// (US) Service Provider Management

Reading time: 3 minutes

European data protection law classifies countries outside the EEA as insecure. Personal data may only be processed in these countries where appropriate safeguards are in place to ensure that the personal data is adequately protected there. This is relevant for many US service providers whose services are a natural part of the IT infrastructure of many companies, including AWS, Microsoft, Mailchimp, Cisco and many more. It is difficult to set up the deployment of these services in a data protection-compliant manner. Violations are now to be increasingly investigated and possibly sanctioned. Find out how to best prepare your business.

Background

With the so-called Schrems II decision (C-311/18), the ECJ overturned the Privacy Shield and thus an important legal option for integrating US service providers in a privacy-compliant manner. In addition, the ECJ questions whether personal data may at all be transferred to the US and processed by US service providers in a privacy law compliant manner. Background are potentially far-reaching possibilities of US authorities to access personal data. As a result, controllers in Europe only have the option to

- implement so-called EU Standard Contractual Clauses and
- additional technical and organizational safeguards preventing US authorities to access personal data.

German regulators are now planning coordinated actions to audit and enforce related legal obligations. According to the Hamburg Commissioner for Data Protection and Freedom of Information (Professor Caspar), German regulators have developed 5 questionnaires for this purpose. These questionnaires are to be systematically sent to companies which then must provide extensive information on deployment of US service providers. The questionnaires cover

- Tracking-Tools
- Mailhosters
- Intragroup Data Transfer
- and two further questionnaires.

The regulators assume that it is possible to operate in these fields without US service providers and plan to enforce this assumption. Fines are apparently not yet in their focus.

How can I reduce the risk to my company?

Companies are well advised to check whether they use US service providers and whether or not they have adequate measures in place. The following checklist may help to identify and mitigate related risks.

/ **Are US service providers used?**

Make a risk inventory and check for US service providers used. Even if processing by the US service provider takes place in the EEA, for example hosting in a European data centre, there may still be relevant data transfers to the US.

/ **Are there alternative service providers within the EEA?**

The most efficient measure to reduce risk is to refrain from using US and other third-country based service providers. Therefore, carefully check whether there are equivalent alternative offers from service providers in the EEA. You should deploy them with priority.

/ **Is there a contractual basis for the involvement of US service providers?**

Deployment of US service providers should only take place on the basis of appropriate (contractual) foundations. These are in particular the so-called EU Standard Contractual Clauses. Binding Corporate Rules can also take over this function for deployment of intra-group service providers. Make sure to check whether corresponding agreements are in place.

/ **Are there additional technical and organizational guarantees (so-called supplementary measures)?**

In addition to implementing adequate contractual safeguards for the assignment of US service providers, there must be additional technical safeguards to effectively prevent US authorities from accessing personal data. This also applies to so-called "warrant canaries" deployed in order to oblige US service providers to disclose any US authorities' attempts to access personal data. Ultimately, anonymization, pseudonymization and encryption, appear to be adequate technical safeguards. Whether the specific service in question may be used with such technical means in place needs to be assessed on a case to case basis.

// Firm

Digitalization is a challenge for small and large companies alike. We are convinced that a flexible and specialized unit like **PLANIT** // LEGAL is most capable of meeting the needs of national and international clients.

PLANIT // LEGAL offers comprehensive advisory services in the field of German and European **IT and Data Protection Law**. The scope of services covers assignments as external **Data Protection Officer, EU Representative**, classical **legal advice** and support for legal, data protection and compliance departments.

We advise on software licensing, IT procurement, e-commerce law, IT and data protection compliance, data protection and IT due diligence. In a close cooperation with you, we develop solutions that best suit your company. In this context, we draft IT and data protection contracts, provide support for IT projects and represent your interests and rights in legal or regulatory disputes.

PLANIT // LEGAL Lawyers have **long lasting experience** in advising IT- and Data Protection matters from their experience in IT- and Data Protection Groups of international law firms, smaller and highly specialized units, their service for Data Protection Authorities and as Data Protection Officers.

PLANIT // LEGAL has a **strong network** of experts covering also other fields of law and technical expertise to always offer the full range of advice.

Kontakt
PLANIT // LEGAL
Jungfernstieg 1
20095 Hamburg
mail@planit.legal
+49 (0)40 609 44 190