IPRinfo VERKKOLEHTI
IPR UNIVERSITY CENTER

What happens to the data when users withdraw consent on social media platforms?

3/2025 17.6.2025

What happens to personal data when consent is withdrawn on a social media platform? This question is not only technically complex but also central to ongoing tension in the enforcement of European data protection law. This tension stems from the gap between the formal recognition of user autonomy and the practical realities of how data is processed in commercial environments. This article will argue that once consent is withdrawn, data controllers (social media platforms) must not attempt to continue processing personal data

under an alternative legal basis, as doing so undermines both the letter and the spirit of the General Data Protection Regulation (GDPR).

Although the GDPR is built upon the basis of individual autonomy, particularly through mechanisms such as freely given consent (Article 7(4) & Recital 42 GDPR), purpose limitation (Article. 5(1)(b)), and the right to withdraw consent at any time (Article. 7(3)), this autonomy is frequently challenged in practice. One of the most significant areas of tension arises when data controllers attempt to justify ongoing processing of personal data by switching from consent to another legal basis, such as contractual necessity or legitimate interests, especially after consent has been withdrawn. This practice raises concerns about whether user choice is truly respected or just procedurally acknowledged.

The debate, therefore, is not about whether autonomy is a foundational principle of EU data protection law; It unquestionably is. Rather, it concerns whether the actions of controllers, particularly large platforms, actually honor that autonomy in practice. When users withdraw consent, they are exercising a fundamental right under Article 7(3) GDPR. If a controller continues processing under a different legal basis without meaningful transparency, it undermines both user control and trust in the system.

Despite being one of the fundamental elements of the GDPR, the legal basis for personal data processing remains a contested area of enforcement. This is especially true when platforms attempt to shift from consent to alternative justifications like contractual necessity or legitimate interests. While Article 6 of the GDPR provides several legal bases for processing personal data, controllers are not permitted to shift from one legal basis to another, particularly after consent has been withdrawn. Such a change must comply with the GDPR's transparency obligations under Articles 13 and 14 and cannot be used to circumvent data subject rights.

This issue has come into sharper focus in the context of online behavioral advertising. Social media platforms, which have relied on user consent for personalized data practices, increasingly argue that such processing is essential to their business model or contractual performance. However, there has been a lot of legal and regulatory criticism against this strategic repositioning.

Two recent decisions reflect an institutional consensus on the limits of shifting legal bases for data processing is developing. First, the Court of Justice of the European Union (CJEU), in *Meta Platforms Inc. v. Bundeskartellamt* (C-252/21), held that Meta could not rely on contractual necessity or legitimate interests to justify extensive data combination and targeted advertising in the absence of valid consent. Second, the European Data Protection Board (EDPB), in its Urgent Binding Decision 01/2023, reinforced this interpretation by concluding that Meta's continued use of these alternative legal basis for behavioral advertising failed to meet the GDPR's requirements. While the CJEU clarified the legal interpretation, the EDPB's decision ensured that this position would be enforced uniformly across the EU.

This article explores the legal boundaries around consent withdrawal and shifting legal basis in detail, examining whether data controllers can continue processing by switching to a different legal basis. It also analyzes how EU bodies are increasingly challenging such shifts, particularly when companies involve invasive data practices and try to justify them by switching to legal grounds that are easier to use than consent.

GDPR Lawfulness of Processing (Article 6(1)(a), (b), and (f)) and EDPB Guidelines 05/2020 on Consent under Regulation 2016/679

What really happens to the data when users (data subjects) tell a social media platform, "No, I do not consent anymore"? According to the GDPR, these platforms, classified as data controllers and processors, are required to establish a legal basis for collecting and using your data, as outlined in Article 6 of the GDPR.

`ne common legal basis is Article 6(1)(a), which allows for data processing when a data subject has given freely, ¹fic, informed, and unambiguous consent. According to Recital 32, this consent must be given through

a clear affirmative action, no pre-ticked boxes or vague language. Platforms rely on this consent for personalized services such as behavioral advertising or facial recognition features (e.g., photo tagging). However, under Article 7(3), data subjects have the right to withdraw their consent at any time. According to this provision, the withdrawal of consent must be as easy as giving it. Controllers are also required under the principles of transparency and accountability to clearly inform users, prior to obtaining consent, of how consent can be withdrawn, and what will happen to their data in such an event (Recital 39 GDPR) . This is part of their obligation to provide clear and accessible information under Articles 12 and 13 of the GDPR . Importantly, withdrawal of consent has no impact on the legality of any data processing that took place before the withdrawal, as long as the original processing complied with the GDPR. In other words, any data processing carried out on the basis of valid consent remains lawful up to the point of withdrawal.

When the platform receives a user's valid withdrawal of consent, it must stop all data processing that depended on that consent. This includes not just the use of data, but also its collection, recording, structuring, and storage, regarding the broad definition of "processing" found in Article 4(2) . However, withdrawal of consent alone does not automatically result in the deletion of data that was previously stored. (Bartolini, Cesare, and Lawrence Siry. "The Right to Be Forgotten in the Light of the Consent of the Data Subject.")

There are different scenarios to consider at this stage:

First, if consent was the only legal basis for processing, and no other lawful grounds (such as legal obligations or legitimate interests) justify continued storage after you revoke the consent, the data controller must delete the data upon your request under Article 17 (1)(b) , the right to erasure. In this way, withdrawal of consent and the right to be forgotten can operate together: the former ends the lawful basis for processing, while the latter provides the means to request deletion of the data that is no longer lawfully held.

Second, if your personal data was originally processed based on multiple lawful bases, for instance both contractual necessity under Article 6(1)(b) and consent under Article 6(1)(a) , then withdrawal of consent only impacts the processing activities tied specifically to the consent. It does not require the deletion of data that remains necessary for fulfilling a contract or complying with a legal obligation. Therefore, controllers should ensure, prior to collection, that they map each processing purpose to a specific legal basis and document this to demonstrate compliance.

Third, in some cases where personal data was initially collected and processed solely on the basis of consent, the controller may, after withdrawal of consent, seek to continue processing that data under a different legal basis, such as Article 6(1)(b) or Article 6(1)(f).

For instance, under Article 6(1)(b), processing is permitted if it is necessary for the performance of a contract to which the data subject is a party. In the context of a social media platform, this could include processing personal data to maintain your account, manage login credentials, provide essential service notifications, or deliver core features integral to your agreement. In such cases, the withdrawal of consent does not invalidate this processing, because the legal basis shifts from consent to contractual necessity, provided that the purposes of the processing are clearly linked to the performance of the contract and were specified at the outset.

Another potential basis companies often refer is found in Article 6(1)(f), which allows processing based on the "legitimate interests" of themselves or a third party, as long as those interests are not overridden by the fundamental rights and freedoms of the data subject. This legal basis requires the controller to conduct a balancing test, weighing the legitimate interest against the potential impact on your privacy. Companies might argue that continued data processing is justified for reasons such as maintaining platform security, preventing fraud, or supporting product development. Recital 47 of the GDPR explicitly notes that direct marketing may constitute legitimate interest, though data subjects retain the right to object under Article 21(1).

However, according to the EDPB Guidelines 05/2020 on consent under Regulation 2016/679 (Paragraph 119 –

123) , controllers cannot silently migrate from consent to another legal basis. If the controller originally relied on consent as the sole legal ground, and that consent is later withdrawn, any attempt to continue processing under a different lawful basis must be communicated transparently to the data subject. This obligation stems from the information duties in Articles 13 and 14 , and from the general principle of transparency under Article 5(1)(a).

How does the CJEU ruling in the Meta decision add clarity?

The Court of Justice of the European Union's ruling in *Meta Platforms Inc. v. Bundeskartellamt* (C-252/21) marked a significant moment in clarifying the boundaries around shifting legal bases for data processing, particularly in the context of online platforms. The case arose from a challenge by Germany's competition authority, which had found Meta (Facebook) to be unlawfully conditioning access to its services on user consent to extensive data combination across Facebook, Instagram, WhatsApp, and third-party websites and apps.

At the heart of the CJEU's reasoning was whether Meta could lawfully justify its processing under Article 6(1)(b) (contractual necessity) or Article 6(1)(f) (legitimate interests) following the non-provision of valid consent (paras. 97-126) . While the CJEU's ruling was not about the withdrawal of consent specifically, the outcome can be relevant to the first and third scenarios above, in which consent is the sole legal basis for processing and, upon its withdrawal by the data subject, the platform seeks to continue processing the data under a different legal basis.

Meta argued that the data processing, used to deliver personalized ads and content, was necessary for the performance of its user contract or served its legitimate business interests, Meta Decision (paras. 94–127) .

The Court rejected this argument. First, the CJEU emphasized that contractual necessity under Article 6(1)(b) requires a strict and narrow interpretation: the processing must be objectively necessary to deliver the core features of the service the user signed up for, not simply desirable for the provider's business model (paras. 97-102) . Data combination for advertising and profiling purposes, while central to Meta's monetization, did not qualify as "essential" to the contract (para. 104)

Second, the Court examined whether Meta could rely on Article 6(1)(f) and justify the data processing through legitimate interests. This basis requires a three-part test, including the interest must be legitimate, the processing must be necessary for that interest, and the data subject's fundamental rights and freedoms must not be overridden (paras. 106-116) . While Recital 47 acknowledges that direct marketing can be a legitimate interest, the Court focused on the balancing test, not on whether Meta's advertising model qualified per se. In doing so, it emphasized users' reasonable expectations: even if they use free services, users do not reasonably expect that their data will be used for extensive behavioral profiling and personalized advertising, especially not without their clear and informed consent (para. 112).

The Court also raised broader concerns about the scale of Meta's practices. It warned against a system of "constant surveillance," where data collection may infringe on users' psychological autonomy and sense of freedom. Even if some users derive value from personalized ads, this must be weighed against the systemic risks to privacy, dignity, and personal control (paras. 118 & 121).

EDBP Urgent Binding Decision 01/2023 on Meta's Behavioral Advertising Practices

Following the CJEU's ruling *in Meta Platforms Inc. v. Bundeskartellamt* (C-252/21), on 14 July 2023, the Norwegian Data Protection Authority (NO SA) took action under Article 66(1) GDPR by issuing provisional measures to prohibit Meta from processing personal data of users residing in Norway for behavioral advertising purposes, where such processing was based on either contractual necessity (Article 6(1)(b)) or legitimate interest (Article 6(1)(f)).

Recognizing the cross-border impact of Meta's practices, the NO SA formally requested an urgent binding decision from the EDPB under Article 66(2) GDPR , asking for final and immediate enforcement measures to apply the European Economic Area (EEA). In its request, the NO SA stated that despite previous rulings by the

Irish Data Protection Commission (IE SA), Meta IE had not stopped the disputed processing nor provided sufficient documentation to demonstrate compliance to GDPR. It continued to rely on contractual necessity and legitimate interests to justify processing personal data for personalized ad targeting, including tracking what users click on, where they go, and how they interact with content (para. 97 EDBP Urgent Binding Decision 01/2023).

The EDPB agreed with this assessment. It concluded that Meta IE's reliance on Article 6(1)(b) GDPR for processing such data lacked justification, as location and ad interaction data were being used to decide what ads to show next. Even though Meta IE claimed this was allowed under its contract, the EDPB noted these practices still counted as behavioral advertising and required proper user consent (paras. 98–99 EDBP Urgent Binding Decision 01/2023).

Moreover, the EDPB expressed concern about Meta IE's reliance on Article 6(1)(f) GDPR. It found that even where Meta had transitioned from a contractual necessity to a legitimate interest basis, especially for data collected directly from its platforms, the processing still failed to meet the required three-part test under Article 6(1)(f). In particular, Meta did not convincingly demonstrate that its behavioral advertising was necessary for its stated legitimate interests (para. 121). It claimed that Facebook and Instagram could not remain free without processing user data for advertising purposes. However, the Irish Supervisory Authority (IE SA) said Meta had not proven that this specific type of advertising (which involves tracking and profiling users) is the only way it can make money or offer free services (paras 124– 126).

Furthermore, the authorities found that Meta's arguments seem to be vague and unconvincing, particularly demonstrating that its legitimate interests prevailed over the users' fundamental rights and freedoms, especially given the intrusive, large-scale, and technically complex nature of the data processing involved (paras. 137–140).

Ultimately, the EDPB ruled that Meta's reliance on legitimate interests could not justify the scope of its behavioral advertising model, which constitutes a continuing infringement of the GDPR. It held that this kind of extensive profiling only requires valid, informed, and freely given consent under Article 6(1)(a), which Meta had not sufficiently obtained (EDPB, Binding Decisions 1/2023 & 2/2023).

Analysis

The legal framework under the GDPR creates a layered and often complex reality for data processing. A single set of personal data may be subject to different legal grounds depending on the purpose. This means that when a data subject withdraws consent, the outcome depends on whether that processing activity was just consent-based or supported by another lawful basis. The GDPR requires that each purpose for processing be assigned a specific legal basis, and withdrawal affects only those purposes reliant on consent.

This leads to tension at the heart of the GDPR: on one hand, the regulation upholds user autonomy through informed, freely given, and revocable consent. On the other, it allows data controllers, like social media platforms, some flexibility to continue processing data under different basis. This flexibility can, in practice, weaken the user's ability to truly control their data after withdrawing consent. The EDPB, in paras 121-123 of its Guidelines 05/2020 on Consent, explicitly warns against "bundling" different legal basis or switching them after the fact (a practice known as post hoc justification). Such actions risk violating the GDPR's core principles of transparency and lawfulness under Articles 5(1)(a), 13, and 14 . Platforms must clearly inform users not only of the original legal basis for processing, but also of any changes to that basis, before continuing to use their data.

The EDPB and the CJEU are increasingly focusing on this issue. They have both criticized attempts by platforms like Meta to justify data processing, especially for behavioral advertising, by switching from consent to other grounds like contractual necessity (Article 6(1)(b)) or legitimate interest (Article 6(1)(f)). These ifications have been found to be inadequate and lacking transparency, especially when users have not been informed or when the data processing in question involves large-scale profiling or tracking. The CJEU has

made it clear that if consent was the original legal basis for a specific processing activity, the controller cannot simply switch to a different legal ground after consent is invalid. This was also reinforced by the EDPB's Binding Decision 01/2023 , which concluded that continued behavioral advertising based on other legal grounds rather than a valid consent, was unlawful under the GDPR.

Finally, controllers must actively assess whether continued retention or processing of data remains appropriate and proportionate, particularly when consent has been withdrawn. If no valid legal basis applies, the data must be deleted in line with Article 17(1)(b) , (the right to erasure when processing is no longer lawful). For social media platforms, this creates both a compliance burden and a reputational risk. They must not only document which legal basis applies to each processing purpose but also ensure that consent withdrawal is implemented in a way that truly stops unlawful processing. They must assess whether continued processing is justified, communicate transparently with users, and, where necessary, delete data without delay. Companies cannot undermine the right to withdraw by quietly shifting to other legal bases. Doing so risks not only regulatory penalties but also user trust.

In light of the developments described, any thorough analysis at this point must conclude that the ECJ has left nothing unclear in this context. It concluded that for data processing carried out for the purpose of behavioral advertising, platforms must not rely on contractual necessity and legitimate interest. However, after adopting this decision by the CJEU, Meta was still processing data based on the mentioned legal grounds, therefore, the binding decision was established by the EDBP following the request of the NO SA. That binding decision indicated that the platforms must get valid consent to process personal data for the purpose of behavioral advertising, and they must not rely only on legitimate interest and contractual necessity.

Main photo: phakphum patjangkata /iStock

Aiheet: Tietosuoja, data

Kirjoittajat

Sahar Karimi

Doctoral researcher University of Turku