Cybersecurity and Foreign Direct Investment Controls

10 November 2020

Digital information and online communication are becoming more and more important. As a result, people are increasingly aiming to protect their IT systems against attacks. Cybersecurity considerations play a special role in governmental restrictions on foreign direct investments (*FDI*) to protect against foreign interference in key infrastructure or security-related sectors. In Germany, this has led to increased scrutiny of M&A transactions by the German Federal Ministry for Economic Affairs and Energy (*FMEA*) – not limited to companies active in key areas of software development or IT security.

Background

Governmental restrictions on FDI are aimed at protecting national security and public order from dangers, which could arise from foreign investments in German companies. The FMEA can investigate such foreign investments and prohibit them where appropriate. In previous years, its review of M&A transactions was seen as a formality, but they are taken increasingly seriously. Following the widespread publicity surrounding the acquisition of robot manufacturer KUKA by the Chinese investor Midea in 2016, the German government tightened its investment control and is continuing to do so.

In 2019, the EU FDI Screening Regulation established the very first European framework for foreign direct investment, which has been directly applicable in all EU member states since October 11, 2020. The German legislator has already implemented requirements of the EU Screening Regulation in the First Amendment to the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz – AWG)* and the 16th amendment to the Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung – AWV*). In particular, the standard of review has been modified. Now, FDI screenings will no longer be based on an "actual threat" but on an "expected impairment" of public safety or order taking into consideration the interests of other EU member states as well. Additionally, a ban on enforcement of investments for the duration of the screening procedure was introduced. Further tightening of the German FDI screening framework is expected as a result of the upcoming 17th amendment to the AWV. According to most recent announcements, the obligation to report investments will be expanded, especially with regard to critical technology areas such as cybersecurity or AI. The previous tightenings are also becoming apparent in practice. Meanwhile, the screening periods of up to four months are often fully exhausted and clearance is sometimes only granted under certain conditions – e.g. the disposal of security-related parts of the business.

Cybersecurity and National Security

The German system of FDI control is three-fold. The strictest control applies to **sector-specific investments** covered by Section 60 Foreign Trade and Payments Ordinance (*FTPO*) (***category 1***). This usually applies to foreign investments in German companies dealing with weapons or other military equipment. Such investments must be reported to the FMEA and require explicit clearance. Before clearance is granted the M&A contracts will not come into force.

Other investments must be reported to the Ministry, but no clearance is required (***category 2)***. The FMEA can block these investments if they endanger national security or public order. Investments by non-EU companies in German companies that have been classified on this basis as security-related may be restricted. This includes companies active in critical infrastructure (e.g. energy, water, the finance and insurance sector, health and transport) and, as of recently, companies in the media industry as well.

For all other investments, there is no reporting obligation (***category 3***). However, the FMEA can generally review any foreign investment, if it considers such review necessary for security reasons. In practice, in some instances, it can be advisable to apply voluntarily for a clearance certificate, and make clearance by the FMEA a closing condition in M&A contracts.

Some **investments in cybersecurity companies** fall within category 1. This applies, in particular, to manufacturers of products authorised by the German Federal Office for Information Security with IT security functions (i.e. encryption technology products), and to companies that have manufactured them in the past (even if it was just a business unit), regardless of the size of the business (no *de minimis* threshold). Investments in such companies must therefore be thoroughly reviewed to ensure that any reporting obligation is met. If the reporting obligation is not fulfilled, the FMEA can still block the investment after several years – and in the worst case can declare the M&A contract void.

The vast majority of non-EU investments in cybersecurity companies likely falls into category 2. This is because IT and telecommunication companies are often part of critical infrastructure. Additionally, investments in companies that develop software for operating critical infrastructure, providers of cloud computer services or communication tools in the health sector (so called "telematics infrastructure"), have to be reported (Section 55 Para. 1 S. 2 & Para. 4 FTPO). The FMEA can prohibit such investments.

Extensive use of Investment Control a Result of Lowering the Review Threshold?

German investment control laws have undergone many changes in the past few years. The fear of theft of "know-how", additionally fuelled by the pandemic caused by the

SARS-CoV-2 virus, is driving national and European legislators towards an extensive investment control. This tendency became especially apparent with the lowering of the FDI screening thresholds for companies of category 1 and 2 in 2018. The German government believed that this was the only way to protect the relevant sectors (e.g. cybersecurity) against damaging foreign investments. It can be assumed that the number of reportable company acquisitions will increase again due to the upcoming regulatory measures, especially in the cybersecurity industry.

Conclusion

The increasing restrictions on foreign investments under the banner of cybersecurity appears to be successful. However, this has meant a reduction in the intensity of competition while increasing government intervention. The government is using its powers of intervention to an even greater extent – especially to protect digital infrastructure. Foreign investors considering an acquisition of a company active in IT infrastructure or surveillance technology are advised to keep these regulatory developments in mind, to avoid delays or failure of the acquisition. Experience shows that transparent communication with the FMEA has a positive effect on the transaction.

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 Leonard von Rummel are more than happy to provide assistance.