REPRINT FINANCIER WORLDWIDE

JANUARY 2016

FINANCIER WORLDWIDE corporatefinanceintelligence

RISK MANAGEMENT

The effect of the safe harbour ruling in Switzerland

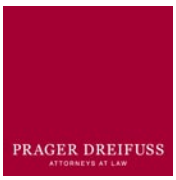
DANIEL HAYEK, DOMINIK SKROBALA AND CHANTAL JORIS

PRAGER DREIFUSS LTD

On 6 October 2015, the European Court of Justice (ECJ) issued its much-anticipated judgment in *Schrems v Data Protection Commissioner*, Case C-362/14 (Safe Harbour Ruling). The case was brought after it had been revealed by Edward Snowden that personal data, which was transferred by companies like Facebook from the EU to the US under the so-called Safe Harbour Framework, had been accessed by the US National Security Agency under the PRISM program. In light of these revelations, the ECJ ruled that the Safe Harbour Framework, which has served trade between the EU and the US for over 15 years, was no longer valid. In 2008, Switzerland and the US concluded a separate Safe Harbour Framework (Swiss Safe Harbour Framework), which contains very similar provisions, but has a wider scope of application encompassing not only data relating to natural persons but also to legal entities. The Safe Harbour Ruling has an impact on Swiss companies that make use of the framework in order to transfer personal data to the US for any number of reasons, be it in the context of M&A transactions, in particular in the course of due diligence processes regarding employee data, the general outsourcing of data processing, or the widespread

PRAGER DREIFUSS
ATTORNEYS AT LAW

Daniel Hayek is a partner, Dominik Skrobala is an associate and Chantal Joris is a trainee at Prager Dreifuss Ltd. Mr Hayek can be contacted on +41 44 254 5555 or by email: daniel.hayek@prager-dreifuss.com. Mr Skrobala can be contacted on +41 44 254 5555 or by email: dominik.skrobala@prager-dreifuss.com. Ms Joris can be contacted on +41 44 254 5555 or by email: chantal.joris@prager-dreifuss.com.



reliance on cloud computing services based in the US.

The Swiss Safe Harbour Framework

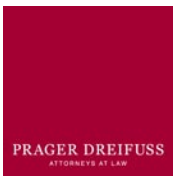
If personal data is transferred from a Swiss company to a US company, such transfer needs to comply with the Swiss Federal Data Protection Act (DPA). The DPA only allows transfers to countries offering an adequate level of protection for personal data (article 6(1) DPA). This also applies if data is disclosed within a multinational corporate group. If no adequate protection is in place in the country of destination, personal data may only be transferred under certain conditions, e.g., if contractual clauses guarantee adequate protection or the individual to whom personal data relates (data subject) has consented to the transfer. Unlike Switzerland and the EU, the US has no data protection law, but regulates information privacy on a sector by sector basis, which is why the consensus has been that the US does not meet the requirement of adequacy. The respective Safe Harbour Frameworks were negotiated to bridge the different privacy approaches between the US and Europe. Until the Safe Harbour Ruling, the Swiss Federal Data Protection and Information Commissioner (FDPIC) had considered that those US companies, which had self-certified under the Safe Harbour programme administered by the US Department of Commerce, guaranteed an adequate protection level and that transfers to such companies were allowed under the DPA.

Why are Swiss companies affected by the ECJ Ruling?

Switzerland is not a member of the EU and the Swiss authorities are not legally bound by the Safe Harbour Ruling. In practical terms it would, however, be difficult for Switzerland to take a different stance *vis-à-vis* its Safe Harbour Agreement with the US. Not declaring Safe Harbour invalid would risk that the EU, Switzerland's most important trading partner, considered Switzerland to be a country with no adequate protection and disallowed data exports to Switzerland. In view of this, the FDPIC issued a communication on 22 October 2015 declaring that the Swiss Safe Harbour Framework did no longer provide for a sufficient legal basis for exporting data. Consequently, the FDPIC removed the US from his list of countries with an adequate level of protection. The FDPIC has no authority to invalidate the Swiss Safe Harbour Framework, so technically it is not illegal for a Swiss company to export data to certified US recipients, until a Swiss court rules otherwise. On 18 November 2015, the Swiss Federal Council stated that for the time being it has no intentions of cancelling the Swiss Safe Harbour Framework but will closely follow the negotiations between the EU and the US. However, in light of the FDPIC recommendation and the uncertain future of the Safe Harbour Framework, Swiss companies should consider alternative safeguards for upcoming data transfers to the US.

Alternative safeguards

Contractual agreements and BCRs. Until a new Swiss Safe Harbour Framework has been negotiated, the easiest way to still abide by the DPA is the conclusion of contractual agreements with the US recipient. The European Commission has published model contractual clauses (EU Model Clauses) which also work under Swiss law and are recognised by the FDIPC. It is further possible to rely on Binding Corporate Rules (BCRs) for data transfers within a corporate group, including to the US. BCRs have to be approved by the data protection authorities of the relevant countries, which is often a complex and lengthy undertaking. Other legal grounds under the DPA, such as consent or performance of a contract, are normally useful for individual transactions rather



than providing for a general legal basis for all data transfers.

In light of the Safe Harbour Ruling, the FDPIC recommends companies to amend contractual agreements under Article 6(2) lit. a DPA as follows by January 2016: (i) the parties have to inform data subjects of the possible access to their data by US authorities; and (ii) the parties undertake to support data subjects with the necessary means to ensure effective legal protection, to conduct proceedings and to accept the judgements rendered in this respect.

Just like the Safe Harbour Framework, contractual agreements bind companies and not state authorities. If personal data continues to flow to US companies under contractual agreements, the data will still remain at risk of disproportionate access by US authorities. This is why the FDPIC considers it necessary to inform the data subject about the risks involved. Given the complexity of data processing, cross-border transfer practices and the difficulty of understanding the bulk collection of data by US authorities, it is questionable if informing the data subject will enhance the protection of their data in the way intended by the DPA. What exactly the two additional requirements mean is not clear. Further guidance would be needed for companies to know how to implement them. It is important to note that there is no legal obligation to amend the contractual agreements as suggested by January 2016. The EU Model Clauses remain legally valid and can still be used by companies to export data to the US in accordance with the DPA.

The FDIPC's statement is somewhat surprising, given that the Article 29 Working Party, the EU advisory body on data protection and privacy, has not established any additional requirements for contractual agreements. What the Article 29 Working Party did state is that while EU model clauses and BCRs can still be used, it "will continue its analysis of the CJEU [European Court of Justice] judgment on other transfer tools". It remains to be seen whether the validity of data transfers based on contractual agreements will be challenged. The German data protection authorities have already declared that for now they will not approve any data export agreements or BCRs.

Technical and organisational measures. Given that as a result of the Safe Harbour Ruling alternative data transfers have also come under scrutiny, we recommend companies review their data flows and consider whether exports of personal data to the US could be minimised. It may further make sense to investigate technical measures and assess whether personal data can be tokenised, encrypted or anonymised before being transferred to the US in order to mitigate the risks. If companies can rely on fully anonymous data, the data would not constitute personal data and fall outside the scope of the DPA.

Future of the Swiss Safe Harbour Framework

The future of the Swiss Safe Harbour Framework and the validity of contractual agreements or BCRs largely depends on the ongoing negotiations between the EU and the US on a revised Safe Harbour Framework. The Article 29 Working Party has warned that if no appropriate solution is found with US authorities by the end of January 2016, the EU data protection authorities will take necessary action, including enforcement actions. Given the importance of personal information transfers for transatlantic trade and the amount of data transferred from Europe to the US, it is to be hoped that negotiations will speed up. In any case, a new Safe Harbour Framework will have to take into account the criticism of the Safe Harbour Ruling, otherwise the risk remains that the ECJ will also overturn the new Safe Harbour Framework. ■