GDPR and DSA
how they interact

EDPB European Data Protection Board

November 2025

The European Union has introduced a series of digital laws to create a safer, fairer, and more transparent online environment that protects users' rights and ensures accountability for digital platforms. When implementing these laws, organisations should be mindful of ensuring the protection of individuals' personal data.

One of these laws is the Digital Service Act (DSA), to create a safe online environment in which the fundamental rights of all users are protected. The DSA applies to online intermediary services, such as search engines and online platforms.

Several provisions included in the DSA entail the processing of personal data.

The EDPB guidelines on the interplay between the DSA and the GDPR help to understand **how the GDPR should be applied in the context of DSA obligations**.

The guidelines focus on specific parts of the DSA where there is a significant interplay with the GDPR.

Scenario 1

Reporting illegal content

Providers of hosting services that store, manage, and make user-generated content available online on behalf of their users must set-up **notice-and-action** systems for reporting illegal content.

Hosting providers should only collect necessary personal data. Notification systems should allow users to report anonymously, unless the identification is needed to verify the claim. If it is necessary to reveal the notifier's identity to those affected, the notifier should be informed beforehand.

Scenario 2

No targeted ads addressed to children

Providers of online platforms should **not show targeted advertisements to users if they know that the user is a minor.**

Online platforms do not need to collect extra personal data to confirm if a user is a child. It is possible to know if a child is using a service in other ways too: for example, if the service is clearly for children (like child-friendly content), or if there are already user data showing the age of individuals for another reason.

Scenario 3

Avoiding invasive age verification systems

Providers of online platforms should **guarantee a high standard of privacy, safety, and security for all users.** Among these users, the online safety and protection of minors remains an increasingly significant concern.

The assurance of the age of an individual can take place without identification of the user by the platform. In general, organisations should **avoid age verification mechanisms that enable unambiguous online identification of their users** (e.g., by asking them to submit proof of their identification via government-issued ID). If age estimation is necessary, providers should limit personal data processing to what is necessary (e.g. if an age range provides reasonable certainty that the recipient of the service is a minor, the exact date of birth should not be verified) for age estimation and should only store that the user fulfils the conditions to use the service.

Scenario 4

Offering a no-tracking option

Providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) use **recommender systems** to automatically show tailored content (like products, posts, or services) to their users. This content appears in a specific order and prominence, based on the users' activities, preferences, or behaviours (such as purchases, clicks, or ratings).

VLOPs and VLOSEs should offer at least one option for each of their recommender systems which is not based on profiling. This means that **this alternative option should not track individuals' behaviours or personal data.** While the non-profiling-based option is active, the provider of the online platform should not continue to collect and process personal data to profile the user for future recommendations. Both options should be shown equally the first time that the service is used.

Scenario 5

Avoiding targeted ads relying on sensitive data

Certain types of personal data, such as health details, religious beliefs, or political views, are highly sensitive.

According to the DSA, providers of online platforms **should never present targeted advertisements to users based on this kind of data**.

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

Read the complete guidelines