

Third-country transfers: what the GDPR says about transferring data outside the EEA

One of the General Data Protection Regulation's (GDPR) key aspects is that it aims to ensure that the level of data protection remains consistent throughout the processing chain, especially if personal data leaves the European Economic Area (EEA). This is why the GDPR the GDPR limits your ability to lawfully transfer personal data to third-countries, by requiring personal data and individuals to be protected to a standard essentially equivalent to that in the EU.

Therefore, when your startup transfers – meaning, discloses, shares or otherwise gives access, even if remotely – personal data to employees, service providers, vendors, etc. located outside the EEA, then you need to fulfil the GDPR's requirements for third-country transfers.

You can do this in two main ways.

Adequacy Decisions: The green light

Adequacy decisions are the most straightforward way to lawfully transfer personal data from the EEA to a third-country.

When the European Commission determines that a non-EU country ensures an adequate level of data protection, data can flow freely from the EU to that country without needing extra safeguards or authorisations. For your business, this removes much of the compliance burden: you don't have to set up additional contracts or undertake assessments for those jurisdictions.

Currently, countries and territories with adequacy decisions include Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay. The EU-US Data Privacy Framework also grants adequacy status to participating US organisations that self-certify and commit to its principles.

To verify if your data transfer destination benefits from an adequacy decision, check the [official website](#) for an up-to-date list. Adequacy decisions can change, so you must do

periodic reviews and stay updated. If your destination loses its adequacy status, you'll need to pivot to alternative data transfer mechanisms to remain compliant.

Standard Contractual Clauses: Your go-to if there is no adequacy decision

Standard Contractual Clauses (SCCs) are pre-approved agreements issued by the European Commission, that businesses use to make sure personal data sent outside the EEA still benefits from adequate protection if the destination country does not have an adequacy decision.

There are different sets of SCCs, tailored for specific transfer scenarios. For example, controller-to-controller SCCs are used when two independent companies exchange data, whereas controller-to-processor SCCs apply when the transfer is to a service provider processing data on your behalf. Therefore, it is important to understand the role you and your counterparties play in the data processing so that you choose the right clauses.

To implement SCCs, you must insert the full, unmodified text of the relevant clauses into your contracts with vendors or partners located outside the EEA. You also need to clearly outline the technical measures and data processing details that the SCCs require.

Since the Court of Justice of the EU's Schrems II judgment, using SCCs also requires conducting a transfer impact assessment (TIA). This means you need to evaluate the destination country's laws and practices to confirm that the level of protection is similar to that of the EU and that data subjects' rights remain protected. If a risk is identified, you must implement supplementary measures – such as encryption, pseudonymization, or organizational controls – to fill any protection gaps. If you reach the conclusion that an adequate level of protection cannot be reached, then, even with SCCs, you cannot transfer personal data to these countries and ought to i.e. anonymize it beforehand.

Other mechanisms

While you should aim for countries subject to an adequacy decision or, if absent, adopt SCCs and a TIA, the GDPR includes other mechanisms for specific use-cases.

For example, Binding Corporate Rules (BCRs) are a solution for multinational groups that need to transfer personal data within their entities located in different countries outside the EEA. They are internal rules approved by supervisory authorities, setting out the group's overall

approach to data protection and the GDPR. As such, they make sense for larger businesses needing an internal transfer solution.

Aside from BCRs, the GDPR also recognizes codes of conduct and certification mechanisms as transfer safeguards. These mechanisms are suited to businesses looking for sector-specific frameworks or wishing to demonstrate compliance via recognized standards. However, adoption is slower as industry-wide codes and certifications are still being developed and approved.

Where to start

Choosing the right mechanism depends on your company structure, transfer frequency, and available resources. While this is an ongoing compliance process, there are some first steps you can take:

1. If you haven't done so already, start by mapping your data flows and focus on identifying the instances where personal data leaves the EEA. Common examples include transfers of personal data for purposes of cloud storage, digital marketing, as well as to remote workers and freelancers.
2. Next, include GDPR compliance checks into your vendor selection and onboarding processes. Make sure all third parties processing personal data outside the EEA meet applicable requirements and document their safeguards during procurement and due diligence. For that, assign responsibility for documenting decisions, risk assessments, and contracts to specific individuals within your startup.
3. Maintain records of transfer mechanisms (such as adequacy decisions, SCCs, or BCRs) for each transfer. Schedule reviews to confirm that your cross-border transfers remain compliant.

Francisco Argá e Lima

January 2026

Paxlegal

✉ paxlegal@paxlegal.pt

🌐 www.paxlegal.pt

📍 Av. Eng. Duarte Pacheco, Torre 1
14.º andar – Sala 1
1070-101 Lisboa, Portugal