COMPLIANCE PARTNERS

Key takeaways

GDPR COMPLIANCE:

WHAT TO CONSIDER BEFORE TRANSFERRING PERSONAL DATA GLOBALLY

Table of Contents

Introduction to GDPR and Third Country Transfers

The GDPR (General Data Protection Regulation) is designed to protect individuals' personal data within the EU and ensure that companies process this data in a transparent and lawful manner. In the case of international transfers, especially to countries outside the EU/EEA, companies need to take extra precautions to ensure that the level of protection required by the GDPR is maintained.

Third-country transfers are particularly relevant for companies working with global partners, suppliers or services located outside the EU/EEA area. It can be a legal and technical challenge to ensure that transfers take place in a secure manner.

Key principles for Third Country Transfers under the GDPR

Adequate level of protection:

- The European Commission assesses whether a third country offers an adequate level of protection for personal data.
- Countries with an adequate level of protection include Andorra, Argentina, Japan, and the United Kingdom.

The Schrems judgment:

- This ruling overturned the EU-US Privacy Shield agreement, which forces companies to use alternative mechanisms like SCCs to transfer data legally.

Transfer mechanisms:

- Options such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) are used to ensure that data is transferred in a legal and secure manner.

Glossary

SCCs (Standard Contractual Clauses): standard contractual clauses approved by the EU to allow lawful transfers of personal data to third countries.
Binding Corporate Rules (BCRs): internal rules of multinational companies that allow the transfer of data within the same group of companies, even outside the EU.
Transfer Impact Assessment (TIA): A risk assessment carried out when personal data is transferred to third countries to ensure compliance with data protection laws.
Schrems II: An important ruling that invalidated the EU-US Privacy Shield agreement, changing how data transfers between these countries are regulated.
Pseudonymization: A method of reducing risks in data processing by replacing identifying information with artificial data.

Transfer of Personal Data: Schrems, SCCs and TIA

Schrems I and II: Impact on Transfers:

- Schrems I: The CJEU annulled the Safe Harbor agreement because it did not ensure sufficient protection for European personal data.
- Schrems II: The CJEU invalidated the Privacy Shield agreement and required all transfers to the US to comply with the GDPR, making Standard Contractual Clauses (SCCs) a necessary mechanism.

Transfer mechanisms:

In the absence of an adequacy decision, companies can use other mechanisms such as:
Standard Contractual Clauses (SCCs): Approved by the European Commission and used to transfer data securely.
Binding Corporate Rules (BCRs): internal data protection policies of companies.

What's new with the updated SCCs?

In 2021, the European Commission updated the SCCs to improve transparency, rights and incident handling. Future changes are expected in 2025.

Transfer Impact Assessment (TIA):

- A TIA should be carried out to assess the risks of transferring data to third countries and to ensure that appropriate safeguards are in place.
- The TIA must include an assessment of the receiving country's laws, legal certainty, and whether there is an independent supervisory authority.

Success and Failure: Case Studies

Success

- A medium-sized technology company correctly implemented SCCs and carried out TIA reports, protecting them from fines and maintaining customer trust.

Failure

- Uber, a global transportation company, was fined €3.3 billion by the Dutch Data Protection Authority for transferring sensitive personal data to the United States without adequate protection. The following personal data was transferred for more than two years:
  - Account details, taxi licenses, location data, photos, payment details, identity documents, criminal records and medical records.

  Uber had initially used SCCs but stopped doing so in 2021 without implementing new transfer mechanisms. Data breaches were detected, which led to hackers gaining access to this data. Uber also failed to inform stakeholders and carry out the necessary Transfer Impact Assessments (TIA).

  This case highlights the importance of:

  1. **Maintain up-to-date transfer mechanisms.**
  2. **Conduct transfer impact assessments (TIAs).**
  3. **Implement technical and organizational safeguards**, such as encryption and pseudonymization.
  4. **Reporting incidents in a timely manner.**

How to Avoid GDPR Fines and Ensure Compliance

- **Clear internal procedures:** Companies should have procedures for handling personal data.
- **Impact assessments (TIA):** Carry out TIAs for each third-country transfer.
- **Documentation:** Document all transfers thoroughly.
- **Monitoring and auditing:** Internal and external audits to detect non-compliance.

Tools and Techniques for GDPR Compliance

- **Data Mapping Tools:** Map data flows and storage locations.
- **Encryption and Pseudonymization:** Use encryption to protect data.
- **Security Certifications:** For example, ISO 27001 and SOC 2 certifications.
- **GDPR Scanners:** Identify risks and ensure compliance.

The future of GDPR and International Data Transfers

Companies should keep themselves updated on new rulings and legislative changes, especially those affecting third-country transfers, such as the role of the U.S. in the current EU-U.S. Data Privacy Framework. Regular changes in legislation, such as updates to the Schrems ruling or changes in transfer mechanisms, can have a major impact on a company's data protection strategy.

Therefore, it is crucial that companies not only adapt their processes but also regularly conduct internal audits and train their employees to ensure they are able to react quickly to new legal requirements and avoid potential GDPR fines.