Data Transfer Impact Assessment

This document assists KLERQ in conducting data transfer impact assessments, particularly following the "**Schrems II**" ruling by the Court of Justice of the European Union and guidelines issued by the European Data Protection Board. The assessment focuses specifically on data transfers to PostMark, U.S.-based service providers.

This Data Transfer Assessment Impact is in Version 1.0, with the latest revision dated
October 11, 2023

Step 1: Describe the Intended Transfer

a) Data exporter:

– KLERQ

b) Country of data exporter:

– Netherlands

c) Data importers:

– Postmark / Wildbit, LLC

d) Country of data importers:

– USA

e) Context and purpose of the transfer:

– Postmark / Wildbit, LLC: Provides email processing services essential for delivering relevant communications as part of KLERQ's services.

f) Categories of data subjects concerned:

– Employees

g) Categories of personal data transferred:

– Contact information, personal information

h) Sensitive personal data:

– Not transferred

i) Technical implementation of the transfer:

– Data is transferred via an encrypted connection and stored on servers in the USA.

j) Technical and organizational measures in place:

– Detailed in KLERQ's Information Security Policy.

k) Relevant onward transfers of personal data:

– None

Step 2: Define the TIA Parameters

a) Starting date of the transfer:

– 1.4.2023

b) Assessment period:

– Three years, ending 1.4.2026, with plans to reassess the situation at the end of this period.

c) Determining the acceptable residual risk of foreign lawful access:

– Given the nature of the data (software usage analytics and customer service communications), the probability of prohibited lawful access is assessed to be below 5%, indicating a low risk.

d) Target jurisdiction for which the TIA is made:

– USA

e) Relevant local laws considered:

– Section 702 of the Foreign Intelligence Surveillance Act (FISA), Executive Order 12333, and Presidential Policy Directive 28 (PPD-28).

Step 3: Define the Safeguards in Place

a) Feasibility of transferring to a whitelisted country instead:

– Postmark: Not feasible due to technical, practical, and economic reasons; services must be based in the US for effective operation.

b) Personal data transferred under one of the exemptions pursuant to applicable data protection law:

– No exemptions apply; transfers are protected under Article 46 GDPR, utilizing EU Standard Contractual Clauses.

c) Is the data transmitted to the target jurisdiction in clear text:

– All transmitted data is encrypted end-to-end.

d) Is the data accessible in clear text by the data importer or a third party in the target jurisdiction:

– Yes, to provide the intended services, access to data in clear text is necessary, making foreign lawful access technically possible.

e) Is the personal data protected by a transfer mechanism approved by the applicable data protection law:

– Yes, through EU Standard Contractual Clauses, ensuring compliance to the extent permitted by US law.

Step 4: Assess the Risk of Prohibited Lawful Access in the Target Jurisdiction

The assessment concludes that the overall risk of prohibited lawful access is acceptably low, at about 5%. This low probability ensures compliance with EU data protection standards, and the data transfer can proceed under these conditions. KLERQ will reassess the risk by 1.3.2027 or earlier if significant legal or circumstantial changes occur. This assessment is based on internal legal analysis, public documentation, and statistics, confirming the security and compliance of the data transfer process.