect the user with people and organisations the user cares about and to empower the user to express themselves on issues that matter to them. Two separate complaints were made in May 2018 to the respective supervisory authorities in Belgium and Austria by individuals who objected to the use of his or her data in this manner on the two platforms, and whom asked NOYB ([www.noyb.eu](http://www.noyb.eu)) to represent them. The complaints were transferred to the IDPC (as Meta's EU HQ is in Ireland) which decided in December 2021 that Meta was entitled to rely on the Article 6(1)(b) basis. As summarised above, the EDPB has now decided that this decision was incorrect and has required the IDPC to alter its decision and take certain other actions including levying a much larger fine on Meta.

## **Issues raised by the EDPB decision**

The decision by the EDPB has decided that Meta's attempt to rely on its terms of service as providing a legal basis for its processing is ineffective. It will have to find another legal basis in the next three months or face (presumably) the risk of further swingeing fines and potentially a shutdown of its services in the EU. A Meta spokesperson said they "will appeal the substance of the decision" but it is highly likely that we will have to wait at least another year and perhaps longer for a final decision. It seems unlikely to us that Meta will get a different decision on appeal but the appeal may give them extra time to decide how to respond in practice – for example, will they adopt a similar approach to other platforms such as Spotify who offer discounts or a free service for the inclusion of adverts and the use of personal data to personalise them? Or will they, as it is reported has been threatened, shut the service down entirely so EU residents will no longer be able to use the platforms? In addition, this decision raises similar questions for other players in the AdTech industry – a massive, global industry which employs a lot of people and makes a lot of money. We have already seen other platforms such as TikTok face similar scrutiny last year when they attempted to modify their privacy policy, switching from relying on users' consent to the "legitimate interests" legal basis for its

'personalised' ads (Article 6(1)(f)). It is highly likely this will not be the last on this topic and, in particular, it will be interesting to see if the UK's ICO follows suit.

There has also been growing concern for a number of years about the use of personal data by BigTech in this way and others and the lack of regulator action. In the UK, this culminated in an action brought by a Mr. Lloyd against Google in respect of Google's use of what has become known as the "Safari Workaround" on iPhones, which enabled Google to track users across websites facilitating Google's distribution of personalised advertising to them. Lloyd sought to bring a representative action against Google to claim damages for this alleged breach of GDPR on behalf of consumers – necessary because the damages likely to be available to most individual claimants for such a breach would be too low to justify the costs of such an action. However the UK Supreme Court ruled that, while a representative action could be brought to establish liability (i.e. that there was a breach of GDPR) the damages claims would need to be dealt with through a group action (where the claimants all have the same interest and loss) or by individual claims. This in effect killed the idea of trying to bring BigTech to heel stone dead (at least in the UK). This was a concern as the regulators had thus far failed to show much interest in such allegations of breach of GDPR. However the recent decision by the EDPB suggests that regulators are going to be much more willing to investigate such allegations which, if proven, may result in significant fines for BigTech – of which there have already been several examples.

Ultimately though, society will need to decide if the harm or the risk of harm as a result of such processing warrants what those in the AdTech industry would argue are restrictive laws which not only are likely to damage the financial viability of many service providers but might damage the ability of businesses to bring their goods and services to the attention of consumers in a cost effective and efficient manner. We look forward to seeing further developments in this area which raise a number of interesting legal and societal questions.