Cybersecurity and the Procurement Procedure

3 November 2020

Cybersecurity is becoming increasingly important. In the wake of cyberattacks on the German parliament, the foreign office and on prominent public figures, there is now greater awareness of the need for the state and companies to protect the integrity of their existing IT systems. The following article explains how a public contracting entity can achieve a higher standard of cybersecurity through its procurement procedures. Another related article provides an overview of some of the particularities that arise in the procurement of cybersecurity goods and services.

Through several strategic decisions concerning the design of the tender procedure, public authorities can help to enhance the technological integrity of the goods or services they are acquiring. The legal framework allows various ways of doing this: the public authority can ascertain the cyber integrity of the future contract holder by setting up specific eligibility requirements (see 1) and through the exclusion of tenderers (see 2). The informational security of the procured goods and services themselves can be guaranteed by including relevant provisions within tender specifications and adding award criteria related to cyber security (see 3). Public authorities can also strengthen the integrity of the procedure itself by requiring tenderers to comply with certain procedural guidelines (see 4).

1. Cyber integrity of the prospective contract holder

The eligibility assessment presents an opportunity for the public authority to set certain standards, which the prospective contract holder must meet. It thereby guarantees a satisfactory level of information security for all parties involved. For instance, public authorities may request evidence of professional experience or seek customer references in the areas of IT-security and data protection. Additionally, they can make qualified and trained personnel and state-of-the-art cybersecurity technology a prerequisite for eligibility. In the context of tenders that include the processing of sensitive data, these elements fall into the category of "technical and professional ability" and can therefore be set as a requirement for all companies interested in a tender.

Even in comparatively simple procurement procedures, public authorities have the option of ascertaining the tenderer's level of cyber integrity, without being forced to having to conduct time-consuming and expensive case-by-case assessments. To do this, they can request general evidence concerning a company's cybersecurity standards, in the form of fully developed security concepts or recognised certificates based on the standards set out, e.g. by the German Federal Office for Information Security (BSI). Also possible – although initially requiring greater effort – is the implementation of a US-style

prequalification system for the area of cybersecurity (cf. for example: https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars-compliance). This would help enormously in making the eligibility assessment process more efficient and reducing the related costs, without having to forego high standards of cyber integrity.

2. Exclusion of tenderers

Public authorities may exclude specific tenderers during the eligibility assessment process if they have experienced data leaks or other IT security breaches in the past or have otherwise violated legal or contractual obligations related to cybersecurity. These prior wrongdoings are sufficient ground for exclusion if the tenderer acted grossly negligent and the consequences of the breach were not negligible. This is because these breaches of duty can be considered "grave professional misconduct" and thereby justify an exclusion from the tender process. If the breaches of cyber security obligations were committed in the context of an earlier contractual relationship resulting from a tender procedure, the tenderer may furthermore be excluded because it has demonstrably performed an essential requirement of a public contract inadequately in the past.

In practice, public authorities will accept a declaration from the bidder stating that there are no grounds justifying exclusion as sufficient proof. If, however, a tender has significant national security implications, this practice should be considered carefully. The contracting authority may also ask individual bidders for information or request them to provide a separate explanation if there are justified doubts as to the accuracy of the self-declaration. The public authority should consider this procedure in particular if press reports or other evidence suggest that bidders have attracted scrutiny in the area of cyber integrity due to earlier violations and misconduct.

3. Cyber integrity of the procured goods and services

Contracting authorities may try to ensure the cyber integrity of the procurement objects in a number of ways. In particular, they may make use of fully developed tender specifications, contract-specific award criteria and corresponding contractual regulations.

The **tender specifications** serve to determine and specify the object subject to the procurement. Public authorities can use this as an opportunity to enhance the protection of sensitive information. Within the scope of the tender specifications and certain legal standards the public authority may, for example, require the bidder to integrate certain certified components into the product. Alternatively, it may also set out special procedures for the provision of services that strengthen the integrity of data communication and processing. The requested goods or services must be described as clearly and in as much detail as possible. A practical way of doing this would be a so-called functional description, which only lists the technical requirements the final product or service has to meet, allowing the tenderers to develop their own solutions.

In addition, the public contracting authorities may consider qualitative aspects as **award criteria** in addition to the price if they are related to the subject of the tender. A satisfactory level of cyber integrity might reasonably be specified as one of the key aspects relevant for the awarding decision. A contracting authority may demand, for instance, a thoroughly thought-out cybersecurity proposal from the bidders. Such a proposal might not only be included in the evaluation of the bid, but also be declared a contractual obligation and thus specify the service to be provided.

Finally, the contracting authority may also lay down **conditions for the execution of the awarded contract**, if these relate to the subject of the tender. Such conditions, for example in the form of obligatory regular "stress tests" of the company's IT infrastructure, are explicitly allowed to protect the confidentiality of information. Another possibility might be to contractually demand that the servers hosting the relevant data are stationed in Europe.

4. Cyber integrity of the procurement procedure itself

Finally, public authorities have various instruments at their disposal to ensure the cyber integrity of the procurement procedure itself. This is not limited to the general legal obligation of the contracting parties to maintain confidentiality. Public authorities may take additional measures to ensure the security of data communication and storage during the procedure. Particular caution is necessary in the communication of questions and answers between the bidders and the contracting authority. The protection of information security is especially relevant in this situation because, according to the principle of equal treatment, the answers that the public authorities give must in general be made available to all tenderers.

Communication between the parties in tenders which have no defence or security implications are supposed to be conducted by electronic means throughout the entire procedure. In addition to the requirement to encrypt tender responses, the contracting authority may choose a higher security level for electronic communications or require advanced or certified electronic signatures or seals, if deemed necessary. If sensitive data is involved, which cannot be properly secured using generally available or alternative electronic means, the contracting authority may also demand a written offer.

In addition to the possibilities mentioned above, the contracting authority must take further measures for tender procedures with security or defence implications. It must strictly guarantee the security of any data or information, in particular if classified information is involved. For example, in cases where even the application for participation requires access to information classified as "confidential" or even more sensitive, bidders must obtain a specific security certificate from the competent ministry before such access is granted. In the case of bidders based abroad, the competent ministry may also request information on the security of the premises used or the personnel employed by the bidder from the relevant national security authority. In discussions with the tenderer,

the contracting authority is free from the outset to choose the most appropriate means of communication in accordance with relevant security considerations. Confidentiality and data protection obligations may even demand that the public authority makes the tender documents available for personal inspection only.

5. Conclusion

Public authorities have numerous tools available to react to the growing relevance of cyber integrity in procurement procedures and to ensure that the standard of information and data protection continues to improve. The contracting authority can strengthen the cyber integrity of the award process and the following performance of the contract by placing specific requirements on the tenderer, the procured goods and services and the procurement procedure itself.

BLOMSTEIN will continue to monitor and report on the developments. If you have questions about the potential impact of cybersecurity in your company or sector, Roland M. Stein and Christopher Wolters are more than happy to provide assistance.