Social media targeting: When to act and what to do

EDPB European Data Protection Board

GUIDELINES AT A GLANCE

November 2026

When your organisation targets specific audiences on a social media platform, you are doing more than just buying ad space. Social media users can be targeted through various methods.

This includes traditional personalised advertisements like banners, as well as content appearing in users' feeds, timelines, or stories alongside their organic posts.

Targeting may also occur through dedicated platform pages or other social media presences, third-party hosted content, or by integrating social media tools such as plugins, logins, application programming interfaces (APIs), or software development kits (SDKs) offered by social media providers.

The EDPB Guidelines on the targeting of social media users clarify the roles and responsibilities of the key actors involved in the targeting process.



Key actors in the targeting ecosystem

Social media users	Registered account holders using social media for different purposes including connection, information sharing, or job searching. Non-registered individuals may also be considered data subjects when they are identified or identifiable.
Social media providers	Organisations offering online platforms that facilitate user networking and community building, enabling information and content sharing among connected users. Social media providers increasingly gather data not only from activities on the platform itself, but also from activities undertaken 'off-platform'.

Targeters	Individuals or organisations using social media to deliver tailored messages to specific audiences based on selected criteria. They typically include brands (product advertising), political parties (campaign strategies), and non-profits (donor targeting/community building).
Other actors	This can include marketing providers, ad networks, ad exchanges, and analytics companies that track user activity across websites and apps. It can also include data brokers and data management providers (DMPs) which collect data from diverse sources (online/offline) and might sell it to targeting stakeholders.

Social media user targeting methods

Social media users may be targeted based on **provided**, **observed**, or **inferred data**.

Targeting with provided data

Provided data is information actively shared by users with social media platforms or targeters.

Examples:

- Profile information (e.g., name, date of birth, gender, age, current employment, address, relationship status and interests)
- Customer data (e.g., email lists) matched with platform data

Targeting with observed data

Observed data is information generated through user activity across platforms and devices.

Examples:

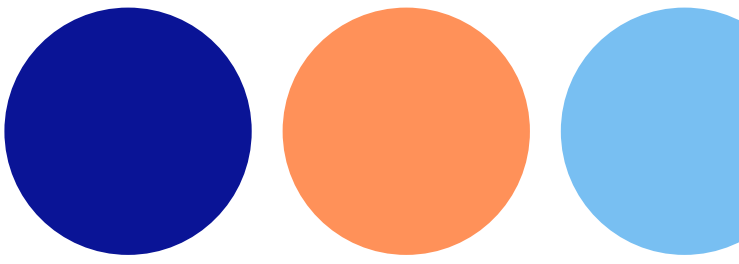
- Platform activity (content shared, viewed, or liked)
- Device data (GPS, phone number)
- Third-party app data (via APIs/SDKs)
- Third-party website data (social plugins/pixels)
- Purchases or loyalty programs
- Data from affiliated services

Targeting with inferred data

Inferred data is information created by controllers from provided or observed data.

Examples:

- Predicted interests based on browsing behaviour
- Likely preferences based on network connections



Key responsibilities at a glance

Your duties as a **targeter** apply before a campaign launches and continue throughout its lifecycle. **You cannot hide behind the platform's terms and conditions.** You share the responsibility for keeping the processing lawful, fair, and transparent, whether you target users based on personal data they **provided**, data you **observed**, or data you **inferred**.

When to act	What to do
Before launching a campaign	**Establish a joint arrangement.** You must have a clear, transparent arrangement with the platform detailing your respective responsibilities for GDPR compliance (Art. 26). **Ask yourself: Who is responsible for handling a user's request to access or delete their targeting data?**
When uploading customer lists	**Ensure a lawful basis.** If you upload a list of your customers' email addresses to find them on social media, you must have informed them of this specific use when you collected their emails. **Ask yourself: Did we tell our customers we would use their emails for social media advertising?**
When selecting targeting criteria	**Beware of sensitive data.** Targeting based on political views, health, or sexual orientation triggers strict Art. 9 GDPR rules, even if the user did not explicitly declare those traits. **Ask yourself: Could our targeting criteria indirectly reveal or exploit a user's sensitive personal data?**

Principles in practice: Key issues

The guidelines highlight several specific data protection points of attention:

1. Joint controllership is the standard

If you use a platform's targeting tools to define an audience, you are participating in determining the purposes and means of the processing. Therefore, you are a **joint controller** with the social media platform. The essential elements of the joint arrangement must be made available to the users, including how users can exercise their rights.

2. The legal basis: Consent vs. legitimate interest

- Consent is usually appropriate if you use profiling practices involving tracking individuals across multiple websites, locations, devices, services or data brokering.
- Legitimate interest might be possible for certain forms of targeting (e.g., advertising relates to services similar to those for which the individual is a customer), provided you inform the individual that their data can be used for that purpose and you offer a clear, easy way to object.

However, "Performance of a contract" is hardly applicable in the context of targeting of social media users.

3. Special categories of data

Inferring sensitive traits (like health status or political affiliation) from a user's clicks, "likes," or browsing history constitutes processing of **special categories of data.** This is strictly prohibited unless you meet strict conditions, for example obtaining the individual's explicit consent or using data that they have manifestly made public.

Practical examples

Here are specific scenarios illustrating how these rules apply in practice:

Example

Pixel-based targeting
(section 5.3, paragraphs 67-68, page 21, example 4)

Context: An online retailer wants to target social media users who visited their website but did not buy anything. They embed a social media "tracking pixel" on their site.



What to do: The retailer and the social media platform are joint controllers. In addition, the retailer should obtain the user's consent before the pixel collects any data.

Example

Inferred sensitive data
(section 8.1.2, paragraphs 123-125, pages 33-34, example 13)

Context: A social media platform tracks a user's "likes" and infers they are interested in left-wing politics. A political party then uses the platform's targeting tool to display ads to users in the "interested in left-wing politics" category.



What to do: Assigning a political opinion to a user constitutes processing of special categories of data (Art.9 GDPR), which is in principle prohibited. Both the platform and the political party must ensure they rely on a valid exemption, such as the user's **explicit consent**, before using this inferred category for targeting.

Example

List-based targeting/custom audiences
(section 5.2.2, paragraphs 60-66, pages 19-20, examples 2-3)

Context: A bank uploads a list of its customers' email addresses to a social media platform to display targeted ads for new financial services to those specific people.



What to do: The bank is the sole controller for the initial collection of the email addresses, but a joint controller for the targeting phase. The bank must ensure it has a lawful basis to use the email addresses for this purpose. If a customer only provided their email address to book an appointment and decided not to use the bank, their email address should not be used for social media targeting.

This document provides a simplified overview of the opinion. For more comprehensive legal explanations and examples, please consult the full text of the opinion.

Read the complete guidelines