

# Cyber-Security und Investitionskontrolle

10. November 2020

Digitale Informations- und Kommunikationstechniken gewinnen rapide an Bedeutung. Im gleichen Maße steigt auch das Bestreben, die IT-Systeme vor Angriffen zu schützen. Das Thema „[Cyber-Security](#)“ findet eine besondere Ausprägung in der [staatlichen Investitionskontrolle](#), die vor Gefahren bei ausländischen Investitionen in kritische Infrastrukturen oder besonders sicherheitsrelevante Branchen schützen soll. Die Folge ist in Deutschland eine zunehmende Kontrolldichte von M&A-Transaktionen durch das Bundesministerium für Wirtschaft und Energie (*BMWi*) – nicht nur für Unternehmen, die im Kernbereich der Softwareentwicklung oder IT-Sicherheit tätig sind.

## Hintergrund

Die Investitionskontrolle dient der Prävention von Gefahren für die öffentliche Ordnung und Sicherheit, die durch den Erwerb inländischer Unternehmen durch ausländische Investoren entstehen können. Das BMWi kann ausländische Investitionen in deutsche Unternehmen überprüfen und gegebenenfalls untersagen. Während die Investitionskontrolle im Rahmen von M&A-Transaktionen vor einigen Jahren noch eine Formalie war, wird sie seit Kurzem zunehmend ernster genommen. Nachdem im Jahr 2016 der Erwerb des Roboterherstellers KUKA durch den chinesischen Investor Midea hohe Wellen schlug, [verschärfte](#) und [verschärft](#) die Bundesregierung die Investitionskontrolle zunehmend.

Mit der [EU-Screening-Verordnung](#) wurde sodann im Jahr 2019 erstmals ein europäischer Rahmen für ausländische Direktinvestitionen beschlossen, der seit dem 11. Oktober 2020 unmittelbar in allen EU Mitgliedsstaaten gilt. Der deutsche Gesetzgeber hat Vorgaben aus der EU-Screening Verordnung bereits teilweise durch die [Erste Novelle des Außenwirtschaftsgesetzes](#) und die [16. Novelle der Außenwirtschaftsverordnung](#) umgesetzt. Verschärft wurde hierbei insbesondere der Prüfungsmaßstab. Bei der Investitionsprüfung maßgebend wird nun nicht mehr eine „tatsächliche Gefährdung“, sondern bereits eine „voraussichtliche Beeinträchtigung“ der öffentlichen Sicherheit oder Ordnung sein, wobei auch die Interessen anderer EU-Mitgliedsstaaten zu berücksichtigen sind. Neu ist auch das Vollzugsverbot für die Dauer der Investitionsprüfung. Weitere Verschärfungen sind durch die 17. Novelle der Außenwirtschaftsverordnung zu erwarten. Schwerpunktmäßig soll nach bisherigen Verlautbarungen die Meldepflicht insbesondere auch in Bezug auf kritische Technologiebereiche, wie Cyber-Security oder KI, erweitert werden. Die bisherigen gesetzlichen Verschärfungen zeigen sich auch in der Praxis. Mittlerweile werden die Prüffristen von bis zu 4 Monaten zum Teil voll ausgeschöpft und Freigaben mitunter nur unter Auflagen – wie z.B. der Abtrennung sicherheitsrelevanter Geschäftsbereiche – erteilt.

## **Cyber-Security und öffentliche Sicherheit**

Das System der Investitionskontrolle ist dreigliedrig aufgebaut. Die stärkste Kontrolle besteht bei der **sektorspezifischen Investitionskontrolle** nach § 60 AWV (**Kategorie 1**). Üblicherweise betrifft die Kontrolle Investitionen aus dem Ausland in deutsche Unternehmen, die mit Kriegswaffen oder bestimmtem militärischem Equipment handeln. Solche Investitionen sind beim BMWi zu melden und erfordern eine explizite Freigabe durch das Ministerium – vorher sind die M&A-Verträge nicht wirksam.

Für andere Investitionen besteht eine Meldepflicht an das Ministerium, aber kein Freigabeerfordernis (**Kategorie 2**). Das BMWi kann diese Investitionen jedoch untersagen, falls sie eine Beeinträchtigung der öffentlichen Ordnung oder Sicherheit darstellen. Das betrifft im Rahmen der **sektorübergreifenden Prüfung** Investitionen von unionsfremden Unternehmen in deutsche Unternehmen, die vom Gesetzgeber als sicherheitsrelevant eingestuft werden. Darunter fallen z.B. Unternehmen, die eine kritische Infrastruktur betreiben (z.B. Energie, Wasser, Finanz- und Versicherungswesen, Gesundheit, Transport) oder auch Unternehmen der Medienwirtschaft.

Für alle anderen Investitionen besteht keine Meldepflicht (**Kategorie 3**). Allerdings kann das BMWi grundsätzlich alle ausländischen Investitionen überprüfen, sollte es die Investition für sicherheitsrelevant erachten. In der Praxis empfiehlt es sich häufig, auch für Fälle der Kategorie 3 freiwillig eine sog. Unbedenklichkeitsbescheinigung beim BMWi zu beantragen und die Erteilung der Unbedenklichkeitsbescheinigung als closing-condition in den M&A-Vertrag aufzunehmen.

Manche **Investitionen in Cyber-Security-Unternehmen** fallen in die Kategorie 1. Das betrifft insbesondere Investitionen in Unternehmen, die vom Bundesamt für Sicherheit in der Informationstechnik zugelassene Produkte mit IT-Sicherheitsfunktion herstellen oder in der Vergangenheit hergestellt haben (vor allem Kryptotechnologieprodukte). Es genügt hier, dass ein Geschäftsbereich eines Unternehmens vor Jahren Kryptotechnologieprodukte hergestellt hat. Auf die Größe dieses ehemaligen Geschäftsbereichs kommt es nicht an (keine *de minimis* Schwelle). Investitionen in solche Unternehmen sind daher besonders sorgfältig auf eine Meldepflicht zu prüfen. Unterbleibt eine Meldung, kann das BMWi die Investition auch nach mehreren Jahren untersagen und im schlimmsten Fall die Nichtigkeit des M&A-Vertrages herbeiführen.

Die überwiegende Anzahl der unionsfremden Investitionen in Cyber-Security-Unternehmen dürfte in die Kategorie 2 fallen. Denn IT- und Telekommunikationsunternehmen zählen häufig zu den kritischen Infrastrukturen. Auch Investitionen in Unternehmen, die Software zum Betrieb kritischer Infrastrukturen entwickeln, bestimmte Cloud-Computing-Dienste anbieten oder Kommunikationsmittel im

Gesundheitswesen (sog. Telematikinfrastruktur) anbieten, sind zu melden (§ 55 Abs. 1 S. 2 i.V.m. Abs. 4 AWW). Solche Investitionen können vom BMWi untersagt werden.

## **Extensive Anwendung der Investitionskontrolle?**

Das Investitionsprüfungsrecht hat in den letzten Jahren viele Änderungen erfahren. Dabei treibt nationalen und europäischen Gesetzgeber die Angst vor „Know-how“-Diebstahl, die nicht zuletzt durch die Corona-Pandemie befeuert wurde, hin zu einer extensiven Investitionskontrolle. Dieser Trend war bereits mit der Absenkung der Prüfungsschwellenwerte für die Unternehmen der Kategorien 1 und 2 von 25 % auf 10 % im Jahr 2018 zu vernehmen. Die Bundesregierung war dabei der Auffassung, dass nur so relevante Branchen wie die Cyber-Security vor schädlichen ausländischen Investitionen geschützt werden können. Es ist davon auszugehen, dass auch die kommenden regulatorischen Maßnahmen zu einer Ausweitung der meldepflichtigen Unternehmenserwerbe, insbesondere auch im Bereich der Cyber-Sicherheitsbranche führen werden.

## **Fazit**

Die Zunahme der außenwirtschaftsrechtlichen Regelungsdichte unter dem Schlagwort der Cybersicherheit scheint hehre Ziele zu verfolgen. Allerdings bedeutet sie eine Verringerung der Wettbewerbsintensität zugunsten staatlicher Interventionsmöglichkeiten. Die Bundesregierung schöpft diese Möglichkeiten auch mehr und mehr aus – insbesondere zum (vermeintlichen) Schutz der digitalen Infrastruktur. Ausländischen Investoren, die einen Unternehmenskauf im Bereich der IT-Infrastruktur oder der Überwachungstechnologie planen, ist daher eine frühzeitige Befassung mit dem Thema anzuraten, um eine Verzögerung oder sogar eine Untersagung des Erwerbs zu vermeiden. Die Praxis zeigt, dass eine transparente Kommunikation mit dem BMWi in den meisten Fällen positive Wirkungen zeigt.

BLOMSTEIN wird die weiteren Entwicklungen beobachten und darüber informieren. Wenn Sie Fragen zu den potenziellen Auswirkungen der Cyber-Security auf Ihr Unternehmen oder Ihre Branche haben, stehen Ihnen [Dr. Roland M. Stein](#) und [Dr. Leonard von Rummel](#) jederzeit gern zur Verfügung.