# CYBERSECURITY AND PRIVACY CROSS-BORDER DATA TRANSFERS



accederes



### WHICH CROSS-BORDER DATA TRANSFER MECHANISM IS BEST FOR MY COMPANY?

The European Union requires that all transfers of personal data to countries outside the EU meet specific "adequate protection" requirements. To meet these requirements, companies outside the EU must adopt a data transfer mechanism deemed adequate by the European Commission.

## COMPARISON OF ADEQUATE DATA TRANSFER MECHANISMS

	EU-U.S. PRIVACY SHIELD*	STANDARD CONTRACT CLAUSES	BINDING CORPORATE RULES
What is the transfer mechanism?	Regulatory framework defining the requirements a company must meet to transfer personal data from the EU to the U.S.	Standard contractual terms stipulating the protections non-EU data controllers or processors must meet to receive EU personal data transfers	Internal corporate rules defining a multinational group of companies' global approach to transferring personal data from an EU entity to non-EU entity
What types of data does the transfer mechanism cover?	Any type of EU personal data the company elects to cover under the framework	Only the EU personal data specifically defined in each contract containing standard clauses	Any type of EU personal data the company elects to manage under the internal rules
Where can the data be transferred (and to whom) under the transfer mechanism?	From anywhere in the EU to only the U.Sbased entity certified under Privacy Shield (unless the appropriate steps have been followed to transfer the data to a third party)	From the EU to the non-EU data controller or processor (any country) party to the contract	From EU-entities of a multinational company group to non-EU entities of the same company group (any country)
How is the transfer mechanism obtained?	Self-certification with the Department of Commerce of compliance with the principles (annual recertification required)	Insertion of the standard clauses in each contract including the transfer of personal data from the EU to non-EU controllers or processors	Authorization from a national Data Protection Authority in an EU country that the company's rules meet the criteria set forth by the European Commission
What documentation is required for approval of the transfer mechanism?	<ul> <li>Company contact information</li> <li>Description of company activities for handling EU personal data</li> <li>Description of company privacy policy for EU personal data</li> </ul>	<ul> <li>Verbatim inclusion of the standard clauses in the contractual terms automatically deemed adequate</li> <li>Amended data transfer contract terms need approval from relevant EU Data Protection Authorities</li> </ul>	<ul> <li>Contact information of the person responsible for rules at the company</li> <li>Description of company structure and EU data processing activities</li> <li>Summary of how the company will satisfy rule requirements</li> <li>Copies of relevant corporate rules (e.g., policies, notices, codes, procedures, contracts)</li> </ul>

## **KEY DEFINITIONS**

#### PERSONAL DATA OR INFORMATION

Data that by itself or in combination with other information can identify an individual.

#### DATA PROCESSING OR PROCESSOR

Any actions or set of actions performed on personal data or the entity carrying out the actions.

#### DATA CONTROLLER

The person or organization that makes decisions about processing personal data.

### BENEFITS AND DRAWBACKS OF DATA TRANSFER MECHANISMS

	EU-U.S. PRIVACY SHIELD	STANDARD CONTRACT CLAUSES	BINDING CORPORATE RULES
BENEFITS	<ul> <li>Allows for continuous data transfers once approved</li> <li>Permits data transfers to the U.S. from any EU-country</li> <li>Waives or automatically accepts EU data transfer "prior approval" requirements</li> <li>Requires companies to formalize or strengthen internal privacy controls</li> <li>Provides cost-effective means to transfer data</li> </ul>	<ul> <li>Provides automatic approval of data transfers with verbatim clause use</li> <li>Enables transfers from any EU- country to any non-EU country</li> <li>Applies to transfers of EU personal data to third parties</li> <li>Imposes fewer internal compliance requirements</li> <li>Provides a cost-effective and expedient means to transfer data</li> </ul>	<ul> <li>Allows for free flow of personal data within a company group</li> <li>Provides automatic approval for data transfers covered by the rules</li> <li>Enables transfers from the EU to any non-EU country</li> <li>Establishes robust internal protocols for managing personal data</li> <li>Builds strong relationships with EU Data Protection Authorities</li> </ul>
DRAWBACKS	<ul> <li>Covers only transfers from the EU to the U.S.</li> <li>Imposes additional contractual requirements to transfer EU personal data to third parties</li> <li>Involves additional requirements for certain types of data</li> <li>Requires annual compliance assessments and recertification</li> <li>Levies an annual certification fee</li> </ul>	<ul> <li>Applies only to data transfers detailed in the contract</li> <li>Requires EU regulatory approval to amend terms</li> <li>Creates obligations for companies to monitor thirdparty compliance</li> <li>Forces companies to assess the privacy practices of third parties</li> <li>Necessitates contracts for new data transfers not covered by existing contracts</li> </ul>	<ul> <li>Limits approval to data transfers within a company group</li> <li>Requires companies to reapply to change the internal rules</li> <li>Invites heightened regulatory scrutiny</li> <li>Imposes significant cost and time burdens to establish the rules and receive approval</li> <li>Necessitates the maintenance of a robust privacy program</li> </ul>

\*As Switzerland is not a member of the EU, the U.S. has agreed to a separate data transfer regulatory framework with Switzerland. The Swiss-U.S. Privacy Shield mirrors the EU-U.S. Privacy Shield framework, with some minor variations. The few exceptions under the Swiss-U.S. Privacy Shield framework are the substitution of the Swiss Federal Data Protection and Information Commissioner's authority for the EU DPAs' authority, a modified definition of sensitive data, and the inclusion of a binding arbitration option. Self-certification under the Swiss-U.S. Privacy Shield is separate from the EU-U.S. Privacy Shield certification and requires a separate annual fee.

#### MICHAEL P. HINDELANG CIPP/US, CIPM 313.465.7412 mhindelang@honigman.com

### CYBERSECURITY AND PRIVACY KARL A. HOCHKAMMER CIPP/US

313.465.7582 khochkammer@honigman.com

