International Law Office

FDPIC finds that Swiss-US Privacy Shield does not offer adequate level of data protection

11 September 2020 | Contributed by Walder Wyss

AUTHORS

Jürg Schneider

Hugh Reeves

Lena Götzinger

Introduction

On 8 September 2020, the Federal Data Protection and Information Commissioner (FDPIC) removed the United States from its list of countries deemed to provide an "adequate level of data protection". Essentially, the FDPIC is of the opinion that legal remedies for data subjects in Switzerland under the Swiss-US Privacy Shield are insufficient.(1) Until now, the transfer of personal data from Switzerland to US-based companies that self-certified under the Swiss-US Privacy Shield were regarded by the FDPIC as compliant with Swiss data protection laws. Going forward, businesses must reassess their cross-border data transfers in light of the FDPIC's statement.

FDPIC decision and recommendations

The FDPIC's decision is a direct consequence of the European Court of Justice's *Schrems II* decision of 16 July 2020, which invalidated with immediate effect the EU-US Privacy Shield. However, contrary to the situation in the European Union where a court invalidated the EU-US Privacy Shield, the FDPIC's requalification of the United States' adequacy from a data protection standpoint does not formally invalidate the Swiss-US Privacy Shield. It therefore remains legally valid (at least from a formal standpoint) and the situation should remain unchanged until the United States decides to withdraw from the Privacy Shield framework.

Given the above, and because the FDPIC's list of countries is not strictly binding as it is only presumed accurate, companies could theoretically continue to base transfers on the Swiss-US Privacy Shield, although such approaches are not expected to occur frequently in practice. Rather, companies that relied on the Swiss-US Privacy Shield for personal data transfers to the United States are well advised to base such transfers on different safeguards such as binding corporate rules (BCRs) or standard contractual clauses (SCCs). In both cases – whether companies turn to BCRs or SCCs – data exporters should conduct a risk assessment in line with the FDPIC's recommendation. That said, the FDPIC also highlighted the potential risks of relying on SCCs and BCRs because these instruments, like the Swiss-US Privacy Shield framework, do not prevent foreign authorities from accessing personal data based for instance on local national security laws.

In such cases, the FDPIC recommends the three following due diligence assessments:

- In cases where the data exporter intends to rely on SCCs or other such contractual clauses to secure data disclosures to countries not deemed to provide an adequate level of data protection: performing a risk assessment prior to any cross-border disclosure to determine whether these clauses sufficiently mitigate the risks existing in the data-importing country.
- Determining whether the company receiving the personal data (in a country with no adequate level of data protection) is subject to special access by the local authorities. This analysis should also determine whether the receiving company is able to provide cooperation towards the enforcement of Swiss data protection principles. Absent such guarantees, SCC provisions on cooperation obligations become irrelevant.
- In these cases, the data exporter should consider technical measures to prevent authorities in the destination country from accessing the transferred personal data. For example, according to the FDPIC, if data is stored solely in the cloud by service providers based in a country without adequate data protection, encryption (based on a bring-your-own-key (BYOK) and a bring-your-own-encryption (BYOE) approach) so that no individual personal data would be available in the destination country and the service provider

would have no possibility to decrypt the data, would be conceivable. For services that go beyond mere data storage, it may be more demanding to use such technical measures. If such measures are impossible, the FDPIC advises against the cross-border transfer of personal data to recipients in countries without adequate data protection on the basis of contractual guarantees.

The FDPIC intends to provide further guidance for companies as this remains an ongoing topic for data protection authorities and the Swiss courts in particular.

For further information on this topic please contact Jürg Schneider, Hugh Reeves or Lena Götzinger at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, hugh.reeves@walderwyss.com or lena.goetzinger@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) The FDPIC's policy paper can be accessed here.