GLOBAL ACCESS

global.de

SAFE HARBOR

THE END OF SAFE HARBOR: WHAT COMPANIES NEED TO KNOW

In a spectacular decision, the European Court of Justice (ECJ) [Europäische Gerichtshof (EuGH)] has declared the Safe Harbor Agreement with the U.S. as invalid. During data exchanges between companies in the EU and the U.SA, sufficient protection of personal data is not provided by this agreement. Companies must act fast.

U.S. • EU
SAFEHARBOR
U.S. DEPARTMENT OF COMMERCE

Reminder: Safe Harbor attested that certified companies in the U.S. had a data protection standard equivalent to that of the EU. This and a correspondinglegal foundation provided for unrestricted data transfer between companies in the U.S. and the EU.

According to the the ECJ decision, adequate data protection is not provided. Personal data in the U.S. are not protected, or at least not sufficiently protected, from arbitrary access by the American authorities.**Legal action against unlawful data processing is also not possible. The ruling explicitly referred to the NSA scandal disclosed by Edward Snowden.**

But what does the end of Safe Harbor mean exactly? The main problem, and this does not only apply to the U.S., is the issue of jurisdictions and powers of national authorities in third countries, which allow access to data as soon as they deem that their national interests are affected. Unlike Germany, jurisdiction is not restricted to the country's own borders – it applies to everything, everywhere. As such powers cannot be regulated by EU law, how can data protection be guaranteed when it is easily undermined by national legislation? The answer is as simple as it is alarming: it can't. This means that if these authorities manage to get the data, they will almost certainly analyse the data. This situation is not expected to change in any time soon.

SO, WHAT SHOULD A COMPANY DO? There is no reason to assume that third countries – which grant their authorities broad accessibility to data – will change their laws due to the Safe Harbor decision. Therefore, companies today have to find other ways to provide proper data protection. Ideally, given the current situation, data should remain in Europe and be protected on-site.

It is wise to incorporate and adhere to the European and German standards as much as possible. All data security certifications and pertinent contractual obligations of providers should be in compliance with EU data protection law, and their servers should be located within the EU.

COMPANIES SHOULD PAY PARTICULAR ATTENTION TO THE FOLLOWING STEPS:

- **Data encryption, including the data infrastructure, in order to prevent unauthorized access;**
- **As much data as possible, at least all sensitive data, should be removed from American providers and relocated to European or German providers with inland servers;**
- **Providers' data security standards and certifications must be verified, e.g. native ISO 27001 based on IT baseline protection [IT-Grundschutz], ISO 9001;**
- **All data-processingcontracts should be thoroughly inspected.**

It is also imperative that further Safe Harbor developments be closely monitored, either by the internal data protection officer or by the appointment of an external DPO. This topic must not be neglected under any circumstances.

General Manager: Manfred Keßler - Amtsgericht München - HRB 113215

Global Access Internet Services GmbH
Management & Administration – Potsdamer Straße 3 – D-80802 München
Sales & Technical Support - Wamslerstraße 8 – D-81829 München
Tel: +49 (0) 89-92 402 0 - **Fax:** +49 (0) 89-92 40 2 150 – sales@global.de - **www.global.de**