



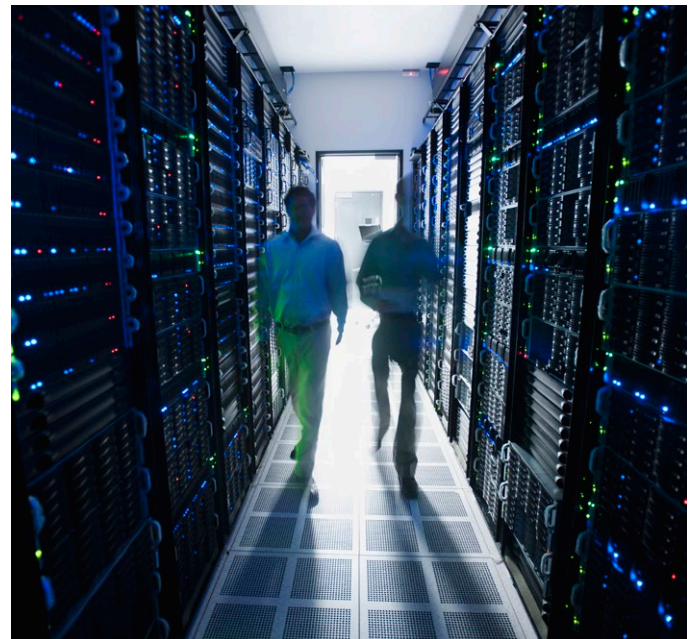
A&M INSIGHTS

Schrems II and Switzerland: a new context for data and privacy

The EU has coughed, and Switzerland has caught a cold. In July, the European Court of Justice (ECJ) ruled in 'Data Protection Commissioner v Facebook Ireland and Max Schrems' – or 'Schrems II' – that US data collection policies are not compatible with EU citizens' rights under the General Data Protection Regulation (GDPR). This invalidated the EU-US Privacy Shield that had governed data transfers between the EU and US.

Now, the Swiss Federal Data Protection and Information Commissioner (FDPIC) has followed in the ECJ's footsteps, ruling that the US should not feature on the list of third countries with 'adequate' protections in place for Swiss citizens' data. The FDPIC now regards US protections as 'insufficient'. Accordingly, the Swiss-US Privacy Shield (designed to mirror the EU-US agreement) has effectively been invalidated in all but name.

This development poses inevitable questions for organisations in Switzerland regarding privacy and its status as a core operational capability. Companies should now look to, at the least, carry out an audit of their data transfer protocols. In worst-case scenarios, organisations may have to drastically change the way they handle data, potentially even pausing certain high risk data transfers while assessing the best route forward. There is a lot at stake if this process is not handled properly.



The context

The Swiss-US Privacy Shield has been in place since 2017, replacing the Safe Harbour agreements that had previously governed data transfers between Switzerland and the US. Safe Harbour was [invalidated](#) in 'Schrems I', Max Schrems' 2015 challenge to transatlantic data transfers.

The Privacy Shield sat alongside other approved mechanisms or derogations such as special legal agreements known as Standard Contractual Clauses (SCCs) to facilitate data transfers between Switzerland and the US. Now, Schrems II has not only compromised

the legal authority of the Privacy Shield but the FDPIC has indicated that it will issue guidance at a later date on additional safeguards to be applied alongside the use of [SCCs](#).

It is important to remember that the Privacy Shield is still valid from a US perspective. Businesses that have been certified under the scheme are still required to comply with the framework until their certifications expire. Nevertheless, it is clear that organisations face new challenges to existing data transfer protocols.



Data and privacy after Schrems II: key priorities

The invalidation of the Swiss-US Privacy Shield could be a valuable opportunity for organisations to reassess and modify their data privacy policies.

The FDPIC has already issued [recommendations](#) aimed at helping Swiss companies properly export data to the US in a new operating environment. Organisations are being encouraged to consider whether the foreign company receiving data is an appropriate steward of Swiss citizens' information. It is also recommended that data exporters encrypt data where possible to ensure a more robust standard of data security.

We recommend following a few crucial steps which should underpin organisations' data protection plans going forward:

- **Continue to monitor guidance from Swiss and US authorities.** This process is not yet fully complete: there may well be further guidance issued as the debate continues as to what defines 'appropriate' additional safeguards.
- **Understand direct and indirect cross-border data flows.** Data transfers do not only apply to your own operations: it is essential to assess the readiness of vendors, service providers and other third parties to adhere to the required standard
- **Make a judgment as to which transfer mechanism or derogation can provide adequate protection.** Whether it be SCCs or specific derogations like consent, organisations need to understand how they can engineer an adequate degree of protection of Swiss user data.
- **Gauge the degree of risk that is comfortable for your organisation.** Different organisations will have different risk appetites, of course. Risk appetites will be contingent on the kinds of data that are being transferred and the sectors in which organisations operate. Conducting a new risk assessment can also help establish a framework that can support ongoing tweaks and changes as guidance evolves.

It is vital for organisations to consider whether SCCs remain a fit with existing data policies and general business priorities. If substantive changes are required, creating an inventory of data could make the difference between effective oversight and a poorly-executed audit.

Many businesses may require a localised solution that eliminates the risk of certain direct and indirect data transfers. To respond to these requirements, A&M offers clients a secure datacentre in Zurich. Switzerland's independent regulatory infrastructure removes any threat of compulsory extraction of data short of a court judgment proving an organisation's guilt or liability.

Taking steps to secure critical data now could add value to the wider business down the line. For example, having a clear and pragmatic data policy in place could make corporate transactions, such as mergers & acquisitions more efficient or ease the delivery of transformation initiatives. Those organisations who can decisively respond to a new operating environment will be in a strong position to deal with the many other challenges 2020 holds and beyond.



A&M: Leadership. Action. Results.SM

Our professionals have both operations and advisory experience together with a proven track record in leading businesses through tough, complex situations. A&M's Disputes and Investigations practice combines deep experience in privacy and risk with specialist litigation and disputes support. Get in touch with our key contacts to learn more about our work.

KEY CONTACTS



Jerry Lay

Managing Director
Zurich

+41 78 668 68 68
jlay@alvarezandmarsal.com



Robert Grosvenor

Managing Director
London

+44 796 161 1505
rgrosvenor@alvarezandmarsal.com



Matthew Negus

Senior Director
London

+44 776 710 2676
mnegus@alvarezandmarsal.com

ABOUT ALVAREZ & MARSAL

Companies, investors and government entities around the world turn to Alvarez & Marsal (A&M) for leadership, action and results. Privately held since its founding in 1983, A&M is a leading global professional services firm that provides advisory, business performance improvement and turnaround management services. When conventional approaches are not enough to create transformation and drive change, clients seek our deep expertise and ability to deliver practical solutions to their unique problems.

With over 5,000 people across four continents, we deliver tangible results for corporates, boards, private equity firms, law firms and government agencies facing complex challenges. Our senior leaders, and their teams, leverage A&M's restructuring heritage to help companies act decisively, catapult growth and accelerate results. We are experienced operators, world-class consultants, former regulators and industry authorities with a shared commitment to telling clients what's really needed for turning change into a strategic business asset, managing risk and unlocking value at every stage of growth.

Follow A&M on:



© Copyright 2020 Alvarez & Marsal Holdings, LLC.
All Rights Reserved.
119972 / October 20

To learn more, visit: [AlvarezandMarsal.com](https://www.alvarezandmarsal.com)