Quick Guide to Understanding the Impending Changes to Safe Harbor

With data privacy laws and regulations shifting, it can be hard for companies that work internationally to keep track of them all. It can be even harder to locate MSPs and data center providers that have a proven track record of navigating laws like Safe Harbor. It’s important to understand how these laws are evolving and what companies must do to remain compliant while managing data and servicing customers. This guide breaks down how companies can do just that while also presenting a rundown of both the data security landscape and the death of Safe Harbor.

The Issue At-a-Glance

With network connectivity from country to country increasing, it’s becoming more critical than ever for multi-national companies to safely and successfully transport data from one country to the next. The key drivers for this expansion include addressing demand for new markets, enhancing customer services and uncovering new revenue opportunities.

Globalization is a reality, and telecom companies are expanding their influence and products into new regions outside the US. More foreign carriers and enterprises are looking to enter the US from other countries as well. As a result of this mixing of networks, data sovereignty will be an issue.

There are many laws and regulations – including the invalidated US-EU Safe Harbor Privacy Principles. It can be difficult for companies that are unfamiliar with them to navigate legal landscapes in new markets. In Europe, those laws have begun to change, and it’s going to affect how MSPs and data center operators – and their clients – transfer data from one country to the next.
What is Safe Harbor?

One of the prominent factors in trans-Atlantic data transport is the stark contrast between how the United States and the European Union approach information privacy. The United States is a bit more open with its legislation, relying on additional self-regulation to protect data, while the European Union looks for more specific legislation that ensures the protection of its members. The US-EU Safe Harbor framework was put into place to provide sufficient data security for EU members while maintaining open channels for both commerce and data transport for US companies.

The Safe Harbor Privacy Principles were designed to find a middle ground between the US and EU’s standards for governing and protecting digital information. To transport data across the Atlantic from the EU, US companies were asked to attest to their adherence to the seven principles outlined in Safe Harbor, which were designed to comply with European privacy laws:

- **Notice:** The purpose behind data collection and usage must be fully disclosed.
- **Choice:** Opt-out opportunities must be provided to all individuals, and sensitive information must require an opt-in.
- **Onward Transfer:** All future data transfers must follow Safe Harbor Privacy Principles or another comparable directive.
- **Security:** Information must be adequately protected.
- **Data Integrity:** All personal data gathered must be relevant, and the data’s reliability should be verified.
- **Access:** If an individual’s personal information has been gathered, they must have the right to access and modify or remove inaccurate information.
- **Enforcement:** The compliance of these rules by each organization must be feasible - with sanctions readily available to be handed out to those who do not follow through on their data privacy commitments.

What Enterprises Need to Know

For 15 years, the Safe Harbor Privacy Principles provided a way for US and EU companies to protect and transport data overseas. While the flow of information across the Atlantic Ocean was not completely open and free, it did provide US companies with access to this information.

That came to a close in early October when Austrian privacy activist Max Schrems filed a complaint against Facebook’s data transfers from Europe to the United States. Citing the company’s cooperation with the NSA’s Prism program, as disclosed by Edward Snowden, Schrems stated the social network was not providing the level of information safeguards required in the European Union.

The European Court of Justice approved Schrems’ argument, finding the data sovereignty of its constituents could not be guaranteed to be safeguarded from United States national intelligence services. As a result, Safe Harbor is no longer in effect, and the push for new legislation is already underway.

When the grace period for Safe Harbor ends in January, the European Union will begin enforcing data transfers. Companies that previously relied on Safe Harbor to bring information to the United States from Europe will have to deal with a more strictly-regulated data environment. There’s a race to put together new legislation before the deadline, but such processes can be very time-consuming. It’s unlikely that new regulatory guidelines will be put into place in time.

Several major players in the cloud service provider world are already prepared for the worst-case scenarios. Just a few weeks after the European Court of Justice’s decision, Amazon Web Services revealed plans to launch cloud services in the UK in 2016.
Microsoft Azure will also be launching facilities in Germany and the UK. While the planning of these projects was certainly under development well before the European Court of Justice’s ruling, it’s easy to look at them in a different light after Safe Harbor.

The major cloud providers may be getting ready for life after Safe Harbor, but where does that leave enterprises that have relied on managed service providers to acquire and manage colocation space in foreign countries? The truth is, some MSPs know the ins and outs of trans-Atlantic data transports, and some do not keep up to speed with both policy changes and the evolving business of transporting data on a global scale. With all these factors in play, it can be a challenge for companies to navigate hosting and transporting data in European countries.

**Preparing for Trans-Atlantic Data Management Success**

Enterprises that need to successfully host and transport data between multiple continents with different regulatory guidelines have three options for managing the process – and they’re most effective when combined together.

**Learn About the Regulatory Guidelines Themselves**

The most straight-forward – yet arduous – method of managing data regulations across multiple continents is to study up on policy evolutions and make well-informed decisions. While there’s a clear benefit to becoming more aware of the intricacies of transporting data between continents, it’s best to couple this strategy with another approach.

**Work with a Knowledgeable MSP**

Clients who work with an MSP that does a great job of navigating the data security space will not have to spend as much time and energy worrying about the regulations themselves. The MSP will be capable of answering questions – and addressing concerns – on international data and privacy laws. It will also be their responsibility to ensure the company is fully compliant.

This is clearly a beneficial option, but it also presents a conundrum of sorts: How can companies identify MSPs that are informed on the ins and outs of data privacy laws when they themselves may not have the regulatory know-how to vet them?

**Partner with a Telecom Consulting Agency**

By working with a trusted telecom consulting agency, companies will have a helping hand with,

- *Learning about data security laws, like the successor to Safe Harbor*
- *Identifying MSPs and data centers that do a good job of navigating the data security space – and partnering with them*
- *Benefit from the experience of having helped other clients with establishing multinational presences, ensuring any trans-Atlantic data transport process is as hiccup-free as possible*

Telecom consulting agencies are able to leverage their tribal knowledge, strategic partnerships and relationships with carriers and service providers across the industry to help companies understand – and overcome the challenges presented by – changing trans-Atlantic data laws.

Want to learn more about data privacy laws, the future of trans-Atlantic data transport, and the intricacies of establishing and maintaining multinational presences? NEF has the experience and expertise to help you understand US-EU data privacy laws and identify MSPs that follow best practices. Call us today at 877.DK.FIBER or visit NEFiber.com.