Controllers & the processing chain: When to act and what to do

EDPB European Data Protection Board

OPINIONS AT A GLANCE

October 2026

When your organisation (acting as a **data controller**) relies on a service provider (**data processor**) to process personal data on your behalf, you remain responsible for the protection of personal data. This responsibility extends down the entire "processing chain" (i.e. the processors of your processor, or sub-processors, sub-sub-processors, etc.).

The EDPB Opinion on certain obligations following from the reliance on processor(s) and sub-processor(s) clarifies how deep a company's oversight should go. You should know who is processing your data and ensure they provide sufficient guarantees, regardless of how long the chain is.



Key responsibilities at a glance

Your duties as a controller apply continuously throughout the lifecycle of the data processing. Here is a checklist of your organisation's key responsibilities at each stage:

When to act	What to do
At all times	**Maintain specific identity information.** You should have the name, address, and contact person of **every** processor and sub-processor in the chain and the description of the processing "readily available". The information should be kept up to date. **Ask yourself: If an individual asks "who has my data?", can I easily provide the full list?**
Before involving a service provider (initial processor)	Before involving a service provider and afterwards regularly, **verify whether the guarantees and measures implemented by your chain of processors are sufficient**. You should ensure that the reliance on a service provider (and their sub-processors) does not lower the level of protection for individuals.

When to act	What to do
	You should ask the service provider to provide relevant documentation on this. **Ask yourself: Are you able to demonstrate that you are satisfied with the guarantees and measures implemented by your processor and the chain of sub processors?**
When transfers occur	**Map the flows.** If a sub-processor transfers data outside Europe (including remote access), your organisation is responsible for the transfer. You should verify the transfer tool and where relevant the Transfer Impact Assessment (TIA). **Ask yourself: Do I know where the data is going, even at the bottom of the chain?**

The verification spectrum: A risk-based approach

Organisations have a duty to verify that all processors in the chain provide "sufficient guarantees". However, the **depth** of this verification varies depending, among other criteria, on the risk to the rights and freedoms of individuals.

1. Low to medium risk

- **Action:** Assess the information and documentation provided by your initial processor. Rely on certifications or audit reports from trustworthy third parties, where possible. Address any questions (e.g. information is incomplete or inaccurate), including on the basis of publicly available information.

2. High risk

- **Action:** You should increase your level of scrutiny of the guarantees. Relying solely on the initial information and documentation received by the initial processor may not be enough.
- **Documentation:** You should consider requesting copies of **sub-processing contracts** to verify that data protection obligations have been passed down correctly down the chain.

Goal: Demonstrate to the Data Protection Authority (DPA) that your organisation has actively checked the guarantees put in place (accountability).

Principles in practice: Key issues

1. Sub-processing contracts

You do not have a duty to systematically read every single contract in a long processing chain. However, you should assess **case-by-case** whether requesting a copy is necessary to demonstrate compliance.

- **Right to audit:** Your contract with the initial processor should allow you to request these documents.
- **What to check:** Ensure that the same data protection obligations you imposed on your service provider (initial processor) are imposed on the sub-processors.



2. Transfers outside Europe

If your service provider (or their sub-processor) transfers data to a third country, both your organisation and the data exporter may bear obligations under Chapter V of the GDPR, depending on the circumstances of the transfer. You must ensure that any such transfer in the chain is covered by a valid transfer mechanism.

- **Mapping:** Ensure your service provider maps out all transfers, including "remote access" from third countries. Distinguish transfers covered by an adequacy decision from those subject to another transfer mechanism.
- **Safeguards:** You should verify that a valid transfer tool (e.g. Standard Contractual Clauses (SCCs)) is used. Verify if a Transfer Impact Assessment (TIA) has been conducted and if possible supplementary measures have been put in place. You can build on your processor's assessment, but you should ensure safeguards are effective.

3. Instructions provided to a processor, "unless required by law"

The GDPR states that a processor must follow your instructions unless required to do otherwise by European Union or EU/EEA Member State law. Some contracts try to expand this by saying "unless required to do so by law or binding order of a governmental body" (implying laws of any country, including outside the EU/EEA).

- **Is this allowed?** Whilst this broader wording may not automatically render a contract non-compliant, it does not relieve the processor of its GDPR obligations — and it should be assessed carefully, including through a Transfer Impact Assessment (TIA), to determine whether it undermines the required level of protection.
- **The risk:** A vaguely worded clause does not turn a foreign government's request into a lawful documented instruction from you as controller to fulfil the request.
- **Good practice:** It is highly recommended to stick to the specific GDPR wording (European Union or Member State law). If a service provider is subject to third-country laws, this should be assessed separately (e.g., via a TIA) to ensure the level of protection is not undermined.

Practical examples

Here are specific scenarios illustrating how to apply these rules:

Example

(section 2.1.3, paragraph 70, page 19)

Context: You discover from publicly available information (or a notification) that your main cloud provider's sub-processor has suffered a data breach.

What to do: The obligation to use processors with sufficient guarantees is a continuous one. You should ask your main service provider for a copy of the sub-processing contract (on the basis of your right to audit). You should review it to verify the security guarantees and data protection obligations passed down to that sub-processor. You should not just blindly rely on the main vendor's assurances once a doubt arises.

Example

(section 2.2, paragraph 88, page 22)

Context: A service provider provides you with a mapping of transfers to their sub-processors, but the mapping fails to specify where the sub-processors are processing the data, or it omits that IT support from a non-European country has "remote access" to the data.

What to do: You should ask for additional information, verify and complete the mapping if necessary. Remote access from outside Europe constitutes a transfer, and your organisation needs a complete picture to fulfil your transparency duties (like updating the privacy notice) and ensure proper safeguards are in place.

Example

(section 2.3, paragraphs 116-132, pages 30-34)

Context: Your processor proposes a contract stating they will follow your instructions "unless required to do so by a binding order of a governmental body."

What to do: This wording should be a red flag where transfers of personal data outside the EEA in the processing chain are concerned. Further analysis of the circumstances would be needed, and this wording should not be considered a documented instruction by the controller to share data with foreign governments.

The accountability checklist

Your organisation's action plan for compliance in the processing chain:

Action point	Why it matters
1. Request the full list	Demand that your service providers proactively provide the identity of all their sub-processors. You should not wait for a security incident to ask for this info.
2. Review your contracts	Ensure your contracts explicitly require the service provider to keep the sub-processor list up to date and to inform you of changes before they happen.
3. Audit based on risk	Do not treat all processors the same. Focus your detailed audits and document requests on processors handling sensitive data or high volumes of data.
4. Check the "unless" clause	Review your Data Processing Agreements. If they mention "compliance with other laws", ensure this is not understood as a possibility for third-country government access without your knowledge.
5. Monitor transfers	Verify that your service providers are not relying on sub-processors in third countries without a valid transfer mechanism and (where needed) a proper Transfer Impact Assessment.

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 opinion