Replenit Transfer Impact Assessment
Last Updated: 28.11.2025

---

1. Executive Summary

This assessment evaluates the risk associated with transferring personal data to the United States in light of the *Schrems II* ruling (CJEU Case C-311/18). The Data Exporter (Replenit) utilizes a hybrid compliance strategy:

1. **DPF Adequacy:** The majority of our sub-processors (Google, Microsoft, Databricks, New Relic) are active participants in the **EU-U.S. Data Privacy Framework (DPF)**.
2. **SCCs + Supplementary Measures:** For any remaining vendors not covered by the DPF, we rely on Standard Contractual Clauses (Module 3) paired with technical safeguards (encryption).

2. Category A: Vendors with Adequacy Decision (DPF)

The following sub-processors are active participants in the **EU-U.S. Data Privacy Framework (DPF)**. On July 10, 2023, the European Commission adopted an adequacy decision concluding that US organizations participating in the DPF provide a level of data protection essentially equivalent to the EU.

Risk Conclusion: Transfer is permitted without further supplementary measures (Art. 45 GDPR).

Sub-processor	Transfer Mechanism	Verification Status (as of Nov 2025)
Databricks Inc.	Adequacy Decision (DPF)	**Active** (Covered by DPF Adequacy)
Google LLC	Adequacy Decision (DPF)	**Active** (Covered by DPF Adequacy)
Microsoft Corp.	Adequacy Decision (DPF)	**Active** (Covered by DPF Adequacy)
New Relic Inc.	Adequacy Decision (DPF)	**Active** (Covered by DPF Adequacy)
Github Inc	Adequacy Decision (DPF)	**Active** (Covered by DPF Adequacy)

(Note: Although these vendors utilize the DPF, our contracts with them also incorporate Standard Contractual Clauses (SCCs) as a redundancy measure.)

3. Category B: Vendors Relying on SCCs or Intra-EEA Transfers

This section covers vendors who may not be DPF certified or are domiciled within the EU.

Sub-processor	Entity Location	Transfer Mechanism

Soda Software	**Belgium (Soda Data NV)**	**Intra-EEA Transfer** (No TIA Required).*
Metabase	**United States**	**SCCs (Module 3)** + Technical Safeguards.

**Note on Soda: If our contract is with Soda Data NV (Belgium), this is an intra-EU transfer and does not require a TIA.*

3.1. Risk Assessment for Non-DPF Transfers (e.g., Metabase Cloud)

For vendors in this category, we assessed the risk of US legislation (FISA 702) impacting the data:

- **Legal Risk:** Medium. The vendor may be subject to US surveillance laws.
- **Technical Safeguards:**
  - **Encryption:** Data is encrypted in transit (TLS 1.2+) and at rest (AES-256).
  - **Data Minimization:** We strictly limit the personal data categories sent to these analytics tools (focusing on metadata rather than raw PII where possible).
- **Contractual Safeguards:**
  - Execution of **Standard Contractual Clauses (Module 3)**.
  - Vendor commitment to challenge overbroad government access requests.

4. Final Conclusion

The Data Exporter (Replenit) concludes that:

1. The bulk of data processing occurs with **DPF-certified vendors** (Databricks, Google, Microsoft), which enjoy a presumption of adequacy under EU law.
2. For remaining transfers, the combination of **SCCs and strong encryption** ensures that the level of protection guaranteed by the GDPR is not undermined.