European Commission

Digital Single Market

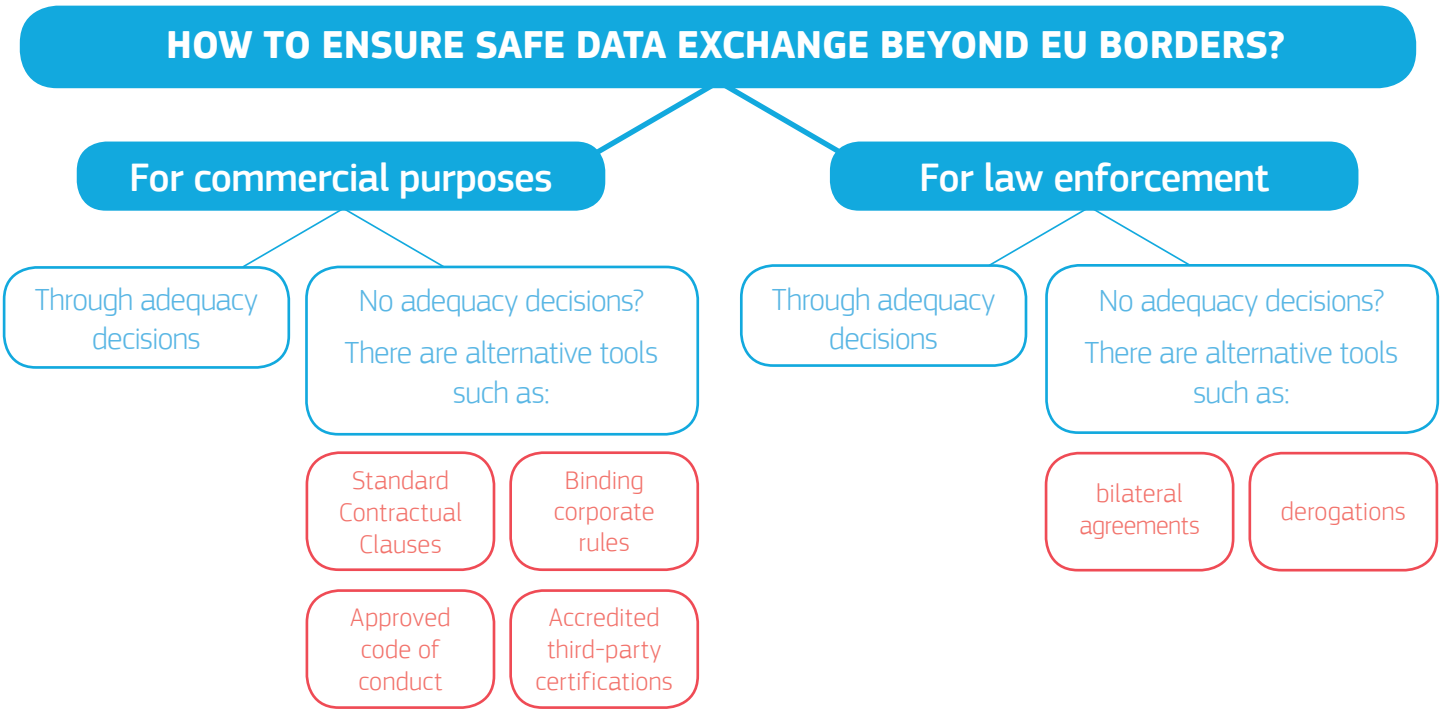
Commission strengthens trust and gives a boost to the data economy

Protection and exchange of personal data in a globalised world

A strong data protection system facilitates data flows by building consumer confidence in the companies that handle their personal data carefully. Companies recognise that strong data protection rules give them a competitive edge, as their customers trust their services.

The same is true for law enforcement cooperation: privacy safeguards are an integral part of the effective and swift exchange of information in the fight against crime. Mutual trust and legal certainty rely on clear and strong data protection standards.

In its Communication on exchanging and protecting personal data in a globalised world, the Commission sets out its strategy on how to facilitate the transfer of personal data to non-EU countries, while ensuring a high level of protection. The Commission will explore the feasibility of adequacy decisions with interested key trading partners. This will contribute to improving law enforcement cooperation, facilitating trade and developing high personal data protection standards globally.



ADEQUACY DECISIONS

What is an adequacy decision?

It is a decision taken by the Commission guaranteeing that a third country provides a comparable level of protection of personal data to that in the EU, through its domestic law or its international commitments. As a result, personal data can flow from the 28 EU Member States and the three European Economic Area (EEA) member countries (Norway, Liechtenstein and Iceland) to that non-EU country, without being subject to further safeguards or authorisations.

What countries are recognised by the EU as providing adequate data protection?

These decisions concern countries that are closely integrated with the European Union and its Member States (Switzerland, Andorra, Faeroe Islands, Guernsey, Jersey, Isle of Man), important trading partners (Argentina, Canada, Israel, the United States), and countries that have a pioneering role in developing data protection laws in their region (New Zealand, Uruguay).

The EU-U.S. Privacy Shield framework ensures adequate data protection to companies abiding by the privacy principles set out in the Shield.

What are the criteria to assess adequacy?

The Commission assesses whether the non-EU country's system offers a level of data protection comparable to the ones in the EU, by analysing both the protections relevant to personal data and the relevant oversight and redress mechanisms available in this country. This also includes the review of the limitations and safeguards applicable to access to personal data by public authorities for law enforcement and national security purposes.

The Communication sets out four key criteria to guide the Commission's approach in its dialogue on adequacy with new partners. The Commission will prioritise discussions with key trading partners in East and South-East Asia, starting with Japan and South Korea as well as in Latin America and the European neighbourhood.

ALTERNATIVE TOOLS TO ADEQUACY DECISIONS

The General Data Protection Regulation provides a set of tools that are flexible enough to adapt to the needs of specific industries or business models.

Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs)

SCCs and BCRs already exist, but the General Data Protection Regulation simplifies and expands their possible uses.

In the absence of an adequacy decision, it will now be possible to use SCCs for "processor-to-processor" transfers. This is particularly relevant for the processing of personal data by cloud service providers which, for operational reasons, may often transfer personal data outside the EU.

BCRs, which currently are limited to entities within the same corporate group, can now also be used for transfers between different corporate groups engaged in a joint economic activity. This could cover for example the transfer of personal data between different flight carriers belonging to the same airline alliance.

These new possibilities should help develop instruments that are better targeted to the needs of particular sectors or industries, business models or operators. In addition, the GDPR further facilitates the use of these mechanisms by abolishing the existing general requirement of notification to and authorisation by national data protection authorities of international transfers based on SCCs and BCRs.

Approved codes of conduct and accredited third-party certifications

New transfer mechanisms such as approved codes of conduct and accredited third-party certifications provide companies with the possibility to introduce tailor-made solutions for international transfers while benefiting from the competitive advantages associated, for example, with a privacy seal or mark.

TRANSFERS FOR LAW ENFORCEMENT PURPOSES

The swift exchange of personal data is key for successful law enforcement cooperation and an effective response to transnational crime. To strengthen legal certainty and build mutual trust amongst law enforcement authorities, these exchanges rely on strong data protection safeguards. To that end, the Commission will:

- Promote the possibility for adequacy decisions under the Police Directive with qualifying third countries.
- Promote the negotiation of agreements in the area of law enforcement with important international partners along the model provided by the Umbrella Agreement with the U.S.
- Work to facilitate the cross-border exchange of e-evidence in conformity with data protection rules.