Data transfers & certification: When to act and what to do

EDPB European Data Protection Board

GUIDELINES AT A GLANCE

May 2026

When your organisation (the **data exporter**) transfers personal data outside Europe to a third party (the **data importer**), you must ensure that the data remains protected in line with EU standards. Under the GDPR, one way to guarantee this is by using an approved **certification mechanism**.

The EDPB Guidelines on certification as a tool for transfers clarify how certification can be used as a transfer tool. For certification to be used as a transfer tool, the data importer must hold a valid certification and you must both sign binding, enforceable commitments to uphold those privacy standards.



Key responsibilities at a glance

Your duties as a data exporter apply before the transfer takes place and continue throughout the processing lifecycle. Here is a checklist of your key responsibilities:

When to act	What to do
Before transferring data	**Verify the certification.** You must ensure the importer's certification is valid, not expired, issued by an accredited body, and explicitly covers the specific transfer you are making. **Ask yourself: Does this certification actually cover the exact data processing and transit routes we intend to use?**
During contract negotiation	**Make it binding.** You must implement a contract (or other legally binding instrument) that legally binds the importer to the certification's rules. **Ask yourself: Does our contract explicitly reference the certification and grant enforceable rights to individuals?**

When to act	What to do
When assessing local laws	**Review the legal landscape.** Ensure the importer has assessed their local laws, that they provided a warranty that nothing prevents them from complying with its commitments under the certification, and that effective supplementary measures will be put in place where necessary to protect data from foreign governments requests. **Ask yourself: Could foreign laws override the safeguards promised by this certification?**
When handling government requests	**Demand transparency.** Require the importer to notify you promptly of any third-country government data requests and to challenge disproportionate requests. **Ask yourself: Will we know if a foreign authority demands access to the transferred personal data?**

Principles in practice: Key issues

Relying on certification as a transfer tool requires a **two-step approach**, like in other transfer scenarios: you must first comply with general GDPR principles (like having a lawful basis for the transfer) and then apply the Chapter V transfer rules. To satisfy the transfer rules, three elements must be addressed:



1. Binding and enforceable commitments

The GDPR requires that the data importer takes on legally binding commitments to apply the appropriate safeguards, in case certification is used as a transfer tool. This is typically done by including specific clauses that refer to the certification in your existing service agreement or Data Processing Agreement signed with the importer.

Crucially, these commitments must grant **third-party beneficiary rights** to individuals, allowing them to directly enforce the rules and seek compensation against the importer before a European court or lodge a complaint with Data Protection Authority (DPA).

2. Assessing third-country legislation

The certification criteria should require the importer to conduct and document an assessment of the laws and practices in their country. As the exporter, you must obtain a **warranty** from the importer stating that they have no reason to believe their local laws (including government access measures) and practices prevent them from fulfilling their obligations under the certification rules.

3. Redress and enforcement

Individuals must have an effective way to complain. The certification must ensure that individuals can lodge complaints with a European DPA. The importer must agree to cooperate with your European DPA, submit to audits, and abide by their decisions and remedial measures.

The accountability checklist

Your organisation's action plan for relying on certification for international transfers:

Action point	Why it matters
1. Verify the exact scope	A certification is not a blanket approval. You must verify that the importer's target of evaluation (ToE) precisely matches your transfer (categories of personal data, purposes, etc.) and check possible onward transfers and the safeguards provided.
2. Secure third-party rights	Your contract must explicitly give data subjects the power to enforce the certification's rules against the foreign importer before a European court.
3. Check the legal warranty	You remain responsible for the transfer. You must verify the importer's documented assessment proving that local laws will not breach the certification.
4. Establish an access protocol	Ensure the importer has a mandatory, documented process to notify you if foreign authorities demand access to the data, and an obligation to minimise any disclosures.
5. Align supplementary measures	If supplementary measures have to be put in place by the importer, such as safeguards (like encryption) to protect the data from foreign governments, you must ensure your own systems are configured to match and support those measures.

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

Read the complete guidelines