

## POSITION STATEMENT

---

# Current Developments in Public Procurement Law

**Position Statement of the Telecommunications, Internet and Media (TIM) Committee of the American Chamber of Commerce in Germany e.V.**

**November 2014**

---

### **1 Background**

The Federal Ministry of the Interior (BMI) published a Decree on April 30, 2014, which introduced two clauses for public invitations to tender with a possible security relevance within the portfolio of BMI:

- A declaration of eligibility, which needs to be signed upon the submission of the tenderer's documents. Beyond the usual confidentiality clauses, the tenderer is to declare that he is legally and factually able to treat confidential information confidentially.
- A contractual clause, which needs to be signed upon the conclusion of the contract. The contractual clause stipulates that in the event of non-compliance with the terms and conditions specified in the declaration of eligibility, a special termination right applies. Moreover, the contractor is obliged to inform the principal of any duties of disclosure applying after the conclusion of the contract.

The objective of the two clauses is to ensure a facilitation of the burden of proof for the benefit of the public authorities. For the rejection of a tenderer in the wake of the reliability check and/or for a contract termination it is to be sufficient in future to prove that the tenderer is subject to a legal obligation of data dissemination.

### **2 Assessment**

The American Chamber of Commerce in Germany e.V. (AmCham) supports a high security level in the public administration. At the same time, we are of the opinion that it is necessary to engage into a fundamental debate about important topics such as national security and data privacy. They constitute an essential basis for the trust of users in the IT systems used by them. The AmCham is, however, aware that there is currently a lack of confidence concerning the integrity of information technology. Nonetheless the necessary discussions should take place between the competent government bodies and should not have an adverse effect on the business activities of private companies. We believe that the submitted

Decree is in its present form not qualified to increase the trust in the integrity of IT:

Firstly: The Decree uses ambiguous legal terms and creates uncertainty for both the public procurement offices and companies. In particular in the field of IT security, clear guidelines and unequivocal obligations and rules are important. The Decree introduces a series of terms which have the opposite effect:

- The term “Confidential Information”: The decree refers to “confidential information”, which is defined as “information which a reasonable third party would consider as worthy of protection or which is identified as confidential; this can also be information which is disclosed during an oral presentation or discussion.” As a result of this definition, companies are obliged to assess the confidentiality of customer data themselves. An extension to all data which “a reasonable third party would consider as worthy of protection” creates legal gray zones, a need for interpretation and eventually legal uncertainty. The confidentiality of data should be established exclusively by the principal and identified clearly as such.
- The term “Possible Security Relevance”: The Decree refers to public procurement procedures with a “possible security relevance”. This creates once again a host of rooms for interpretation and ambiguities. As a result of this rule, it might in future be necessary to make a declaration of eligibility on a regular and general basis. In this connection, a concretization is necessary concerning the data classified as relevant in terms of security as well as in respect of the threat scenarios. This should be implemented closely in line with the already existing framework of the Public Procurement Code Defense and Security (VSVgV).

Secondly: The clauses bear an ambiguous relationship to the specifications. The underlying principle of public procurement law is the unequivocal and final specification of the service. The clearer this specification is drafted, the lower the risk of misunderstandings, miscalculations and eventually budget overruns. The decree submitted qualifies the specification and creates ambiguities concerning the concrete requirements in the field of IT security. The latter can only be usefully defined by objectifiable criteria. The current form of the Decree is not appropriate for this purpose.

Thirdly: The existing decision of the 2nd Public Procurement Tribunal, which deals with the current “No Spy” Decree, emphasizes that the issue of an obligation of data dissemination cannot be solved by a reliability check within the framework of the eligibility check of a tenderer, which takes center stage in the Decree. According to this decision, “personal” characteristics matter, also with a view to the European legal framework, and not the subjection to a foreign legal order. It should, therefore, be carefully considered how under these conditions the applicable legal norms and hence the stated goals can actually be achieved with a view to a de facto exclusion from public procurement procedures.

Fourthly: The Decree exacerbates the problem of incompatible international legal norms. Companies are under a worldwide obligation to cooperate with the security authorities. In Germany, this applies e.g. to the Act to restrict the Privacy of Correspondence, Posts and Telecommunications (Article 10 Act). A clause which requires the companies to contractually exclude these duties of cooperation, creates an irresolvable dilemma for the companies. They cannot meet the statutory requirements under the public contract without violating regulations in other countries and vice versa. Consequently, this scenario applies not only to foreign

groups which have a subsidiary in Germany, but also to German groups operating abroad. As a result, the Decree accentuates the problem of international, incompatible legal norms and transfers responsibility for resolving this dilemma to the companies.

Fifthly: The complication of the burden of proof for the tenderer is unfair because an abstract legal or technical suspicious circumstance is considered as sufficient proof; i.e. the suspicious circumstance is equated to a violation of a duty and establishes the exclusion from the procedure and/or justifies a termination of the contract. Consequently, the tenderer has no opportunity to prove that there has not been any breach of confidentiality.

### Recommendations

- **In terms of procurement law:** a clearer definition of the terms used and an orientation on the applicable principles of procurement law. This applies, more particularly, to the completeness of the specifications.
- **In terms of security policy:** focusing on objectifiable criteria at the definition of IT security standards, which have a real influence on the security level and minimize risks.
- **Internationally:** Understanding in respect of the handling of incompatible legal norms, within the scope of the TTIP negotiations amongst others.

### Contact AmCham Germany Telecommunications, Internet, and Media (TIM) Committee

#### *Chair*

Dr. Nikolaus Lindner, LL.M.  
Head of Government Relations Germany, eBay GmbH

#### *Co-Chair*

Mike Cosse  
Vice President Government Relations Middle & Eastern Europe, SAP SE

#### *Co-Chair*

Dr. Gunnar Bender  
Head of Corporate Communications, Marketing & Politics

#### *Staff Contact*

Constanze Krüger  
Assistant, Government Relations  
American Chamber of Commerce in Germany e.V.  
Charlottenstrasse 42, 10117 Berlin  
T +49 30 288789-24  
F +49 30 288789-29  
E [ckrueger@amcham.de](mailto:ckrueger@amcham.de)