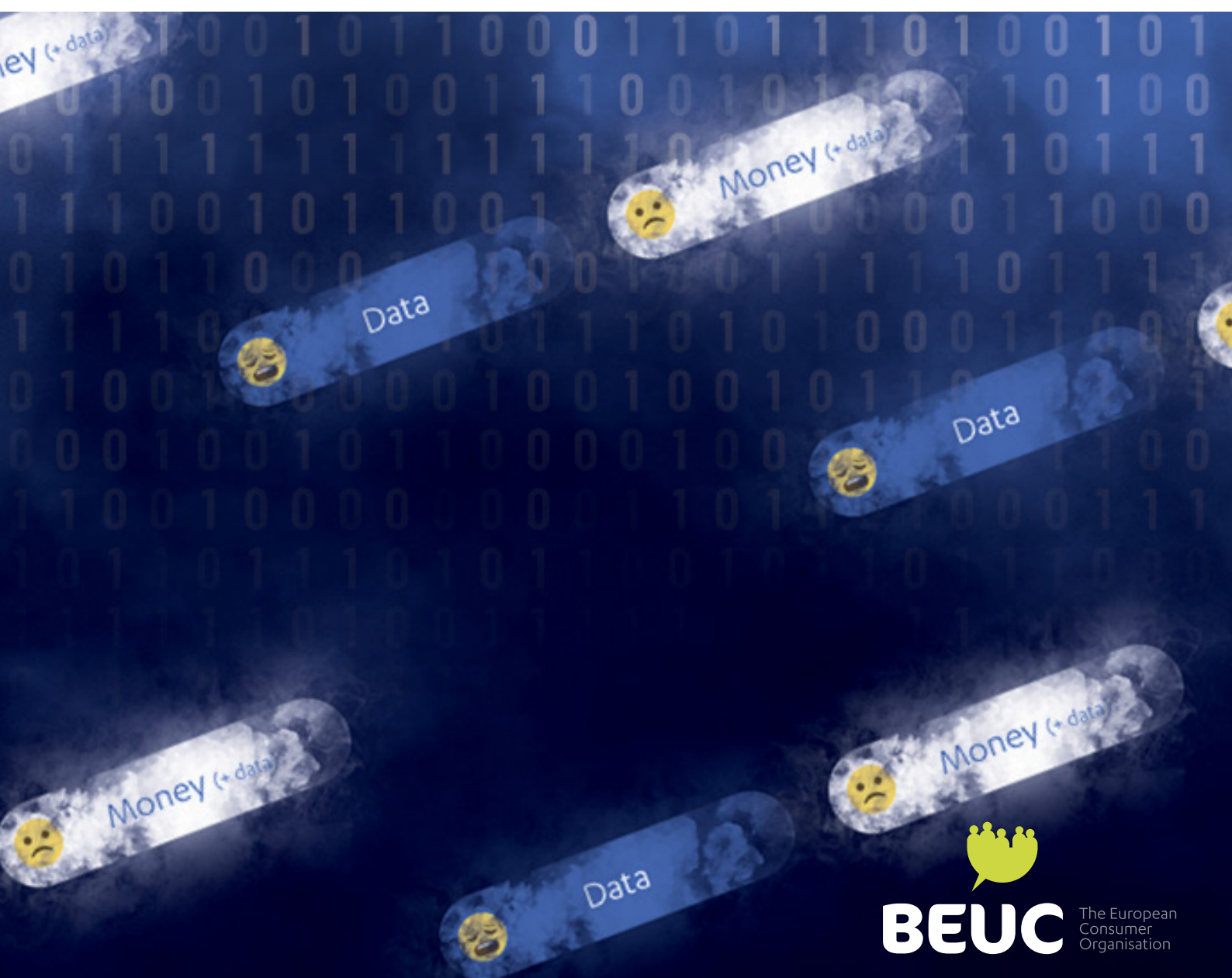




HOW META IS BREACHING CONSUMERS' FUNDAMENTAL RIGHTS



The European Consumer Organisation
Bureau Européen des Unions de Consommateurs
Europäischer Verbraucherverband

Rue d'Arlon 80,
B-1040 Bruxelles
Tel: +32 (0)2 743 15 90
www.beuc.eu
Contact: digital@beuc.eu

February 2024



co-funded by the European Union

Views and opinions expressed do not necessarily reflect
those of the European Union or EISMEA 2024

META HAS BEEN PROCESSING CONSUMERS' PERSONAL DATA ILLEGALLY SINCE 2018

In 2018, the GDPR¹ became applicable, requiring companies to have a valid legal basis for processing consumers' personal data.

Meta, a company with a business model that relies on the mass collection and processing of personal data at scale,² has been in the limelight for regulators for its data processing practices for many years. In a series of decisions in 2022 and 2023³, the Irish Data Protection Commission (DPC) and the Court of Justice of the EU (CJEU) have declared Meta's legal bases for processing personal data invalid. To be clear, this means that Meta has been operating for years without a valid legal basis for its processing of massive amounts of personal data about hundreds of millions of European consumers.

After being forced by regulators to comply with the GDPR, Meta has started, in November 2023, to ask consumers using Facebook and Instagram to give their consent to the processing of their personal data for advertising purposes or alternatively to pay a fee of up to 311 € per year.⁴

While public discussions revolve around this 'pay-or-consent' model, Meta carries on with its privacy-invasive business model. Each time regulators confirmed that the legal basis Meta relied on was invalid, the company has simply made changes in its privacy policy, while continuing its structural surveillance of consumers.

After analysing Meta's practices, BEUC and its members have found that Meta processes personal data in a way that is fundamentally incompatible with European data protection law, as it

1. breaches the data protection principles of the GDPR, such as the principles of purpose limitation, data minimisation, fair processing and transparency;
2. has no valid legal basis under the GDPR for its data processing.

This comes on top of the breaches of European consumer law, where BEUC and members already filed a complaint in November 2023⁵.

META'S COMMERCIAL SURVEILLANCE PRACTICES ARE FUNDAMENTALLY ILLEGAL

According to Meta's privacy policy, Meta collects and processes various categories of personal data about consumers for the purpose of behavioural advertising. Examples are data categories such as location-related information, how the consumer interacts with Meta's content and apps, as well as Meta's partners' content and apps.⁶

The vague wording Meta uses obscures the fact that Meta's data processing enables the company to infer private details about the consumer.⁷ Researchers have found that Facebook likes can be used to infer personal characteristics such as sexual orientation, political views, use of addictive substances, and parental separation.⁸ A consumer's clickstream pattern on a website can be sufficient to generate predictions for that person's education levels, and location data can be used to infer social ties between individuals, as well as the consumer's emotions.

Meta uses all this information to automatically profile and group consumers according to the likelihood that each consumer will click on an advertisement, make a purchase, or similar actions. In practice, this means that consumers can be profiled according to their sexual orientation, financial (in)stability, susceptibility for addictions, emotional state, and so on.

Meta seems to be of the opinion⁹ that in order for the company to earn money with advertising, it is justified to collect any imaginable data on consumers' activities, location, personalities, behaviour, attitudes and emotions. In reality, the massive exploitation of the private lives of hundreds of millions of European consumers for commercial gain fails to respect various fundamental principles of the GDPR enshrined in its Article 5(1), such as the principles of purpose limitation, data minimisation, fair processing and transparency:

- Meta's data processing is not limited to specified, explicit and legitimate purposes, as it profiles consumers for multiple purposes, without clarifying which types of profiling are necessary for which purposes.
- Meta fails to show that its data processing is limited to what is necessary, whereas it is questionable that the processing of every aspect of consumers' life would be necessary for the purpose of targeting ads towards them.
- Meta's data processing is inherently unfair, due to the company's use of its dominant position to force consent, and its frequent switching of legal bases in ways which frustrate the exercise of data subject rights. Additionally, while consumers can have a vague idea that Meta uses their data, they would not expect this to mean that their behaviour may lead to them being automatically classified as someone who is prone to addictions, for example.
- Meta's data processing is not transparent, as consumers are completely kept in the dark about the true extent of the processing, and the extent to which data is used for different purposes.

META IS STAGING A CONSENT MASQUERADE THAT DOES NOT ACTUALLY GIVE CONSUMERS A FREE CHOICE

While Meta's processing activities are as such already fundamentally in breach of several of the GDPR's core principles, the way Meta asks for consumers' consent is also highly problematic and according to our analysis in breach of European laws. BEUC and its members have already filed a complaint to the CPC network¹⁰ against Meta for using misleading and aggressive commercial practices to deceive and pressure consumers into giving up their data. The analysis of BEUC and its members shows that the way Meta asks for consent also does not comply with the GDPR.

Meta continues to process consumers' data without a valid legal basis, as the consent the company asks for is not valid. The GDPR requires consent to be, inter alia, freely given, whereas Meta is trying, with its consent model, to coerce consumers into accepting its processing of their personal data. Meta keeps consumers in the dark about its data processing, making it impossible for the consumer to know how the processing changes if they choose one option or the other. The company also fails to show that the fee it imposes on consumers who do not consent is indeed necessary, which is

a requirement stipulated by the Court of Justice of the EU (CJEU). Under these circumstances, the choice about how consumers want their data to be processed becomes meaningless and is therefore not free.

Meta also has a dominant position on the social network market. Facebook and Instagram (both Meta companies) each have over 250 million EU users, more than twice as many as the other big social networks Twitter, TikTok and Snapchat. Due to this market dominance and the network and lock-in effects that are inherent to social networks, consumers have no alternatives. Consumers using Facebook and Instagram who neither want to be tracked nor can or want to pay 311 € per year cannot simply switch to another social network provider, because they will not find their network of friends and family there.

It is crucial that any consent provided by consumers is valid and meets the high bar set by the law, which requires such consent to be free, specific, informed and unambiguous. This is not the case with Meta's 'pay-or-consent' model.

OUR REQUEST: META MUST OPERATE IN ACCORDANCE WITH EUROPEAN LAWS

Meta must stop any illegal processing of consumers' personal data, including for the purpose of advertising. Any illegally collected personal data must be deleted.

In addition, if Meta would like to use consumers' consent as legal basis for its data processing, it must ensure that this consent is indeed freely given, specific, informed and unambiguous, as required by the law.

LEGAL ANALYSIS: META BREACHES THE GDPR'S CORE PRINCIPLES

A legal analysis performed by BEUC and its members¹¹, together with Data Rights Law Firm AWO¹², concludes that the processing of consumers' personal data that Meta is engaged in breaches the GDPR in several ways:

- Meta's personal data processing for advertising purposes lacks a valid legal basis because it relies on consent which has not been validly collected for the purposes of the GDPR;
- Some of Meta's processing for advertising purposes appears to rely invalidly on contract;
- Meta cannot account for the lawfulness of its processing for content personalisation since it is not clear – and there is no way to verify – that all of Meta's profiling for that purpose is (a) necessary for the relevant contract and (b) consistent with the principle of data minimisation;
- It is not clear – and there is no way to verify – that all of Meta's profiling for advertising purposes is necessary for that purpose and therefore consistent with the principle of data minimisation;
- Meta's processing in general is not consistent with the principles of transparency and purpose limitation; and
- Meta's lack of transparency, unexpected processing, use of its dominant position to force consent, and switching of legal bases in ways which frustrate the exercise of data subject rights, are not consistent with the principle of fairness.

Endnotes

- ¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- ² Amnesty International, 2019, Surveillance giants: How the business model of Google and Facebook threatens human rights, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>.
- ³ Data Protection Commission, 31 December 2022, Final Decision: Meta Platforms Ireland Limited (Facebook service), <https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20DECISION%20%28ADOPTED%29%2031-12-22%20-%20IN-18-5-5%20%28Redacted%29.pdf>;

Data Protection Commission, 31 December 2022, Final Decision: Meta Platforms Ireland Limited (Instagram service), <https://www.dataprotection.ie/sites/default/files/uploads/2023-04/Meta%20FINAL%20Decision%20%28ADOPTED%29%20-%20IN-18-5-7%20-%2031-12-22%20%28Redacted%29.pdf>;

Judgment of the Court (Grand Chamber) of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, Request for a preliminary ruling from the Oberlandesgericht Düsseldorf, Case C-252/21, para. 117, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=275125&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=3214329>.
- ⁴ The monthly fee for one account is 12.99 € when subscribing via the mobile version of Facebook/Instagram, or 9.99 € when subscribing via the desktop version. Each additional account costs 8 € or 6 € respectively, but only if the consumer links these accounts in Meta's 'Account Center', which entails additional processing of personal data across Meta's services. A consumer using one Facebook and one Instagram account on a mobile device, and not wishing to have their personal data combined and used across these accounts, must pay 25.98 € per month, or 311.76 € per year.
- ⁵ BEUC, 2023, Choose to Lose with Meta, <https://www.beuc.eu/choose-to-Lose-with-Meta>.
- ⁶ For a full list, see: <https://www.facebook.com/privacy/policy/>
- ⁷ Amnesty International, 2019, Surveillance giants: How the business model of Google and Facebook threatens human rights, <https://www.amnesty.org/en/documents/pol30/1404/2019/en/>.
- ⁸ Privacy International, 2018, Examples of Data Points Used In Profiling, https://privacyinternational.org/sites/default/files/2018-04/data-points-used-in-tracking_0.pdf.
- ⁹ Meta, 2023, Facebook and Instagram to Offer Subscription for No Ads in Europe, <https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/>.
- ¹⁰ The Consumer Protection Cooperation (CPC) network is the network of consumer authorities in the Member States.
- ¹¹ CECU (Spain), dTest (Czech Republic), Forbrugerrådet Tænk (Denmark), Forbrukerrådet (Norway), EKPIZO (Greece), Spoločnosť ochrany spotrebiteľov (S.O.S.) Poprad (Slovakia), UFC-Que Choisir (France) and Zveza Potrošnikov Slovenije – ZPS (Slovenia) have filed GDPR complaints with their data protection authorities. Consumentenbond (Netherlands) has written to its national authority to alert them about Meta's practices.
- ¹² AWO, <https://www.awo.agency/>.

