Contractual necessity for online services
When to act and what to do

EDPB European Data Protection Board

GUIDELINES AT A GLANCE

March 2026

The General Data Protection Regulation (GDPR) allows the processing of personal data when it is “necessary for the performance of a contract.” This is a key lawful basis for providing online services.
However, this basis is not a “catch-all” for any data processing mentioned in a contract. It strictly covers what is objectively necessary to deliver the core service.

The EDPB Guidelines on the processing of personal data under Article 6 (1) (b) GDPR in the context of the provision of online services to data subjects clarify when this lawful basis applies. In particular, the Guidelines highlight that, while processing operations that are essential for the service to function may rely on this lawful basis, this is not the case for additional processing activities that are not inherently linked to the provision of the service (e.g., as a general rule, processing for online behavioural advertising).



The core concept: Objective necessity

Your strict limit. Just because a processing activity is written into a contract does not make it lawful under this basis. The processing must be objectively necessary to perform the service.

Key principle	What you need to know
Objective necessity	**Ask yourself: Can the service technically function without this specific data processing?** If yes, then the processing is not “necessary” for the contract, even if it is useful for your business.
Separation of services	If a contract bundles multiple services, you must assess necessity for each one separately. This means that you need to assess what is necessary to provide the individual service(s) that the user actively signed up for, not what is necessary for the package as a whole.
Pre-contractual steps	This legal basis also covers steps taken at the request of the individual before signing a contract (e.g., providing a quote based on a postal code).

Principles in practice: Key steps for organisations

When relying on contractual necessity, organisations must distinguish between core service delivery and other business interests like **service improvement**, **fraud prevention**, and **advertising**.

1. Service improvement

Collecting data to improve your service or develop new features is generally **not necessary** for performing the current contract.

- **The rule:** You cannot rely on contractual necessity for service improvement analytics. You must find another lawful basis (usually **legitimate interest** or **consent**).

2. Fraud prevention

While preventing fraud is important, it is rarely "necessary for the performance of the contract" itself.

- **The rule:** Profiling customers for fraud prevention usually goes beyond contractual necessity. In this case, you may be able to rely on **legitimate interest** or a **legal obligation** (if applicable).

3. Behavioural advertising

Tracking user behaviour to fund a "free" service via ads should not in itself be considered necessary for the performance of the contract.

- **The rule:** In general, tracking and profiling users to personalise ads is not "necessary for the contract". You must obtain **consent** before placing cookies used for tracking and behavioural advertising.

Practical examples

Here are specific scenarios illustrating how to apply these rules:

Example

(section 2.5, example 1, page 10)

Context: An online retailer processes a customer's home address for delivery and credit card details for payment.



What to do: This processing is lawful under the GDPR because the contract (delivering goods) cannot be performed without this data.

Contrast: If the customer chooses a "pick-up point" instead of home delivery, processing the home address is no longer necessary for the contract. You must stop processing the home address or find another lawful basis.

Example

(section 3.4, example 7, page 16)

Context: A hotel search engine tracks a user's past bookings to build a profile of their spending habits and recommend hotels.



What to do: You should not rely on contractual necessity. Profiling spending habits is not objectively necessary to provide the service. You should obtain **consent** or consider whether it is possible to rely on **legitimate interest** for this personalisation.

Example

(section 3.4, example 8, page 16)

Context: An online marketplace personalises product suggestions based on a user's viewing history to increase interactivity.



What to do: You should not use the contract as a valid basis. While useful for engagement, personalisation is not "objectively necessary" to run the marketplace. You should obtain **consent** or consider whether it is possible to rely on **legitimate interest**.

Your action plan for contractual necessity

Data controllers should rigorously assess their contracts.
Use this checklist to ensure compliance:



Action point	Why it matters
1. Audit your contracts	Review your terms of service. Identify which data processing is actually essential for the service vs. what is merely "useful."
2. Remove "bundling"	Do not force individuals to agree to marketing or tracking as part of the service contract. These require separate consent.
3. Check termination rules	If a contract ends, you generally should stop processing the data based on contractual necessity. Ensure you have data retention/deletion policies in place.
4. Define "necessity" strictly	If you can deliver the service without a specific piece of data, you cannot argue that it is necessary to perform the contract.
5. Be transparent	Clearly explain in your privacy notice which legal basis applies to which processing activity. Do not confuse "signing a contract" with "giving consent."

By strictly applying the "necessity" test, you ensure that your reliance on contractual performance is robust and lawful.

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