securiti

Post-Schrems-II 5 To-dos for Transatlantic Data Flows

1. Catalog data flows and identify applicable transfer mechanisms other than Privacy Shield.

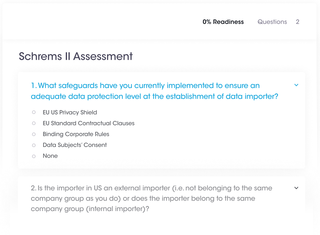
The highest priority should be identifying any transfers subject to Privacy Shield and considering alternative transfer mechanisms like SCCs or BCRs.

It is estimated that up to 5,000 companies relying on Privacy Shield will have to shift to SCCs or BCRs to maintain data transfers to the US. Identify all data transfers from the European Union, generate visual data maps, and Identify cross-border data transfers using our automated data mapping solution.

2. Conduct "transfer impact assessments" to identify exposure to surveillance authorities and the US government's likelihood of access.

Data Mapping is a crucial initial step for many organizations to identify transfer risks.

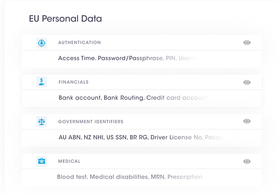
Use a reliable Data Mapping Automation solution to map and identify data transfers to US-based data processors, dynamically assess data risk, and automate RoPA reports.



3. Evaluate the effectiveness of available legal mechanisms for data subjects to obtain redress against unlawful government access to personal data.

The ECJ identified two surveillance authorities – Section 702 of FISA and Executive Order 12333.

Companies need to document and assess the risk that EU personal data will be accessed via these authorities. Considerations for each surveillance authority are distinct, and the relevant risk and supplementary measures will be different.



4. Identify processors/sub-processors to assess onward transfer risks and seek assurances.

Vendors/Third Parties acting as Data Processors or Sub-processors for EU Personal Data can create significant risk under Schrems II.

Initiate Vendor Risk Assessments today to start managing and remediating vendor risks. Get a comprehensive view of risks with trendlines through a consolidated risk score.

5. Consider additional supplementary measures for high-risk data (e.g., personal communications, PII Data). For example:

- Data localization – keep in EU (avoid Schrems-II entirely)
- Encryption of data with keys held in the EU - better data security
- Commitments to challenge orders in FISA court
- Disconnect from high-risk processors/sub-processors under Schrems-II
- Move cloud data, "on-premises."

See Demo Now

WINNER CNBC "Most Innovative Startup" RSAC 2020

Forrester Wave LEADER in Privacy Management

WINNER CNBC "HPE-MPP Innovation Award" 2020

WINNER CB Insights "Most Innovative" Frost & Sullivan

FORBES Top 10 Most Promising Cyber Security Companies