Update

October 2015

E-Commerce – Data Protection

VON BOETTICHER
RECHTSANWÄLTE

SPEED READ

1. **ECJ Prohibits "Safe Harbor" Transfer of Personal Data to the US**
   - European companies must check their data transfers and outsourcing projects and take appropriate action. US companies should consider offering EU standard contractual clauses.
2. **High Penalty for Unspecified Contract on Commissioned Data Processing**
   - Supervisory authority fines a five-digit amount because of inexact description of data security measures.

1. ECJ Prohibits "Safe Harbor" Transfer of Personal Data to the US

On October 6, 2015, the European Court of Justice invalidated the "Safe Harbor" Principles of data transfer to US territory. European companies that have relied on "Safe Harbor" in the past now have to react. US companies should consider offering their European customers to use EU standard contractual clauses or set up new services within European borders, in order not to forego business with customers, which strive to comply with applicable data protection laws.

Until now, transfers of personal data from within the European Union to the US were allowed if the US company complied with the "Safe Harbor" rules. Thus, businesses quite simply could, for example, use US cloud services, process data of their employees or third parties in the databases of their US mother company, or outsource complex IT projects to the US.

The ECJ, however, now has invalidated the "Safe Harbor" principles with immediate effect and without any grace period. German data protection authorities already had stated during litigation that they are scrutinizing several companies with respect to "Safe Harbor" and that they would defer further action only until the ECJ decision.

Besides the "Safe Harbor" principles, an alternative compliance standard for data transfers to "third countries" like the US might be use of the so-called standard contractual clauses approved by the European Commission. These clauses may be negotiated between the European customer and the service provider in a third country. But in its decision on "Safe Harbor", the ECJ stated that any statutory provision, which in fact allows an unlimited access to electronic communication by secret services is not compatible with European fundamental rights. Thus, the risk remains that even the existing EU standard contractual clauses cannot avoid a violation of European data protection rules, as contracts between companies can of course not restrict the powers of US authorities.

However, the standard contractual clauses at least provide a factual interim solution: The ECJ further states that only the Court itself may invalidate a decision of the European Commission. Until such invalidation decision by the ECJ, it should therefore be admissible to rely on the continuing validity of the decision of the Commission regarding the standard contractual clauses.

There are other alternatives of a legal data transfer to the US, e.g. Binding Corporate Rules (BCR) implemented by some groups of companies. At this point in time, existing BCRs are not affected by the ECJ decision. A further possibility is obtaining an individual consent by the competent data protection authorities. After the ruling it is, however, in doubt to what extent such consents will be granted in the future.

Not affected by the current decision are data processings within the EU or the European Economic Area (EEA), even if the servers are operated by US companies or their affiliates. A European company may, even after the ECJ judgment, still agree to a so-called contract on commissioned data processing if the data are processed in, e.g., Ireland. Although German data protection authorities raised concerns in this regard as well, we do not know of any case of an authority having actually taken action against such a contract. But it remains most important that such contracts comply with all legal requirements – failure to comply is subject to a fine of up to 50.000 Euros.

Supervisory authorities are expected to examine more closely data transfers to the US in the near future. Because German companies are threatened with fines in the six-digit-range, they should evaluate as soon as possible whether they transfer personal data to third parties (including affiliated companies), and if so, on what legal basis such transfer takes place. This includes commissioned data processings outside the EC/EEA – e.g. the use of cloud services in the US or use of e-mail accounts hosted by a US provider. If the legal basis was "Safe Harbor" (or worse: there was no legal basis at all), immediate action is required.

Providers in the US should consider proactively suggesting their European customers implementing the EU standard contractual clauses: These presently are the sole option for most companies to legalize data transfers to the US. US companies not offering such a contractual solution will face customer complaints when the data protection authorities start enforcing the ECJ "Safe Harbor" decision.

European Commission and US government have been negotiating a revised "Safe Harbor II" for some time. But due to the high hurdles set up by the ECJ, successful completion of these negotiations now seems unlikely: As long as US legislation allows "authorities to generally access the content of electronic communication", such legislation would contradict the EU fundamental rights and as a result any data transfer into such country would be unlawful on the basis of even a revised "Safe Harbor" clause. However, exactly these extensive access rights granted to the US secret services have been reported to be not negotiable for the US.

Further Information:

EuGH, judgment of 2015-1-06, Case C-362/14

https://www.boetticher.com/15101a

2. High Penalty for Unspecified Contract on Commissioned Data Processing

The Bavarian Office for Data Protection Supervision (BayLDA) recently set a fine in the five-digit-range be-

cause the affected company, in a contract on commissioned data processing, did not specify the technical-organizational measures to protect data, but only made general statements and repeated the wording of the law.

If companies engage external service providers for the processing of personal data – even if they only operate e-mail accounts through external servers or outsource their IT maintenance –, they must have written contracts in place. In addition to such written form – a contract document bearing the signatures of both parties – the law requires certain minimum content.

Of special importance are the so-called technical-organizational measures, i.e. data protection measures. Many contracts on commissioned data processing only repeat the purposes of data security provided by law or are limited to a few general remarks. Now the Bavarian authority punished exactly such a contract with a five-digit fine. Law stipulates that every single security measure has to be identified in the contract, because only then a meaningful evaluation of the level of data security at the provider's site is possible.

Companies should not take lightly the obligation to conclude contracts on commissioned data processing complying with the legal requirements. Even though inspections by data protection authorities have until recently been exceptional – these contracts are virtually always reviewed because such inspection is only a minor effort. In case such contract is missing or insufficient, penalties of up to 50.000,- Euros are the consequence. Moreover, secure data processing on a clear and unambiguous contractual basis is in the company's own best interest: The customer remains fully legally responsible for the data processing – and has to bear the economic consequences of any data mishap.

Key Contact:

If you would like to know more about any of the subjects covered in this publication or our services, please contact:

Matthias Bergt
E-Mail: mbergt@boetticher.com
Tel. +49 / 30 / 61 68 94 03

Dr. Anselm Brandi-Dohrn, maître en droit
E-Mail: abrandi-dohrn@boetticher.com
Tel. +49 / 30 / 61 68 94 03

or your usual contact at VON BOETTICHER.

VON BOETTICHER Rechtsanwälte
Oranienstraße 164
D-10969 Berlin

VON BOETTICHER Rechtsanwälte
Widenmayerstraße 6
D-80538 München