BIANCHISCHWALD

NEWS

NEW CHALLENGES FOR INTERNATIONAL DATA TRANSFERS

New data protection tasks for companies in Switzerland. The transfer of personal data from Switzerland to other countries should occur only after a review of potential legal and data protection implications. The Swiss Federal Data Protection and Information Commissioner ("FDPIC") published a statement on 8 September 2020, which creates new data protection challenges.

Who is affected?
There is a need for action for companies that transfer personal data from Switzerland to the US. Given the importance of big tech companies (such as Google, Facebook, Amazon, Apple, Microsoft), a considerable proportion of Swiss companies are affected by the FDPIC's statement.

This is true irrespective of the categories of data transferred, the recipients of the data or the purpose for which the transfer is made.

Furthermore, a risk assessment is indicated if personal data is transferred to third countries based on contractual guarantees (such as standard contractual clauses or «SCC»).

Background:
Pursuant to the requirements of Switzerland's and the EU's data protection laws there is no adequate protection for personal data in the US. The main problem lies in the unrestricted power of US intelligence services, which are not subject to any statutory limitations. As a result, the protection of an individual's right to privacy may be infringed, if personal data is transferred to the US. For this reason, the transfer of personal data from Switzerland to the US requires additional (legal) safeguards.

In order to enable a less restricted flow of personal data, Switzerland and the US established the «Swiss-US Privacy Shield Framework» in 2017. This followed a virtually identical (also informal) understanding between the US and the EU («EU-US Privacy Shield Framework») from 2016. In order for the (voluntary) framework to apply, the US company (the intended recipient of the data) needs to submit to its rules. It can do so by ensuring compliance with the data protection rules (set out in the framework) and preparing the necessary documentation. In addition, the company has to self-certify (i.e. notify) with the competent US authority.

Current development:
In July 2020, the European Court of Justice («ECJ») ruled that the «EU-US Privacy Shield Framework» does not ensure adequate protection of personal data[1]. As a result, it is no longer permitted to transfer personal data based on the framework. In case of non-compliance, companies are liable to sanctioning by EU data protection authorities. Formally, this decision has no direct effect on the legal situation in Switzerland.

In light of the decision, the FDPIC re-examined whether the «Swiss-US Privacy Shield Framework» conforms to the requirements of Swiss data protection law. He concluded that it does not offer sufficient protection for individuals (contrary to his former opinion). While this assessment is not legally binding, it is to be expected that Swiss courts will follow the FDPIC's assessment.

[1] Data Protection Commissioner v Facebook Ireland Ltd, Maximilian Schrems and intervening parties, Case C-311/18, 16 July 2020 ("Schrems II")

If personal data is transferred solely based on the «Swiss-US Privacy Shield Framework», additional safeguards have to be implemented. In order to determine which safeguard(s) to opt for, the specific circumstances have to be taken into account.

The FDPIC further states in his opinion that a risk assessment must always be carried out when personal data is transferred to third countries on the basis of contractual guarantees (such as standard contractual clauses). In particular, companies need to determine whether the contractual guarantees address the data protection risks in the target country. In the view of the FDPIC, the use of standard contractual clauses (without prior risk assessment) is not sufficient. The main reason for this statement appears to be the ECJ's decision mentioned above, which (also) addressed the validity of standard contractual clauses. Unfortunately, the legal uncertainty caused by the ECJ's decision will now also challenge companies in Switzerland. The obligation to conduct such risk assessments will apply to future transfer only, according to the FDPIC's statement.

A risk assessment is required if personal data is transferred to third countries based on contractual guarantees (in the future).

It is unclear what requirements are placed on this risk assessment. Both European and Swiss data protection authorities have announced that they will issue additional guidance (e.g. directives, guidelines). In the meantime, we strongly recommend that all decisions made by the company in this regard be adequately documented.

If you have any questions, please feel free to approach your contact person at BianchiSchwald.

CHRISTOPH GASSER
Attorney-at-law, Dr. iur., LL.M. University of Michigan
Part-time judge at the Federal Patent Court
Partner | Zurich

THIERRY BURNENS
Attorney-at-law, M.A. HSG, CIPP/E
Associate | Zurich

BIANCHISCHWALD LLC
mail@bianchischwald.ch
bianchischwald.ch

GENEVA
5, rue Jacques-Balmat
P.O. Box 5839
CH-1211 Geneva 11
P +41 58 220 36 00
F +41 58 220 36 01

ZURICH
St. Annagasse 9
P.O. Box 1162
CH-8021 Zurich
P +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
P.O. Box 5410
CH-1002 Lausanne
P +41 58 220 36 70
F +41 58 220 36 71

BERN
Elfenstrasse 19
P.O. Box 133
CH-3000 Bern 15
P +41 58 220 37 70
F +41 58 220 37 71