Business Law Magazine

In this issue

Corporate Sanctioning Act – Competition law – Cybersecurity – International law
Dear Reader,

This issue of Business Law Magazine focuses on the reform of competition law. In two articles, we highlight the innovations that lie ahead for corporate and consulting practices. Don’t miss the articles by Michael Holzhäuser, Nadja Waksman and Peter Giese.

Cyberattacks on enterprises are growing more and more threatening, and the possible resulting damages are enormous. Our author Klaus Brisch has an exciting idea how practices can effectively arm themselves against cyberattacks: the cyberthreat platform. This is also a must-read.

Finally, the topic of digitization in the legal market is a trend-setting issue for (in-house) lawyers. We would therefore like to invite you to attend our fourth In-house Matters conference in Frankfurt on the afternoon of December 2, 2019. To see the first-class speakers and panels that await you, please visit following link. We look forward to seeing you at the Frankfurt School of Finance.

Yours sincerely,

Thomas Wegerich
Companies should prepare for the new law

Significance of the draft law regarding collective sanctions for foreign associations

By Dr. Bernd Federmann and Michael Pohl

The German Federal Ministry of Justice (BMJV) has drawn up a draft of a “law to combat corporate crime,” the most essential part of which is the “draft of a Corporate Sanctioning Act” (Verbandssanktionengesetz or VerSanG-E). The draft has not yet been published, but it is available to certain associations for review purposes. The VerSanG-E aims to create an independent legal framework for sanctioning associations and thus to subject them to the principle of legality (Legalitätsprinzip), according to which proceedings must be initiated if there is suspicion of wrongdoing. Compared with the current German legal situation, the VerSanG-E also contains some changes for foreign associations.

Offense and scope

An association sanction will be imposed if a leader of the association has committed an association-related crime or a nonleader has committed an association-related crime in the performance of the association’s tasks, provided that companies now have time to prepare for the new law, particularly by means of compliance measures.
a leader of the association could have prevented or substantially impeded the crime by means of appropriate preventive measures. An offense committed by an association may include property or tax crimes as well as all categories of crimes within German criminal law, particularly environmental crimes, personal injury crimes (for example, as a result of defective products) and crimes related to certain competition regulations.

An association within the meaning of the VerSanG-E can be a legal entity under public or private law, an association with no legal capacity or an incorporated partnership. New to the current legal situation is the extension of the scope of the VerSanG-E to include crimes committed abroad, as up until now, multinational corporations have been able to evade responsibility for violations abroad by hiring foreign employees. This gap will now be closed: The VerSanG-E is intended to cover offenses committed abroad where German criminal law does not apply if the relevant association has a seat in Germany at the time of the offense, the offense is punishable in Germany and the offense also constitutes a criminal offense at the place of wrongdoing or is not subject to criminal enforcement there. It is not necessary for the legal seat of the association to be located in Germany; the existence of a German administrative seat is enough. However, due to the required existence of a seat in Germany, the VerSanG-E still clearly falls short of the “long-arm jurisdiction” of the FCPA or the UK Bribery Act.

Sanctions

The possibilities contained in the draft law regarding association sanctions go far beyond the existing instruments of German administrative offense law. The draft bill provides for the following association sanctions:

- financial penalties for associations (Verbandsgeldsanktion),
- warnings reserving the right to impose a financial penalty (Verwarnung mit Verbandsgeldsanktionsvorbehalt), and,
- as a last resort, the dissolution of the association (Verbandsaufsässung).

Depending on the size of the company and the degree of fault, sanctions can total up to € 10 million. If a large company (average annual turnover of more than € 100 million) is to be sanctioned, the sanctions can be calculated as a percentage (5%-10%, again depending on the degree of fault) of the annual turnover of the entire group of companies.

The draft includes the possibility to warn a company of an impending financial penalty, provided it is to be expected that such a warning is sufficient to prevent future offenses (for example, if a warned company establishes a compliance management system).

Finally, as a last resort, the dissolution of the association will be applicable as a sanction. However, this will only be possible in exceptional cases — inter alia, if “persistent and considerable offenses committed by the association” have been committed by managers and it is to be expected that considerable offenses will continue to be committed by the association in the future. However, the dissolution of foreign associations is excluded due to the German courts’ lack of jurisdiction. This is also the reasoning behind the draft.

In general, the draft bill states that associations may not be prosecuted if sanctions are to be expected against the association abroad and the sanctions that might be imposed in Germany are not significant.

Contingent liability

Another aspect of the draft bill is contingent liability (Ausfallhaftung). If the association becomes defunct after the announcement of opening proceedings or if its assets are moved to such an extent that the enforcement of the sanction is impeded, the VerSanGe-E provides avenues of recourse. To this end, a separate liability amount may be established against associations, which, at the time of the offense, formed an economic unit with the association in question or took over its essential assets.

In case of doubt, contingent liability could also apply to foreign group parent companies not domiciled in Germany but that could be held liable for subsidiaries domiciled in Germany. The text of the draft bill does not exclude the possibility of such claims. It is particularly doubtful whether the limitation to associations domiciled in Germany also applies to contingent liability, as contingent liability does not constitute a formal sanctioning of the foreign holding company but rather represents a recourse liability for the group subsidiary. Additionally, the respective section of the draft bill does not contain a corresponding exclusion of
associations not domiciled in Germany with regard to contingent liability.

**Encouraging compliance measures**

At various points in the draft, it is expressed that the aim of the VerSanG-E is to promote the improvement of compliance measures. The existence of a suitable compliance management system, for example, should be enough to prevent the fulfillment of conditions for sanctioning. Should a sanction nevertheless be imposed, the existence of a suitable compliance management system should be relevant in the determination of the sanction type and amount. A compliance management system should also be taken into consideration when a warning is issued with the suspension of a financial penalty and when behavior is assessed after an offense has been committed. It is still unclear, however, which specific measures must be taken to establish an appropriate compliance management system. The FCPA Sentencing Guidelines and the Guidance Document on the Evaluation of Corporate Compliance Programs issued by the US Department of Justice, Criminal Division, for example, are much more precise in this respect.

**Internal investigations**

The VerSanG-E also aims to create a legal framework for internal investigations. Internal investigations can lead to a reduction in penalties only under certain conditions, including that the association genuinely contributes to clarifying the facts, cooperates fully with the prosecuting authorities and fully respects certain newly introduced employee rights. The prohibition of seizure is to be limited to the relationship of trust between the defendant and defense counsel and shall not protect records made prior to the initiation of the investigation proceedings or records that served other purposes.

**Register of sanctions**

The draft provides for an association sanctions register, which is not open to public inspection. All legally enforceable court decisions issued against an association are to be entered there.

**Timeframe**

The law will not come into force until two years after its publication, and the respective legislative process will likely not be completed until next year. As a result, companies now have time to prepare for the new law, particularly by means of compliance measures.

---

[www.kpmg-law.com](http://www.kpmg-law.com)

Dr. Bernd Federmann
Rechtsanwalt, Partner
KPMG Law Rechtsanwalts
geellschaft mbH
Stuttgart
bfedermann@kpmg-law.com

Michael Pohl
Rechtsanwalt, Manager,
KPMG Law Rechtsanwalts
geellschaft mbH
Leipzig
mpohl@kpmg-law.com
Tightening the screws on tech titans

Responding to digitization in the German Competition Act

By Dr. Michael Holzhäuser and Nadja Waksman

Continued legal reforms are necessary to keep up with a rapidly developing digitized world that is intertwined with data protection and privacy. In investigating abuse of “dominance” (market power) cases, old parameters, such as market shares and barriers to entry, no longer provide adequate tools to truly capture a data-intensive company’s position in an inherently dynamic market. With data being the new raw material of the future, regulators must find a delicate balance between under- and overenforcement to protect innovation in markets where entry can easily be disruptive. Further, new tools are needed to deal with the economics of multisided platforms.

Germany has sped ahead with a further draft amendment (Novelle) to its Competition Act (GWB), having already adjusted its merger notification thresholds to capture the transaction value of deals. German competition legislation has also introduced the concept that a “market” need not be linked to monetary compensation. The Novelle focuses on the challenge of “access to data” as an indicator of market power, countervailing the tendencies of monopolization of platform markets and the position of intermediaries in multisided platforms. This legislative change is accompanied by a call by the German Competition Authority (Bundeskartellamt, BKArtA) for more competencies, particularly in the areas of consumer and data protection.

At the time of this writing, other jurisdictions (such as Australia, France and Singapore) have focused on carrying out market reviews and setting out recommendations, with some countries being satisfied that their current legislative tools are sufficient to deal with the challenges of a digital economy. The UK government has indicated that recommendations set out in the Furman Report will be included in a competition green paper later this year and the JFTC in Japan has indicated that “unfair means of personal data collection,” and “unfair utilization of personal data” could be new types of abuses. Responding to changes in a digitally transformed economy...
also calls for a reform on a European level, including an evolvement of Article 102 of the TFEU. The Commission’s response to the “Competition policy for the digital era” report and the G7 summit this summer remains eagerly awaited.

Background to the Novelle

The German Federal Ministry of Economics and Technology intended to address both German and European platforms with its latest draft amendment to the GWB (as of October 7). The Novelle will be presented to other ministries for their approval before being laid before the German Parliament.

The amendment runs in tandem with the recent industry report titled “Commission Competition Law 4.0” and is designed to implement the ECN+ Directive increasing the efficiency of competition law. Dealing with data in defining market power, broadening the scope of abuse of dominance theories and granting better consumer protection form the backbone of the Novelle. It also echoes a study by Haucap, Kerber and Schweitzer, which was commissioned in 2018.

The amendment should also be seen against the backdrop of recent EU Commission decisional practice that emphasizes the low “capability to restrict” standard in abuse of dominance cases and novel theories of harm. For example, the infringement decision in Google Shopping was based on a theory of “self-preferencing” that was deemed capable of excluding rival comparison shopping sites. In that sense, the EU Commission is sanctioning a “new type” of practice.

Data as indicator of market dominance

To demonstrate abusive behavior, it is first necessary to prove an undertaking was dominant (had market power). The Novelle contemplates introducing the concept of “access to data,” which is a new parameter in assessing dominance alongside established factors including market shares. The broadening of the concept of market power is significant, as it is likely to apply to a large group of data-driven businesses including social media platforms, fintech businesses and online booking sites.

Businesses will now need to have a good grasp of the volume and type of data they hold and to what extent their data set is unique and if, how, where and which other market operators would be able to access a data set from other sources. Not only is greater vigilance needed to avoid a potential abuse of such market power (such as unlawfully “restricting access to data”), but the wider definition of dominance will also influence how data-intensive mergers are assessed where incumbents may have a competitive advantage that is not reflected in their market shares.

The importance of an intermediary’s service as indicator of market dominance

Further, in the context of multisided markets, the importance of an intermediary’s services in accessing supply and sale markets has to be considered in determining a company’s market power. The increasing presence and growth of online multisided platforms (such as Uber, Airbnb and online travel agents) have long prompted the need for greater intervention.

The 2018 study by Haucap, Kerber and Schweitzer introduced the concept of “intermediary power” as a criterion of market dominance. The more an intermediary can bundle the demand for products, the more the suppliers of such products will be dependent on the platform for access to the customers. This dependency can exist even below the current thresholds for market dominance, as the BKArtA following the contemplated legislative wording will now have the power to conclude that an undertaking in a multisided market enjoys a position of “paramount importance.” This language mirrors the notion of digital platforms with “strategic market status” in the Furman Report. One of the factors the BKArtA will look at in determining this status is “access to data.”

Refusing supply of data: a new type of abuse

Applying traditional theories of harm to “digital problems” while preserving legal certainty is arguably the main challenge that legislators face. Although the list of potential abuses of dominance is not closed, there are clear difficulties in mandating “access to data” within a predictable legal framework.

Today, an undertaking would have to offer access to data if it has a dominant position and if that data was deemed “essential” or “indispensable.” However, EU Competition Commissioner Margrethe Vestager stated earlier this year: “Access to data has to be redesigned so that newcomers can compete with big tech giants.” The Novelle has attempted to redesign access to data. Under the proposed amendment, a dominant undertaking may be liable if it refuses to grant access to data, data networks or other infrastructure (including its own)
where such supply of data is “objectively necessary” for a market participant to operate in either an upstream or downstream market. This is subject to the caveat that such a refusal would harm effective competition and there is no objective justification for such a refusal.

If this concept is ultimately adopted in the GWB, it remains to be seen how “objectively necessary” will be interpreted by the courts in Germany and how much lower a threshold it will be compared with the current “essential facilities” standard. However it may be applied, this is a remarkable change, as it broadens the traditional “refusal to supply” theory of harm; it may require access to data without compensation (according to the commentary in the amendment); it removes the defense that supplying data would be impossible or unreasonable to expect; and the duty may be applied to businesses that lack market power in the traditional sense (given the broader data-based definition of dominance described above).

Applying the proposed amendment could mean that it would be unlawful for a bank to refuse fintech companies access to customers’ banking data if the bank is the sole owner of that data and provided that customer consent has been granted.

Banks arguably have an incentive to foreclose fintechs when they offer competing products based on bank-account data — an area to be watched closely, particularly if companies like Facebook and Google enter the financial services space.

The requirement to obtain consent also highlights the jurisdictional conundrum of which enforcement body should be responsible for determining that access to data should be granted — in other words, is it more a competition or a data-protection issue? Although the recent decision by the OLG court in Düsseldorf could be heralded as a victory for Facebook, it does show that it could be appropriate for the BKArtA as a competition authority to investigate a privacy matter given that an exploitative theory can accommodate privacy-related issues. In that case, the BKArtA had, however, failed to show what the competitive level of privacy would have been, which shows one of the many difficulties of competition authorities assessing privacy matters.

Access to data has moved to the forefront of the debate surrounding the digital economy. EU officials have recently suggested that providing access to data could also be a form of remedy to restore competition, even after a business has been found guilty of abuse.

New types of abuse in multisided markets

As explained above, the BKArtA has the power to determine that an undertaking enjoys a position of “paramount significance for competition across markets,” that is, an intermediary that has a special strategic position — this a separate question as to whether an undertaking is dominant. In fact, rule 2 below shows that these questions are treated separately. If so, some types of behavior may now infringe competition law, such as:

1. Treating offers from competitors differently from its own offers (of services or products) when providing access to supply and sales markets

2. Shutting out competitors to the detriment of competition where the undertaking enjoys a competitive advantage and can expand rapidly (even in the absence of any market power)

3. Creating barriers to entry in a dominant market by “free riding” on data that has been collated by another undertaking or demanding terms and conditions permitting such use of data

4. Making the portability of data more difficult and thereby preventing competition

These types of conduct are subject to the traditional (and notoriously difficult to prove) exemption that a restriction was objectively justified, which the company accused of any wrongdoing must demonstrate.

The rule against self-preferencing or discriminating against competitors’ offers (rule 1) may be particular stringent, as it is designed to capture undertakings that offer goods or commercial services on a platform on which other undertakings strongly depend and where consequently a strong asymmetry exists. Businesses cannot therefore prefer their services to those of competitors (Selbsbevorzugsverbot).

Applying this rule means that platforms such as Amazon, for example, would have to ensure that they do not discriminate against offers from other merchants where a platform has a dual role of providing its own products as a merchant and advertising those of third-party merchants.

In response to the BKArtA’s investigation into Amazon, Amazon changed its
terms of business for sellers on its online marketplace. Despite this settlement, Amazon remains under scrutiny, particularly as small and medium-sized businesses in Germany argue that they are being squeezed out of the market — a sentiment echoed by some political parties and trade associations in Germany. Their main concern is that small and medium-sized businesses increasingly depend on dominant digital players.

Linked to this is rule 3, which is designed to prevent dominant undertakings from using data collated by third parties to their own advantage. One way of preventing this would be to create Chinese walls, although it begs the question how this could be practically achieved.

Rule 4 enhances consumer protection by increasing data portability — a key concern voiced in the industry report. In practice, users’ search history could be transferred from one search engine to another, for example. Again, this raises considerable data protection issues.

Greater data portability also prevents the risk of “tipping” in highly concentrated markets as explained below. The industry report had highlighted the concern that platforms with pronounced positive network effects can lead to highly concentrated markets in which an undertaking can become a “gatekeeper.” Such effects can create high barriers to entry precluding the entrance of new market players (referred to as the “tipping effect” once entry into a market is no longer possible).

According to the industry report, this phenomenon is increased when a company benefits from customer experience on one side of a platform to grow on another side of the market. Facebook, to illustrate this with an example, operates a social network platform and online advertisements provided by third parties. The more consumers use Facebook’s network and hit certain “likes,” the more advertisements will be targeted at them.

Another way of reducing this risk is to encourage consumers to “multihome” (that is, to list services on several sites), which in turn requires greater data portability as the industry report suggests.

Mergers: some relaxation of rules, but no killer solution

One of the notification thresholds has been increased, which has arguably excluded some transactions that do not have a significant impact on the market. This is reinforced by the introduction of a de minimis clause that exempts transactions below a certain threshold.

Given the recent debate surrounding them, it is surprising that the Novelle is silent on “killer acquisitions” — that is, acquisitions of an innovative target company with the aim of “killing” either the target product (as in cases in the pharmaceutical sector where an incumbent buys out a pipeline product belonging to the target) or eliminating future independent competition in that market (as is arguably more the case in the digital sector).

Identifying killer acquisitions in the digital sector is particularly problematic, as it not only requires an assessment of immediate harm but also an evaluation of how an embryonic competitor may have developed absent the merger. Given that it is hard to predict what the future effects on an existing or potential competitor are on a forward-looking basis, calls for an ex post review of mergers (that is, once the merger has completed) have become louder. However, the Novelle makes it clear that the current ex ante approach could remain in place, despite the BKArtA’s call for an ex post review.

One way of dealing with such acquisitions would be to capture the deal value of transactions. The EU Commission seems to have adopted a wait-and-see approach depending on how the BKArtA and the Austrian competition authority enforces their newly amended notification thresholds. A further difficulty raised by such acquisitions is who should bear the burden of proof: The EU Commission’s policy report referred to in the introduction of this article recommends shifting the burden to the incumbent to prove the pro-competitiveness of its conduct.

Burning questions remain unanswered. One way of dealing with killer acquisitions in the digital sector may be to focus on an innovation-based competition assessment as developed in the GE/Siemens Alstom, Dow/Dupont or Bayer/Monsanto strand of cases and the protection of “innovation spaces” as the CMA has suggested by the CMA in its consultation on digital mergers.

Guidance on restrictive agreements

A change to be welcomed is the introduction of a voluntary notification request for collaboration agreements that is reminiscent of the premordenization EU approach under which parties would have to first notify a competition authority about an agreement. This move will inject more legal certainty into the current approach in the spirit of collaboration
between market players and the BKArtA, especially where agreements are complex. Parties will receive a decision within six months of submitting such a request.

Conclusion: some answers, many further questions

Breaking up tech giants completely (as increasingly suggested by Elizabeth Warren, the current Democratic front-runner in the US) was deemed to be a method of last resort by Vestager when she spoke at a tech conference earlier this year. However, more empirical evidence is needed to understand how easy market entry is where businesses face large incumbent digital players.

While the suggestions in the recent Novelle may be applauded as an attempt to deal with new challenges in a digital era, competition regulators and legislative bodies around the globe still face a number of to-dos on their list. Some of these are set out in the questions below. Not all of the industry report’s recommendations have been adopted in this Novelle — this includes the suggestion that platforms with a certain minimum level of users or sales implement an alternative dispute-resolution procedure using independent third parties to address infringements on platforms.

But perhaps we need to wait for the next wave of another Novelle ...  

Further questions

- How should coding of software and platforms be analyzed?
- How should competition law deal with blockchains?
- Should competition law deal with unfair commercial practices harming individual consumers?
- Should EU and domestic competition law adopt the US concept of “predatory innovation”?
- Should more parameters be introduced to define the “relevant market” given the last definition dates from 1997?
- How real is the threat of collusion through algorithms and artificial intelligence?
- Should enforcement be pre-emptive? Should competition authorities seek a dialogue with undertakings instead of imposing fines following lengthy investigations?
- Who should bear the burden of proving anticompetitive harm?
- What can be done to promote “open data” institutions for publicly held data?
Inhouse Matters 2019:
Digitalisierung im Rechtsmarkt –
nichts ist beständiger als der Wandel

2. Dezember 2019
Audimax der Frankfurt School of Finance & Management,
Adickesallee 34, 60322 Frankfurt am Main

Weitere Informationen: www.deutscheranwaltspiegel.de/inhouse-matters
Digitization and beyond

The draft 10th amendment of the German Act Against Restraints of Competition

By Peter Giese

Recently, the German Federal Ministry for Economic Affairs and Energy (FMEE) announced that it had finished its preparatory work on the 10th amendment of the German Act Against Restraints of Competition (ARC) and had started the interministerial coordination for the draft bill.

As expected, the draft bill contains fundamental changes to abusive practices in competition law. The aim of the changes is to tackle obstacles arising from the digital economy and the growing importance of access to data. To that end, among other things, the draft bill explicitly introduces new rules for intermediaries and companies with paramount significance across markets. The title of the draft bill, GWB (or ARC) Digitization Law, and previous press coverage regarding the draft bill create the impression that digitization constitutes the main part of the draft bill.

This is, however, far from the truth: The new digitization rules are not the only centerpiece of the draft bill. Rather, with the draft 10th amendment of the ARC, the German FMEE would substantially amend the law in several places. Some of these changes can be traced back to the December 2018 ECN+ Directive of the European Parliament. Furthermore, the draft bill also contains important changes to the German merger control regime and German cartel damages law. Last but not least, the powers and competencies of the German Federal Cartel Office (FCO) should also be substantially increased.

ECN+

In December 2018, the European Parliament adopted Directive (EU) 2019/1 “to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market,” known as the ECN+ Directive. In order to implement the ECN+ Directive in Germany, several changes were anticipated and are in fact contained in the draft bill.

In order to comply with Article 24 and following of the ECN+ Directive, there are detailed provisions in the draft bill concerning cooperation between the German FCO and competition authorities from other EU Member States. In addition to general cooperation obligations, the draft provisions cover, for example,
rules regarding the enforcement of decisions that impose fines in other EU Member States as well as information obligations.

In line with the provisions of the ECN+ Directive, the draft bill also foresees detailed provisions regarding the leniency procedure and the reduction of fines as a result of successful leniency applications.

**Cartel damages claims**

The last amendments of the German ARC and especially the implementation of the EU Damages Directive in Germany introduced several provisions that aimed to facilitate actions for damages before national courts. The draft bill follows this trend and introduces a further facilitation answering whether purchases or sales that fall within the scope of an infringement decision by the FCO are affected by an established infringement. This question has been disputed in the past, and in 2018 the German Federal Supreme Court ruled there was no prima facie evidence here in favor of claimants for damages. The lawmaker intends to close this loophole by introducing a rebuttable presumption in favor of future claimants for damages.

**Merger control**

The draft bill will make slight changes to the conditions under which notification of a transaction has to be filed with the German FCO prior to its implementation. Currently, a notification obligation arises if, among other requirements, the German turnover of at least one of the parties to the transaction exceeds €25 million and the German turnover of at least one further party to the transaction exceeds €5 million. The draft bill will increase the €5 million threshold to €10 million. According to the draft bill’s reasoning, this reduces the workload of the German FCO for merger control matters by about 20%.

In the future, the FCO will focus more on transactions raising concerns related to competition. Thus, the deadline for the FCO to adopt a decision will be extended from four to five months after the filing of a transaction with the FCO.

**Procedural powers of the FCO**

The 10th amendment of the ARC introduces a whole array of new powers for the German FCO. Those of particular note are the new rules for interim injunctions and requests for information, as well as an active cooperation obligation during dawn raids.

Following the European Commission’s new approach — as seen, for example, in the Broadcom abuse case — the draft bill intends to facilitate the conditions under which the German FCO can issue interim injunctions in ongoing competition procedures.

Furthermore, the draft bill introduces the power of the German FCO to issue extensive requests for information to companies under suspicion. In contrast with the current situation in cartel and criminal proceedings, companies will be obliged to answer such requests accurately, completely and without any misleading information, even if the answers contain incriminating information. With this approach, the draft bill follows the lead of the European Commission, limiting companies’ rights to the extent that the only action they are not obliged to take is active confession of participation in an infringement.

This cooperation obligation will apply not only to the FCO’s written requests but will also be pertinent in the context of dawn raids. The draft bill foresees an active cooperation obligation for representatives of raided companies. Under current legislation in Germany, representatives can rely to a large extent on the right to nondisclosure of incriminating information to the German FCO. Currently, a raided company and its representatives are generally only obliged to tolerate a legally permissible dawn raid, not to actively cooperate.

**Assessment of fines**

The draft bill intends to clarify the assessment and calculation of fines by the German FCO and the competent cartel courts. Thus, the draft bill introduces a nonexhaustive list of criteria to assess the appropriate level of a fine. Among other items, the list includes the scope of the infringement, the turnover associated with the infringement and the degree of organization.

**What is missing?**

The draft bill, rather surprisingly, does not contain any provisions to limit “killer acquisitions.” Following earlier public discussion, it was expected that the 10th amendment of the ARC would make it more difficult for large and/or market-leading companies to acquire small but innovative start-ups with the intent of subsuming them before they effectively start to compete with established
companies. From a legal perspective, it was hard to imagine how the German FMEE would handle this matter. It appears the FMEE has come to the correct conclusion that provisions of this kind would not fit into the established German competition regime.

Companies and lawyers were also hoping for one other missing provision. Under current law, the German FCO may publish information about ongoing cartel investigations. Considering that the presumption of innocence also applies to companies under cartel investigation, and taking into account companies’ massive loss of reputation as a result of cartel investigations, it would be justified to publish this kind of information only after the German FCO’s investigations have been concluded and, at least from the perspective of the German FCO, an infringement has been proven.

**Conclusion**

The draft bill contains even more changes and amendments to the current legislation. Nevertheless, it should be clear from this article that the draft 10th amendment of the German ARC is not merely a “digitization law,” as indicated in its title, but rather a substantive overhaul of German competition law. In the upcoming legislative process, it remains to be seen whether all the proposed changes will stand and whether even more changes to the current legislation will be introduced.

---

**Peter Giese**

Rechtsanwalt, Counsel
CMS Hasche Sigle
Stuttgart

peter.giese@cms-hs.com

www.cms-hs.com
How to organize effective protection against cyberattacks

The cyberthreat platform

By Klaus Brisch, LL.M.

Every year, cyberattacks cause considerable economic damage. According to one study, worldwide losses of approximately $600 billion were incurred in 2017 alone. In Germany, for instance, total damages to businesses were estimated at €43.4 billion through September 2018. Experts expect the risk of becoming a victim of cybercrime will continue to grow. Among other things, increasing digitalization leads to greater potential for cyberattacks, and with time and experience, attackers can enhance the technological efficiency of their cyberattacks.

Most large companies recognize the importance of cybersecurity. Small and medium-sized enterprises (SMEs), however, act quite differently. They assume they won’t be affected because other companies are much more interesting for hackers. People in positions of responsibility are unaware that hackers are sometimes not interested in the company itself, but rather in accessing data or computing capacity. This can affect SMEs at any time, causing long-term damage to their businesses. In such cases, it is likely that some alarmed customers will no longer want to transfer their sensitive data to the affected company.

Though regular installation of IT system updates and periodic password changes have become normal, it is clear that these steps alone do not provide adequate protection against cyberattacks. It is equally important to be informed immediately about any security gaps discovered in software programs, as only then can a company react accordingly. However, this has not yet been organized on a national level in Germany.

The legal situation in Germany: No nationwide warning system, IT Security Act 2.0 in its preparatory stages

Germany does have a Federal Office for Information Security (BSI), an authority whose responsibilities include such tasks as providing information on current IT threats. There is even a specific law (BSIG) that regulates communication and information paths for security-related subjects and events in information technology.

Under current legislation, however, only operators of critical infrastructure must report their IT failures to the BSI without delay. Additionally, the BSI only informs and warns certain economic players about current IT threats. This means there is no nationwide warning system.

The IT Security Act 2.0 is currently being prepared. Among other points, the current draft includes an extension of...
the obligation to report IT attacks, meaning the legally standardized exchange of information would also encompass the defense, automotive and chemical industries, the media and some others. This can certainly be seen as a step in the right direction. The current draft, however, does not address all the weaknesses in current legislation, especially from the point of view of the business community. In the future, the BSI’s flow of information — about existing security threats, for example — would remain restricted to certain segments of the economy. This would not be a comprehensive solution. In addition, not all economic players would be obliged to report cyberattacks. Furthermore, the BSI lacks networks and regulated cooperation with authorities and offices in other countries. Finally, the draft legislation contains no concept that would directly connect providers and users of security services.

What needs to be done ...

It is therefore all the more important to create an electronic B2B platform solution that brings together all parties: as many businesses as possible, security authorities and cybersecurity companies. This platform could also enable information to be exchanged among all parties in real time. The cyberthreat platform would then receive alerts directly from cybersecurity companies regarding potential threats. The users of the platform, and thus the recipients of such alerts, could be companies from the private sector as well. Unlike in the past, industry and company size would be irrelevant. Of course, government agencies should be connected to this platform as well. They could also contribute insights and relevant information regarding security issues. However, it would be important for these institutions not to have full access to company data, as that could look like government monitoring and deter some companies. It is also important to note that companies who report an attack on their IT system to the platform should be allowed to remain anonymous to avoid damage to their reputation. Nevertheless, the list of companies connected to the platform needs to be transparent for all users. A cyberthreat platform of this type would obviously have a number of legal implications. For example, the cybersecurity companies that would be involved are usually competitors, thus requiring the signing of some kind of cooperation agreement. This agreement would regulate the respective rights and obligations of the cooperating companies. It would also be necessary to establish clear conditions for the companies’ participation. These would need to include minimum requirements for IT standards within the companies as well as specific codes of conduct within the platform to protect the users’ reputation and integrity.

... and how it should be done

These kinds of platform solutions are by no means new. Comparable approaches already exist on both a national and an international level. Thus far, however, they have been limited to clearly defined groups of participants. There are two basic types of platforms. First, there is a group of Information Sharing and Analysis Centers (ISACs). These centers are more technologically oriented. One such center is the Malware Information Sharing Platform (MISP), which is cofinanced by the EU Commission. Here, participants exchange information regarding malware, imminent IT attacks and possible defensive actions. The experiences gleaned by these existing platforms would certainly be useful when developing the cyberthreat platform outlined above, facilitating a relatively quick implementation. A solution of this kind would help strengthen the industry’s competence in the realm of cybersecurity, make it easier to identify threats more quickly and enable those potentially affected to address threats in a comprehensive manner. As a result, preventative measures could effectively limit economic damage.

Klaus Brisch, LL.M.
Rechtsanwalt, Partner
Global Head of Technology
DWF
Cologne
klaus.brisch@def.law
www.dwf.law

The second type of platform focuses on networking. These platforms intend, for instance, to bring cybersecurity companies together with companies that want to protect their IT infrastructure. Germany, for example, has the Alliance for Cyber Security (ACS) — with more than 3,600 participants — and the Initiative Wirtschaftsschutz (Initiative for Economic Protection), for whom cybersecurity is only one of several elements. Comparable networking platforms also exist in some federal states.
A fundamental framework

China’s new Foreign Investment Law

By Dr. Stephan Rippert, Amy Yin and Catherine Jing

On March 15, 2019, the National People’s Congress passed the Foreign Investment Law of the People’s Republic of China (new FIL) after several rounds of public consultation. This new law, which will come into effect on January 1, 2020, constitutes a fundamental framework for foreign investment in China, covering market access, promotion, protection and administration. As of its effective date, it will supersede the existing legislation governing foreign investment: the Sino-Foreign Joint-Venture Enterprise Law, the Sino-Foreign Cooperative Enterprise Law and the Foreign-Invested Enterprise Law (together: the FIE laws).

Background

There are both internal and external factors that contributed greatly to the formulation, approval and promulgation of the new FIL.

Internal factors

The FIE laws were formulated and implemented during the early period of reform after China’s opening, between 1978 and 1988. At that time, China’s legal system was still under construction, and there was no legislation generally applicable to all kinds of companies and partnerships.

The FIE laws are products of that specific period when different types of foreign-invested enterprises were regulated by disparate rules. The FIE laws only applied to greenfield investments; legal rules regarding other foreign investment activities, such as cross-border mergers and acquisitions, were scattered across many other regulations. Despite several revisions after their promulgation, the old FIE laws have been unable to adapt to the new needs generated by China’s rapid economic development.

In the context of China’s recent process of improving its legal system, it became necessary to abolish the special administrative system only applicable to foreign-invested enterprises under the FIE laws and to adopt a unified administrative system that applies to both domestic-invested and foreign-invested...
enterprises. After repeated efforts to update the FIE laws to make them conform with China’s current legal and economic environment, the Ministry of Commerce (MOFCOM) finally unveiled in January 2015 a draft of a new foreign investment law for public comment.

External factors

On March 23, 2018, US President Donald Trump officially signed the Memorandum on the Actions by the United States Related to the Section 301 Investigation, directing the US Trade Representative to impose increased tariffs on goods from China and to place restrictions on investments in the US that are directed or facilitated by China. Soon afterward, on April 2, 2018, the MOFCOM responded by imposing tariffs on 128 products it imports from the US, marking the beginning of the China-US trade war. After several rounds of talks between China and the US intended to bring an end to the trade war, both parties temporarily agreed to work together to resolve existing problems. Among other endeavors on China’s side, a new draft foreign investment law was formulated and published for public comment during the negotiations in December 2018. This draft had been reviewed and discussed three times by the competent authorities over the course of a mere three months and was finally approved by the National People’s Congress on March 15, 2019.

This new FIL is designed to ease restrictions on foreign enterprises’ operations in China that the US had alleged were and explicitly addresses some major US concerns, including the practice of forced technology transfers, protection of intellectual property and market entry restrictions.

Developments

The new FIL comprises six chapters made up of 42 articles that cover general provisions, investment promotion, investment protection, investment administration, legal liability and supplementary provisions. The new developments it contains in comparison with the current FIL laws are listed as follows.

Market entry

During the investment entry period, foreign investors (including natural persons, business entities and other organizations from a foreign country) and their investments (investment activities directly or indirectly conducted by one or more foreign investors within China, including establishing a foreign-invested enterprise within China; acquiring stock shares, equity interests, interests in assets or other rights and interests of an enterprise established within China; investing in a new project within China; and investments in other forms) in sectors that are not on the negative list are accorded treatment that is no less favorable than that accorded to domestic investors and their investments.

The negative list is an official list of specific sectors that are subject to special administrative measures on foreign investment entry. In March 2016, the National Development and Reform Commission (NDRC) and the MOFCOM published a Draft Negative List for Market Access (Trial Version) for a pilot program conducted in four provinces and municipalities (Tianjin, Shanghai, Fujian and Guangdong), which marked the beginning of the negative list administration system. The negative list is updated annually. The current negative list is the Special Administrative Measures on Foreign Investment Entry (Negative List; 2019 Edition) published by the NDRC and the MOFCOM, which came into effect on June 30, 2019 (2019 Negative List). Compared with the previous year’s negative list, the 2019 Negative List contains far fewer sectors subject to special administrative measures (48 versus 40).

Foreign investors cannot invest in those sectors on the negative list in which foreign investment is prohibited. For instance, the 2019 Negative List provides that foreign investors are prohibited from investing in industries such as social surveys, compulsory education institutions, news agencies and movie production companies.

Foreign investors who invest in sectors on the negative list in which foreign investment is restricted must satisfy the requirements provided in the negative list. For instance, the 2019 Negative List provides that foreign investment in industries such as basic telecommunications, domestic waterway transportation and publication printing are subject to the restriction that the Chinese party is the controlling shareholder.

Foreign investment information reporting system

According to the new FIL, China is to establish a system for reporting details regarding foreign investments. Foreign investors or foreign-invested enterprises shall report details regarding investments to the authority responsible...
for commerce matters by means of the enterprise registration system and the enterprise credit information disclosure system.

Since the beginning of the negative list administration system in 2016, China has issued several relevant regulations, such as the Interim Measures for Record-Filing Administration of the Establishment and Change of Foreign-Invested Enterprises, issued by the General Office of the State Council of China in 2011 (known as Circular 6).

Circular 6 provides specific requirements regarding the scope, content, work mechanism and procedures related to the security review, while the new FIL only contains a single article stating that foreign investments that affect or might affect national security shall be subject to a security review and the decision made in accordance with the law is final.

It remains to be seen whether the detailed provisions under Circular 6 will be replaced by the new FIL’s implementation rules, which have yet to be formulated and issued.

However, it is still unclear whether the Filing Regulation will remain effective after the new FIL takes effect on January 1, 2020. And it remains to be seen whether foreign investments that are not in sectors on the negative list will still be subject to record-filing through MOFCOM’s online platform after detailed procedures regarding the foreign investment information reporting system are further specified in the new FIL’s future implementation rules.

**Foreign investment security review system**

The new FIL reiterates the requirement to establish a security review system, which was initially provided under the Notice on Establishing a Security Review System for Foreign Investors to Acquire Domestic Enterprises, issued by the General Office of the State Council of China in 2011 (known as Circular 6).

Circular 6 provides specific requirements regarding the scope, content, work mechanism and procedures related to the security review, while the new FIL only contains a single article stating that foreign investments that affect or might affect national security shall be subject to a security review and the decision made in accordance with the law is final.

**Incentives for foreign investment**

Under the new FIL, the following incentives for foreign investment are provided:

**Protection of IP rights.** IP rights of foreign investors and foreign-invested enterprises, as well as lawful rights and interests of the holders of IP rights and relevant right holders thereof, shall be protected. Any person or entity that infringes upon IP rights shall be held legally accountable. In addition, authorities and their officers shall, in accordance with law, keep confidential the commercial secrets of foreign investors and foreign-invested enterprises they obtain while performing their duties and shall not disclose or illegally provide such information to others.

**Transfer of technology.** The conditions for technological cooperation in the context of foreign investment are to be determined through “equal negotiation” by the investors in compliance with the principle of fairness. Authorities and their officers shall not force technological transfer through administrative measures.

**Local administration.** Local governments and their departments shall not, without a basis in law or regulations, add any restriction or requirement to local regulatory documents concerning foreign investment that may derogate the lawful rights and interests of foreign-invested enterprises, augment their obligations, impose conditions for market entry and/or exit or intervene in the normal production and operation activities of foreign-invested enterprises.

**Equal treatment.** Foreign-invested enterprises will be treated the same as domestic enterprises, in accordance with the law, as regards the various state policies supporting the development of enterprises, their participation in the setting of standards, the application of mandatory standards and the state procurement of products and services provided by foreign-invested enterprises within China.

**Financing.** The new FIL also confirms that foreign-invested enterprises may raise funds in China through the public offering of shares or the issuance of corporate bonds.

**Free remittance.** Foreign investors may, in accordance with law, freely remit profits, capital gains and royalties from intellectual property rights, lawfully obtained compensation and the proceeds of liquidation out of China.
Further implementation rules

The new FIL is expected to bring about significant changes in future foreign investment transactions, and its promulgation marks the beginning of a long-term reform of China's system for administering foreign investment. However, compared with the current FIE laws, the new FIL only outlines principles and contains somewhat vague provisions. Many features, such as the detailed registration, filing and reporting procedures for foreign-invested enterprises, need to be further specified by implementation rules and other ancillary regulations that have yet to be formulated and issued by the relevant authorities. Examples of efforts made so far in different regions and industries within the framework of the new FIL are enumerated below:

Free trade zone

On August 6, 2019, the State Council unveiled an overall plan (the Lingang Overall Plan) to add the new Lingang area into China (Shanghai) Pilot Free-Trade Zone. This new Lingang area, which is planned to cover 119.5 square kilometers, will double the size of the Shanghai Free-Trade Zone.

Pursuant to the Lingang Overall Plan, industries such as telecommunications, insurance, securities, science and technology, education and health will enjoy more openness in this new Lingang area.

In addition, and more importantly, all reputable foreign arbitral institutions are allowed to establish their offices in the new Lingang area. The Overall Plan suggests that these institutions, once registered, will be able to lawfully administer PRC-seated civil and commercial arbitrations in fields such as international business, maritime affairs and investment. The involved parties, both domestic and those from overseas, will be supported and provided security during the application process and enforcement of provisional measures such as preservation of property, preservation of evidence and preservation of conduct.

Just a few weeks after the promulgation of the Lingang Overall Plan, the State Council further published a series of new overall plans for free-trade zones to be established in six other provinces in China: Shandong, Jiangsu, Guangxi, Hebei, Yunnan and Heilongjiang. These six provincial overall plans, together with the aforementioned Lingang Overall Plan, all play a part in China's new efforts to further implement the general requirements provided under the new FIL.

Banking industry

On July 20, 2019, the Finance Stability and Development Committee of the State Council announced 11 new policies aimed at accelerating the further opening of the financial sector to foreign investors.

Under the new policies, limits on foreign shareholdings in securities, fund management, futures and life insurance companies in China will be lifted earlier than previously anticipated, restrictions on foreign investment in insurance companies and insurance asset management companies will be further relaxed, and foreign financial service providers and investors will have broader and more streamlined access to China's bond market.

For instance, the upper limit of 51% on foreign shareholdings in life-insurance, securities, fund-management and futures companies will be abolished in 2020, one year ahead of the previous timetable. Foreign investors will be supported in establishing wholly or partly owned currency brokerage companies in China. Furthermore, foreign investment in insurance asset management companies will be permitted to exceed 25%.

Practical notes

Although many details regarding the implementation of the new FIL are yet to be specified in future ancillary regulations, it is certain that the special corporate governance rules regulating foreign-invested enterprises provided in the current FIE laws will be replaced by general rules in the Company Law and the Partnership Enterprise Law.

For instance, this would apply for a Sino-foreign joint venture under the new FIL:

- The highest authority will be the shareholders’ meeting, rather than the board of directors as previously provided under the FIE laws.
- The company may have only one executive director, rather than at least three directors with distribution of the quota of directors be determined by the shareholders in accordance with the proportionate ratio of their capital contribution, as previously provided under the FIE laws.
- Dividends may be distributed to shareholders in a proportion other than the actual capital contributions paid by the shareholders, as long as all the shareholders agree.
- Equity interests of the company can be transferred to a third party if such
a transaction is agreed on by more than half of the other shareholders, rather than all the other shareholders as provided under the FIE laws.

As such, as soon as possible after the new FIL comes into effect, existing foreign-invested enterprises in China should consider amending their articles of association or other organizational documents to bring them into alignment with their actual circumstances in order to comply fully with the requirements under the new FIL. For example, joint venture agreements and the articles of association of Sino-foreign joint ventures should be adjusted to make the shareholders’ meeting the highest authority within the company.

Furthermore, foreign investors doing business in China are encouraged to participate when the Chinese government seeks public comment on the draft implementation rules and to keep abreast of the new developments in laws and regulations.

Amy Yin  
Partner  
Reed Smith LLP  
Shanghai

ayin@reedsmith.com

Catherine Jing  
Partner  
ReedSmith  
Shanghai

cjing@reedsmith.com

www.reedsmith.com

Roundtable im November 2019:

11. November 2019

Compliance international: Interne Untersuchungen in Zentralosteuropa – Alles, was Sie wissen müssen

Redaktionsgebäude der F.A.Z., Frankfurt am Main, 15:30–19:00 Uhr

Kooperationspartner: WOLF THEISS

Der Der Roundtable richtet sich an Unternehmensvertreter aus Rechts-, Finanz- und Compliance-abteilungen, an Vertreter der Finanzindustrie sowie an Rechtsanwälte und Unternehmensberater. Nähere Informationen zum Programm sowie das Anmeldeformular finden Sie unter www.deutscheranwaltspiegel.de/roundtable
Dr. Christian Rau, LL.M.
General Counsel
OLYMPUS EUROPA SE & CO. KG
christian.rau@olympus-europa.com
www.olympus-europa.com

Dr. Georg Rützel
SVP Legal & Governance
e-shelter services GmbH
Frankfurt am Main
georg.ruettzel@e-shelter.com
www.e-shelter.com

Matthias Schwarz
Executive Director
Talanx Reinsurance (Ireland) SE
matthias.schwarz@talanx.com
www.talanx.com

Martina Seidl
Chief Legal & Compliance Officer
Group Vice President Corporate Legal, Compliance & Data Privacy, Giesecke+Devrient GmbH, Munich
martina.seidl@gi-de.com
www.gi-de.com

Dr. Hanns Christoph Siebold
Managing Director
Morgan Stanley Bank AG
Frankfurt am Main
hanns.christoph.siebold@morganstanley.com
www.morganstanley.com

Timo Matthias Spitzer
Banco Santander
Head of Legal Corporate and Investment Banking D-A-CH, Frankfurt am Main
timo.spitzer@gruposantander.com
www.gruposantander.com

Prof. Dr. Michael Smets
Said Business School
University of Oxford
michael.smets@sbs.ox.ac.uk
www.sbs.ox.ac.uk

Dr. Klaus-Peter Weber, LL.M.
Executive General Counsel & Chief Compliance Officer
INNIO Group
Jenbach, Austria
Klaus-Peter.Weber@ge.com
www.goodyear-dunlop.com

Professor Dr. Stephan Wernicke
Chief Counsel, Director of Legal Affairs
DIHK – Deutscher Industrie- und Handelkammertag e. V.
Berlin
wernicke.stephan@dihk.de
www.dihk.de

Michael R. Winkler
Rechtsabteilung Integrity&Legal/Legal Supply&Sales
Daimler AG
Stuttgart
michael.twinkler@daimler.com
www.daimler.com

Morgan Stanley

DAIMLER
German American Chamber of Commerce, Inc.
Suzanne Gellert, LL.M., Attorney at Law
Director, Legal Department & Business Development Consulting
80 Pine Street, Floor 24 | New York, NY 10005
Telephone: +1 (212) 994 8846
sgellert@gaccny.com
www.gaccny.com

German American Chamber of Commerce of the Midwest
Jayne Riemer-Chisty
Director, Membership and Chamber Development
321 North Clark Street, Suite 1124 | Chicago, Illinois 60610
Telephone: +1 (312) 494 2153
riemer-chisty@gaccmidwest.org
www.gaccmidwest.org

German American Chamber of Commerce of the Midwest
Jayne Riemer-Chisty
Director, Membership and Chamber Development
321 North Clark Street, Suite 1124 | Chicago, Illinois 60610
Telephone: +1 (312) 494 2153
riemer-chisty@gaccmidwest.org
www.gaccmidwest.org

German Brazilian Chamber of Industry and Commerce
Dr. Claudia Bärmann Bernard
Head of Legal Department
Rua Verbo Divino, 1488, 04719-904 São Paulo - SP, Brazil
Telephone: +55 11 5187 5216
juridico@ahkbrasil.com
www.ahkbrasil.com

Canadian Chamber of Commerce and Industry Inc.
Alexandre Ratiu, Mag. iur.
Manager Business Support Canada
480 University Avenue, Suite 1500, Toronto, ON M5G 1V2, Canada
Telephone: +1 (416) 598-7124
alexandre.ratiu@gccchamber.ca
www.gccchamber.ca

German-Dutch Chamber of Commerce
Ulrike Tudyk
Head of Legal Department
Nassauplein 30, NL – 2585 EC Den Haag, Netherlands
Telephone: +31 (0)70 314 14 57
u.tudyk@dnhk.org
www.dnhk.org

German-French Chamber of Industry and Commerce
RA Joachim Schütz, MBA
Head of Legal and Tax Department
18 rue Balard, F-75015 Paris, France
Telephone: +33 (0) 405 83 35 34
jschule@francoallemand.com
www.francoallemand.com

German Industry and Commerce Greater China
Wolfgang Ehmann
Executive Director
3601 Tower One, Lippo Centre, 89 Queensway, Hong Kong
Telephone: +852 2526 5481
ehmann.wolfgang@hongkong.ahk.de
www.china.ahk.de / www.hongkong.ahk.de

German Chamber of Commerce and Industry in Japan
Patrick Bessler, Director, Editor in Chief, JAPANMARKT
Sanbancho KS Bldg., 55, 2-4 Sanbancho, Chiyoda-ku 102-0075, Tokyo, Japan
Telephone: +81 (0) 3 2383 7962
p.bessler@dhjk.or.jp
www.dhjk.or.jp

German Emirati Joint Council for Industry & Commerce
Katharina Didszuhn
Head of Dubai Office, Head of PR & Communications
Business Village, Building B, Office 618, Port Saeed, Deira, P.O. Box 7480, Dubai, UAE
Telephone: +971 (0) 4 4470100
katharina.didszuhn@ahkuae.com
www.ahkuae.com

Indo-German Chamber of Commerce
Sabina Pandey, Head – Legal Department, Indo-German Chamber of Commerce,
36, Gurusaday Road, Kolkata 700 019, India
Telephone: +91 33 2283 7962
s.pandey@indo-german.com
legaldepartment.mumbai@indo-german.com
www.indo-german.com

German Chamber of Commerce and Industry in Japan
Patrick Bessler, Director, Editor in Chief, JAPANMARKT
Sanbancho KS Bldg., 55, 2-4 Sanbancho, Chiyoda-ku 102-0075, Tokyo, Japan
Telephone: +81 (0) 3 2383 7962
p.bessler@dhjk.or.jp
www.dhjk.or.jp

Canadian Chamber of Commerce and Industry Inc.
Alexandre Ratiu, Mag. iur.
Manager Business Support Canada
480 University Avenue, Suite 1500, Toronto, ON M5G 1V2, Canada
Telephone: +1 (416) 598-7124
alexandre.ratiu@gccchamber.ca
www.gccchamber.ca

German Chamber of Commerce and Industry in Japan
Patrick Bessler, Director, Editor in Chief, JAPANMARKT
Sanbancho KS Bldg., 55, 2-4 Sanbancho, Chiyoda-ku 102-0075, Tokyo, Japan
Telephone: +81 (0) 3 2383 7962
p.bessler@dhjk.or.jp
www.dhjk.or.jp

German Chamber of Commerce and Industry in Japan
Patrick Bessler, Director, Editor in Chief, JAPANMARKT
Sanbancho KS Bldg., 55, 2-4 Sanbancho, Chiyoda-ku 102-0075, Tokyo, Japan
Telephone: +81 (0) 3 2383 7962
p.bessler@dhjk.or.jp
www.dhjk.or.jp