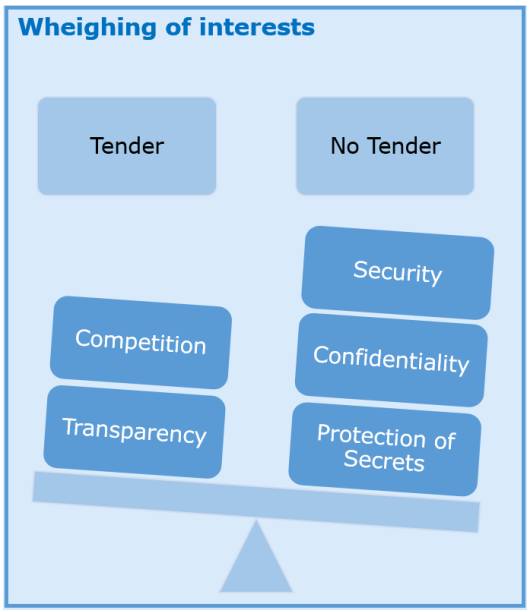
Purchasing Cybersecurity Goods and Services

29 October 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 will provide an overview of some of the particularities that arise in the procurement of cybersecurity goods and services. Another article explains how a public contracting entity can achieve a higher standard of cybersecurity in its procurement procedures.

Many companies already offer a wide range of effective products and services that increase cybersecurity standards. These vary from simple, standardised software solutions such as firewalls and virus protection, to highly secured server rooms, and advice on the creation of coherent cybersecurity structures. It even extends to specialist software for security agencies carrying out investigations designed to access third party computer systems.

When acquiring cybersecurity goods or services there is significant tension between, on the one hand, compliance with relevant public procurement law regarding non-discriminatory and transparent competition and, on the other hand, the public contracting authority's need for tailored solutions. National security and confidentiality concerns also play an important role. Embedded industry interests in building and developing German and European expertise in this particular field create further complexity. How this tension is resolved in each case largely depends on which public procurement procedure is appropriate and available:



- The **negotiated procedure without a call for competition** is predestined for the acquisition of a particular product or service provided by a specific company. As it hinders competition, the procedure is available only in very specific circumstances and subject to strict requirements. In general, it is permissible in cases in which only one available product or supplier meets the required minimum standard regarding IT security. The procedure might also be employed if migration of sensitive data to a new system or incompatibility between different

systems used by the public authorities would lead to serious security risks. Lastly, it is also regularly permissible in cases in which certain proprietary rights restrict the tender to only on possible supplier. This occurs, for example, when the public contracting authority seeks to obtain updates for existing software, software maintenance services or additional licences for particular IT security products that are already in use.

- If the public authority's choice is not limited to one product or one supplier, then the **negotiated procedure with a call for competition** is preferable for complex projects. In this procedure, companies present their solutions based on the requirements set out by the public authority and the parties can negotiate specific terms. The public authority may then select the best product or services from those offered. This process enables the public authority to modify and refine the terms of the contract and to thereby purchase innovative solutions and state-of-the-art technology. In the past, this procedure has been used to acquire goods and services aimed at analysing vulnerabilities and weaknesses in IT infrastructure, for big-scale projects aimed at increasing employee awareness of cybersecurity topics, and for the creation of contingency plans to be used in the case of successful cyberattacks.

- To build or expand on state-of-the-art technology a public authority may use an **Innovation Partnership**. This type of tender offers the possibility of developing new products and services that are not available on the market yet in collaboration with one or several selected companies. While this procedure has not yet gained significant relevance in practice, it could help to minimise dependence on non-EU products or systems in the IT security sector and strengthen the German and European presence on the cybersecurity market. These innovation partnerships could be suitable for large-scale projects in the field of IT, such as the development of complex spy software or defence systems.

- Tenders for standardised goods and services without security implications can also be dealt with in an **open procedure**. This procedure is suitable for tenders for basic employee training on IT security or regular, general analyses of the current cyber threat level ("threat assessments").

- In the very limited cases set out in **Article 346 of Treaty on the Functioning of the European Union**, the public authority is permitted to acquire a specific product or service without calling for a tender at all. This only applies if the "essential interests of [a member state's] security" are affected. According to the newly introduced Section 107 Paragraph 2 Sentence 2 of the German Act against Restraints of Competition (GWB) this is also the case where the public contract concerns key defence or security technologies. These key technologies also

include security-relevant IT and communication systems, such as cyber defence systems, and solutions using artificial intelligence (AI).

The coming years will show how contracting authorities can best resolve the tension between competition and security concerns and which types of procedures will prevail in the procurement of goods and services in the area of cyber security.

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