In this issue:

3. The end of investment protection within the European Union?

9. Germany’s lonesome actions against internet giants

12. Cyber attacks have increased

15. Wind of Change
Dear Readers,

Dr. Daisy Walzel reports on the upcoming German Act against Restraints on Competition. This new law intends to restrict the bundling of market power following from an ever increasing digitization. One or two people in Silicon Valley might want to take a closer look at it.

GDPR – it is getting serious. Dr. Fiona Savary deals with the handling of the enforcement rules of the EU data protection authorities (DPA). One development is noticeable: Fines seem to be rising for companies who do not comply with the GDPR concept.

Do you feel the same way? In these demanding times every positive story is more than welcome. Here is one: Maria Varsellona describes in our ACC column her career path, which so far has led her to the position of General Counsel at ABB.

Sincerely yours,

Thomas Wegerich
The end of investment protection within the European Union?

The Termination Agreement of 5 May 2020: what it entails for investors and how (existing) intra-EU investments can be protected in the future

By Arne Fuchs, LL.M. (GWU), and Pauline Walde

Although questionable for many reasons, the Termination Agreement marks a historic turning point for the protection of cross-border investments within the EU.

The saying “you never know what you’ve got till it’s gone” is bound to hold true for many European investors whose investments in other Member States may become threatened by measures of the host state that are incompatible with rule of law standards. Maybe this sentiment will eventually also find its way into the departments of the German Federal Government responsible for foreign trade and investment. The economic success of countless German companies – and thus many jobs in Germany – depends on business ventures in other Member States. If foreign investments in these countries are taken or damaged without adequate compensation, this can have severe economic repercussions in Germany.

Until recently, foreign investments within the European Union (“EU”) were protected by almost 200 intra-EU bilateral investment treaties (“BITs”). Germany was a party to 13 of these intra-EU BITs. These treaties ensured certain minimum standards of treatment for foreign investments that we consider essential in a rule of law state.

For example, this include the obligation to pay compensation if the host state expropriates investments for the public good, the obligation to treat foreign investors and their investments fairly and equitably and to grant them full protection and security. BITs also prohibit discriminatory treatment against foreign investors. To ensure that the rights guaranteed in these BITs could be enforced in a
neutral forum with an independent and impartial decision maker, the majority of these treaties provided for dispute resolution clauses, offering investors the possibility to settle their disputes with the host state through international arbitration.

This legal framework has now changed dramatically. By signing the Agreement for the Termination of Bilateral Investment Treaties between the Member States of the European Union of 5 May 2020 ("Termination Agreement"), 23 Member States\(^1\) terminated their intra-EU BITs under the leadership of the European Commission ("Commission").\(^2\) In total, this concerns 132 BITs. Only the United Kingdom, Finland, Ireland,\(^3\) Austria and Sweden withstood pressure from the Commission and refused to sign the Termination Agreement.

From the Achmea Judgement to the Termination Agreement

The Termination Agreement was signed approximately two years after the Court of Justice of the European Union ("CJEU") rendered its judgement in the case Slovak Republic v. Achmea BV (C-284/16) of 6 March 2018 ("Achmea Judgement"). In this judgement, the CJEU ruled that a provision "such as Article 8" of the Dutch-Slovak BIT is incompatible with certain provisions of the Treaty on the Functioning of the European Union ("TFEU"). In its very brief reasoning, the CJEU heavily relied on the fact that under Article 8 of the Dutch-Slovak BIT, the arbitral tribunal must not only apply the relevant provisions of the BIT but also a Member State's domestic law. The CJEU found that this could potentially include provisions of EU law. It also found that arbitral tribunals lack the power to request preliminary rulings from the ECJ and therefore concluded that the full effectiveness of EU law was not guaranteed. The CJEU also argued that the offer to settle disputes with a foreign investor through arbitration constitutes a violation of the principle of mutual trust between the Member States.

The Achmea Judgement followed a long-running campaign by the Commission against intra-EU BITs. For years, this campaign was unsuccessful since the Commission’s arguments had repeatedly been rejected in arbitrations in which the Commission had intervened as amicus curiae. However, backed by the Achmea Judgement, the Commission gained the upper hand. It swiftly proclaimed that the CJEU had allegedly confirmed the Commission’s view and that all intra-EU BITs – even the ones which do not contain a provision “such as Article 8 of the BIT” on the application of domestic law (which is the majority of the relevant BITs) – violate EU law. According to the Commission, all offers to arbitrate contained in intra-EU BITs are therefore invalid and the respective treaties to be terminated by the Member States. The Commission repeatedly threatened Member States that non-compliance with its demands would lead to infringement proceedings under Article 258 TFEU.

A number of Member States (which found themselves in the role of Respondents in investment arbitrations) had already adopted the Commission’s views voluntarily in order to seek the dismissal of the claims pending against them for lack of jurisdiction. One year after the Achmea Judgement was rendered, the Commission was able to persuade the majority of the other Member States to issue a declaration on the legal consequences of the Achmea Judgment undertaking to terminate intra-EU BITs. The Termination Agreement is the last step in this process, implementing the declaration of the Member States.

Notable: Termination of so-called Sunset Clauses

It is already astonishing that the Member States – under the leadership of the Commission – would turn against public international law treaties which aim to guarantee the most fundamental rule of law principles and promote the peaceful, depoliticized resolution of international disputes. It is even more surprising that in doing so, they would not even safeguard provisions which were specifically designed to ensure a minimum level of legal certainty in case of the termination of these treaties.

In principle, BITs can be terminated with effect for the future after a certain minimum term of validity as prescribed in the individual treaty has expired. However, because foreign investments often involve high up-front investment costs that can only be recovered over a long amortization period, most BITs contain so-called ‘sunset clauses’. These provisions guarantee that investments made prior to the termination of a treaty are still protected for a specified period of time after the termination, usually 10-20 years.
The Termination Agreement not only terminates the intra-EU BITs in question, it also specifically targets and terminates their respective sunset clauses. That is, the Termination Agreement not only changes the framework for new investments, it also changes the rules of the game for investors who have already committed (substantial) funds in reliance on the minimum standards of treatment guaranteed by the BITs. This can hardly be reconciled with rule of law principles such as non-retroactivity, legal security and the protection of legitimate expectations.

Impact on (pending) arbitrations

In principle, the Termination Agreement stipulates that the host state's consent to arbitration expressed in the relevant BIT is invalid and cannot serve as legal basis for arbitrations. As explained, it is generally possible to create such legal effect for the future (subject to the sunset clauses). However, the Termination Agreement (once again) goes beyond this “normal” ex nunc regulation.

The Termination Agreement distinguishes between three categories of arbitrations: “new”, “pending”, and “concluded”. This classification is not undertaken in relation to the effective date of the Termination Agreement. Instead, it uses a date that is more than two years in the past: 6 March 2018, i.e. the date of the Achmea Judgement.

Only arbitration proceedings “concluded” prior to 6 March 2018 are not affected by the Termination Agreement. Moreover, for an arbitration to qualify as “concluded” within the meaning of the Termination Agreement, it is not sufficient that a final award had been rendered by this date. Rather, any attempt by the respondent state to challenge the award must also have failed and enforcement measures must have been “duly executed”.

Since setting aside and annulment proceedings often extend over years, the desired legal effect of the Termination Agreement is shifted back in time even further. Moreover, states that have not complied with an arbitral award and resisted enforcement in violation of their public international law (and contractual obligations) are rewarded and put in a privileged position in comparison to states that have diligently complied with the awards.

“Pending” proceedings are defined as all arbitrations that were initiated before 6 March 2018 but have not yet been concluded in the (very narrow) sense of the Termination Agreement. For such proceedings, the Termination Agreement provides for so-called “transitional measures” according to which investors can chose to either conduct a non-binding “structured dialogue” with the host state in an attempt to reach a voluntary settlement or to pursue their claims before the national courts of the host state.

Both options are less than satisfactory for the foreign investors.

First, the Termination Agreement does not clarify how the dialog should be “structured” and what happens if a settlement cannot be reached during this process. It seems that the investor would then be left empty-handed. Second, in order to be “allowed” to pursue its claim before the national courts, an investor must irrevocably waive all rights and claims under the BIT and renounce the execution of any arbitral awards already issued but not yet executed or enforced. The investor must then start from square one before the national court.

It seems obvious that this is neither a fair nor an economically viable alternative for an investor who has already invested a lot of time, money, and resources in the arbitration. Moreover, it bears recalling that the Commission itself has already taken action against both Poland and Hungary because it deemed the independence of the judiciary and the rule of law in these countries to be at risk. Indeed, the Commission yet again initiated infringement proceedings against Poland to safeguard the independence of Polish judges on 29 April 2020 – a few days before the signing of the Termination Agreement. The Global Competitiveness Report 2019 rated Croatia’s judicial independence at 2.4, Poland at 2.7 and Hungary at 3 out of 7 points. Finally, all arbitrations initiated on or after 6 March 2018 are qualified as “new” proceedings. For these arbitrations, not even the transitional measures are available. This means that investors who may have initiated an arbi-
istration two years before the Termination Agreement with regard to investments made long before that are left without any recourse under the new legal framework.

With concerns over non-compliance with rule of law principles, the few states that decided not to sign the Termination Agreement did so to protect their investors engaged in pending arbitrations against other Member States from this unfortunate fate. For instance, several Austrian banks are currently pursuing ICSID arbitrations against Croatia under the Croatian-Austrian BIT. Unfortunately, the German Federal Government has not prioritized the interests of its nationals investing in other Member States. This may be due to the fact that the Federal Republic of Germany is currently being sued by the Swedish state-owned company Vattenfall AB for damages allegedly incurred in connection with the state’s decision to accelerate the phase-out of nuclear energy for the commercial generation of electricity in the aftermath of the Fukushima nuclear accident.17

The consequences of the Termination Agreement and what investors must now consider

In light of the intended effects of the Termination Agreement, it is unclear how arbitral tribunals will deal with this treaty in the future. Under public international law, they can (and must) make an independent assessment of the relevant legal issues. They may therefore reach different conclusions than those intended by the Commission and the Member States.

However, two points can be made with certainty.

First, the Termination Agreement will be front and center of many coming procedural battles in arbitrations initiated under the relevant intra-EU BITs. This will inevitably create significant additional costs for the investors.

Second, the Termination Agreement and the manner in which the termination is executed therein, demonstrates that there is absolute political determination to prevent payment of damages by Member States in the context of intra-EU investment arbitrations. Therefore, even if an arbitral tribunal were to reject the line of argument of the Termination Agreement and an investor were to prevail in an intra-EU arbitration, the financial value and enforcement prospects of such an arbitral award is uncertain at best.

The unsuccessful host state will certainly not comply with the award voluntarily. Enforcement measures in other Member States that signed the Termination Agreement will also not have any prospect of success. This leaves enforcement efforts outside of the EU. Even if the investor manages to find (sufficient) assets that are not subject to state immunity, considerable political resistance is still to be expected.18

Importantly, this applies not only to the intra-EU BITs in question. The Commission and the Member States have already announced that they hold the same legal view with regard to the Energy Charter Treaty under which many arbitrations, including by German investors, are currently pending and pledged to address this matter next.

The fact that the Commission initiated infringement proceedings against the United Kingdom because it refused to sign the Termination Agreement also demonstrates that the Commission’s approach is driven more by ideology than by the application of law. The Termination Agreement was signed on 5 May 2020 – several months after Brexit on 31 January 2020.

Against this background, German investors who have already invested in other Member States or intend to make such investments in the future must be particularly careful. New investments should be structured through a subsidiary in a non-Member State to ensure that they can benefit from investment treaties to protect against political risks. Often, investors can also restructure existing investments as long as a dispute with the host state has not yet arisen. Following Brexit, the United Kingdom could become an attractive jurisdiction for such purposes. To determine the best possible options, investors should consult an experienced investment arbitration specialist who can usually provide guidance at minimal costs.

Conclusion

Although questionable for many reasons, the Termination Agreement marks a historic turning point for the protection of cross-border investments within the EU. This is particularly unfortunate in view of the current surge of nationalism and populism. Effective means to safeguard the rule of law and protect against political risks are now needed more than ever. With its prominent lack of enforcement mechanisms for individuals, the EU legal
framework alone does not provide such means. It is therefore particularly regrettable that the Commission has not taken any effective steps to close the gaps for the protection of foreign investments that result from the Termination Agreement. Although the Commission’s fight against intra-EU BITs has been ongoing for many years, it has only launched public consultations on this issue in May 2020. So even if there were political will to actually protect intra-EU investments at the level of the EU law, experience shows that concrete measures would still be years away. For the time being, the only way for investors to protect their investments in the event of a crisis is to structure them via third countries with strong investment treaties in place.

1 These 23 Member States are the following: Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia and Spain.

2 See Article 2(1) of the Termination Agreement as well as its Annex A. The Termination Agreement entered into force on 29 August 2020.

3 However, it needs to be noted that Ireland has already terminated its only intra-EU BIT with the Czech Republic in 2011. The protective mechanism of the so-called sunset clause ends in the year 2021.


7 See Article 2(2) and 3 of the Termination Agreement. There is also a provision concerning BITs terminated before the Termination Agreement in respect of which sunset clauses have not been challenged so far. See Article 3 of the Termination Agreement.

8 See Article 1(6) of the Termination Agreement.

9 See Article 1(5) of the Termination Agreement.

10 See Article 1(4) of the Termination Agreement.

11 See Article 6 of the Termination Agreement. A “concluded arbitration proceeding” is defined in Article 1(4) of the Termination Agreement as “any Arbitration Proceeding which ended with a settlement agreement or with a final award issued prior to 6 March 2018 where: (a) the award was duly executed prior to 6 March 2018, even where a related claim for legal costs has not been executed or enforced, and no challenge, review, set-aside, annulment, enforcement, revision or other similar proceedings in relation to such final award was pending on 6 March 2018, or (b) the award was set aside or annulled before the date of entry into force of this Agreement”.

12 See Article 8-10 of the Termination Agreement.


16 See Article 1(6) of the Termination Agreement.

17 Even though this arbitration was brought under the Energy Charter Treaty (“ECT”), the political considerations likewise apply as the Commission – and a number of Member States – argue that the Achmea Judgment also applies to the ECT.

18 For example, the Commission actively tried to prevent the enforcement of the award in Micula v Romania I (ICSID Case No. ARB/05/20) and participated in the enforcement proceedings in US-courts as amicus curiae. This was long before the Termination Agreement.
Setting up a GmbH

New co-publication between Globe Law and Business and German Law Publishers

For full details go to www.globelawandbusiness.com/GMBH
Germany's lonesome actions against internet giants

A glimpse at the envisaged reform to the German Act Against Restraints on Competition and recent case law

By Dr. Daisy Walzel, LL.M. (oec.)

Germany is hitting the headlines with increasing regularity for its ambitious fight against tech giants’ presumed market power. Not only has the German Federal Cartel Office (FCO) intervened against Facebook’s practices of combining user data from different sources, a decision which the Federal Court of Justice (Bundesgerichtshof) recently upheld. A few weeks ago, the German government also submitted to the German parliament a draft 10th amendment to the German Act Against Restraints on Competition (Gesetz gegen Wettbewerbsbeschränkungen, ARC). The intended changes aim at tackling the bundling of market power associated with increasing digitization. In the foreground is a considerable expansion of the rules on the prohibition of abuses of dominance. The Act will also implement the so-called ECN+ Directive, which aims at strengthening the national competition authorities in applying EU competition rules (Art. 101, 102 TFEU) and is due to enter into force in early February 2021.

Both the FCO’s stance against Facebook as well as the envisaged changes to German law offer novel approaches against tech giants’ conduct.

Pioneering versus harmonizing

As much as one may understand the need to take such action, one may be startled by how these German go-it-alone fits into the harmonised EU antitrust regime. How-
ever, unlike in cartel matters involving bilateral agreements and concerted practices, member states are not precluded from adopting or applying stricter national laws which sanction unilateral conduct engaged in by undertakings (Art. 3 (2) Reg. 1/2003). In other words, when it comes to the (unilateral) abuse of market dominance, EU law only sets a minimum standard and member states may adopt and apply stricter rules. The envisaged reform strikes exactly into this flank. As a result, it is very well possible that large tech companies and their counterparts (customers and competitors) may in the future face a patchwork of varying legal standards throughout different EU member states. In any event, it will be interesting to observe whether the special routes chosen by Germany will nevertheless have (factual) persuasive authority on the application of the EU rules by national competition authorities and courts as well as by the EU Commission.

Key elements of the envisaged legislative reform

Background

German law in principle distinguishes between companies enjoying "absolute" market dominance (Art. 19 ARC) and companies enjoying "relative" dominance because others are dependent on them (Art. 20 ARC). In the latter scenarios, the "stronger" company does not reach the threshold of absolute market dominance. The legal boundaries applicable to those companies are less strict than those which apply to companies which enjoy absolute market power.

The German government identified the increasing power of a small number of large digital corporations (such as Google, Amazon, Facebook etc.) as an issue which cannot be tackled properly by the current legal provisions. Such companies are presumed to occupy decisive channels to customers ("gatekeepers") and to possess a rich, constantly growing data store. The latter could be used to solidify existing market positions or to expand into other areas. Therefore, the crux of the envisaged reform centres around gaining a better "legal grip" on these new forms of power and the corresponding misconduct. The envisaged changes relate to issues of platform power (so-called "intermediation power") and access to data.

Criteria for absolute market power

To determine whether a company enjoys "absolute" market dominance, German law not only looks at market shares (e.g. > 40 %), but also at a set of other criteria (Art. 18 ARC). These criteria will now be adapted further: For example, access to competitively relevant data will be introduced as a new criterion for assessing an undertaking’s market position across the entire digital economy. The same applies to so-called intermediation power, typically enjoyed by large platforms (as a special form of intermediary power in procurement and sales markets for third parties). Intermediation power, too, will form a new and distinct criterion for determining market dominance.

Data as an "essential facility"

Pursuant to the so-called essential-facility doctrine, a market-dominant undertaking must provide another undertaking with access to its own infrastructure at reasonable conditions if the claimant cannot otherwise compete with it (Art. 19 (4) ARC). The draft extends this provision to digital business models where, for example, access to platforms or interfaces as well as to data can play a pivotal role. In other words, in future, mavericks may have a legal means to tap into the data pools harvested by tech giants. While requests for data access so far may not seem like a particularly pressing topic, they may become crucial in creating a level-playing field with tech giants in those areas where large data pools will pose a significant competitive advantage in the future. However, the exact legal and "technical" framework applicable under the new law for demanding and granting such access (maybe even on a permanent basis) remains somewhat blurry.

New possibility of intervention
(Section 19a GWB-E)

Finally, the draft also introduces a new type of supervisory power which shall enable the FCO to prohibit certain types of conduct by undertakings enjoying a "significant overarching importance to the market" ("überragende marktübergreifende Bedeutung für den Wettbewerb") without (as hitherto) requiring proof of market dominance or of an abuse of such dominance. This will particularly concern large digital platforms whose activities aim...
at linking the different sides of multilateral markets and profit from direct and indirect network effects.

The term "network effect" describes a phenomenon whereby increased numbers of participants improve the value of a good or service e.g. an increased number of users in a social network increases its value for other users (direct network effect) and for advertisers (indirect network effect).

However, any prohibition decision by the FCO must be preceded by an order establishing the existence of an undertaking's "significant overarching importance to the market". Only based on such an order may the FCO intervene against various types of behaviour by the undertakings in question, including self-preferencing and certain forms of obstruction e.g. related to certain forms of data usage, the interoperability of products or services or to performance assessment. It is at least debatable whether this complex procedure will not end up creating more bureaucratic obstacles than tangible benefits for competition.

Practical tips

Is your company dependent on another company (e.g. in the technology sector) and does the other company practise the following behaviour?

• It charges "excessive" prices for a mediation service;

• It refuses access to data, interfaces or platforms required for your business operations or renders access exceedingly difficult;

• It uses business practices that you may otherwise find unfair or disruptive.

Check whether you can make the change in the law work for your company!

Competition law and the law on data protection

A topic not touched on by the draft is the role that the rules on data protection should play in competition matters. Noticeably, the FCO based its decision against Facebook primarily on an alleged breach of the GDPR, which (in the FCO's reading) amounted to a breach of the German prohibition on the abuse of market dominance. It argued in essence that users could not validly and voluntarily consent to Facebook's terms, whereby users are only able to use the network under the precondition that Facebook can also collect user data outside the Facebook website on the internet or on smartphone apps and link these data to the user's Facebook account. The Federal Court ultimately upheld the FCO's decision.

So far, EU competition law has been agnostic to the question of whether infringements of data protection law (or of any other statutory provisions for that purpose) may constitute an infringement of antitrust law. However, data protection law is a genuinely European topic and access to large data pools is turning into a more and more decisive source of market power. It would therefore seem necessary for the EU Commission to clarify this topic in the future.
Cyber attacks have increased

GDPR Enforcement – Key Trends and Takeaways

By Dr. Fiona Savary

The General Data Protection Regulation (“GDPR”) first created headlines when businesses were still scrambling to update their data protection concepts ahead of the GDPR coming into force on 25 May 2018. Initially, the EU data protection authorities (“DPAs”) were more lenient and tended towards giving advice rather than handing down fines. However, both the number of fines and their amount have increased significantly over time.

Recently, a number of particularly high fines have once again garnered a lot of media attention. But what kind of violations attract such heavy penalties and which business sectors are under intense scrutiny by the DPAs? To look into the DPAs’ fining activities in more detail and provide answers to these questions, the GDPR Enforcement Tracker Report analyses the fines based, inter alia, on the type of violation, the country and the relevant business sector. The analysis is based on the publicly available data on fines that CMS collects and compiles at hier.
Most Common Legal Basis for Fines and Most Affected Sectors

The analysis revealed two predominant groups of GDPR violations which led to both the highest number and the largest amounts of fines: insufficient legal basis for data processing (Articles 5 and 6 GDPR) and insufficient technical and organisational measures to ensure information security (Article 32 GDPR). This holds true for all business sectors.

A recent example for a fine based on insufficient data security is the GBP 20 million penalty imposed on British Airways by the UK's DPA. The ICO (Information Commissioner’s Office) fined British Airways for failure to take adequate IT security measures to prevent a cyber attack affecting more than 400,000 customers.

Regarding business sectors, DPAs appear to focus a lot on businesses in the media, telecoms and broadcasting sector, while also imposing high fines on companies operating in the transportation and energy sectors.

Ensuring a Sufficient Legal Basis

To avoid being fined for not having a sufficient legal basis for data processing, companies should ensure that the data they collect and use is actually necessary, e.g. for the fulfilment of a contract. Additionally, they should ascertain that any declarations of consent are valid for the respective purpose, e.g. for marketing communications. In case that companies want to rely on their legitimate interests as a legal basis, they need to thoroughly assess whether the company’s interests outweigh the individual’s interest.

Bolstering Data Security

The risk of being fined for lacking data security can be significantly reduced by introducing and maintaining state-of-the-art technical and organisational security measures. Primarily, this includes the implementation of industry standards such as ISO/IEC 27001. However, this is not a “one-off exercise” as data security measures should be reviewed and adjusted regularly.

When imposing a fine, DPAs have to consider multiple different factors in each individual case.

In addition, businesses should hold training sessions on GDPR requirements for their employees. Regarding their products and services as well as internal business processes, companies should take into account the “privacy by design” and “privacy by default” principles.

This means that companies should consider data protection aspects whenever possible.

Dealing with a Data Breach

Unfortunately, even a wide range of data security measures may not entirely prevent data breaches. In many cases where data breaches occur, companies are legally required to report it to regulators and/or affected individuals. It is critical for businesses to react promptly and take immediate action. Otherwise, they could be faced with tougher fines and greater reputational damage.

However, many companies fail to act quickly enough once a data breach has been discovered. This is underlined by an unnecessarily high number of GDPR fines issued due to non-compliance with breach notification obligations. In order to equip businesses with ready-to-access guidance on how to deal with a data breach, CMS developed the Breach Assistant app. The Breach Assistant not only guides users through interactive data breach response checklists, but also provides detailed sector-specific guidance. Furthermore, the Breach Assistant covers more than 70 jurisdictions, thus reducing complexity for international businesses.

Factors Determining the Amounts of Fines

When imposing a fine, DPAs have to consider multiple different factors in each individual case. These factors have also been reflected in the DPAs’ justifications collected at the enforcement tracker. By way of example, the ICO explained in its statement regarding the British Airways fine that, in particular, the large amount of affected customers as well as the fact that the cyber attack went on unnoticed
for several months until it was brought to British Airways’ attention by a third part led to the harsh fine. Additionally, British Airways should have used numerous measures such as multi-factor authentication to reduce or prevent the risk of such an attack, none of which would have entailed excessive cost or technical barriers.

Other factors include the nature of the data involved as well as whether the infringement was intentional or caused by negligence. In October 2020 for instance, the Hamburg DPA imposed the highest fine to date in Germany in the amount of EUR 35 million on H&M, partially due to the particularly sensitive data involved which included employees’ health data and religious beliefs, but also because the data was collected intentionally by the management and used to make employment decisions.

Mitigating Factors

However, there are also various options at companies’ disposal which may noticeably reduce the amount of a fine. First of all, it can be advantageous to promptly notify the relevant DPAs and other regulatory authorities rather than waiting until a third party brings the infringement to the authorities’ attention. Additionally, collaborating closely with the DPAs and taking their advice on measures to implement may pay off significantly. Besides, DPAs might also view it favourably if a company apologizes to the affected individuals and offers them adequate compensation as it was highlighted in the Hamburg DPA’s decision against H&M.

Although a business’ economic situation in general and its annual turnover are certainly also taken into account by the DPAs, businesses should not expect too much leniency from the DPAs’ due to the economic impact of COVID-19 as recent fines have shown.

Main Takeaways

The DPAs’ GDPR enforcement activities show that businesses should particularly pay attention to relying on sufficient legal bases for all processing operations, but also to bolster their data security measures. Additionally, they should keep in mind that data protection concepts are not something to put away somewhere to collect dust, but instead concepts must be tested and overhauled regularly.

Furthermore, companies should be mindful of potential data breaches and be prepared to immediately take the necessary actions. A breach caused by a cyber attack has become even more likely, as cyber attacks have increased through the COVID-19 pandemic.
Wind of Change

Corporate Investigations weathering COVID-19 and AI

Guest contribution by Benjamin Kunde, CFE

The global pandemic has not only impacted the lives of billions around the world, but it has also forced entire corporate sectors into uncharted territories. Company lawyers, managing directors and attorneys often rely on private investigators to assist with gathering intelligence, investigating facts, and analysing forensic data. In the complex world of corporate investigations, the impact of the pandemic comes when we are already fighting other serious threats, and this unexpected global pandemic may just spell the end of traditional corporate investigations … or will it?

In recent years, Artificial intelligence (AI) has been driving private investigation firms into unknown waters, but the ongoing disruption of the global pandemic has forced firms to rely on machines more than ever.

Benjamin Kunde, CFE
Interfor International LLC,
New York
Executive Vice President, Investigations
Ben.Kunde@interforinc.com
www.interforinc.com
Technical innovations are making their mark on business operations who are seeing technical advancement at unprecedented levels. Because of this, they are fighting to future proof themselves while they still can.

The corporate intelligence industry has to show that it can deal with the threat of cyber-attacks and uncontrollable risks of the current global pandemic, all while still being able to advise on the fraud detection, prevention, and mitigation.

Those who advise in-house and external lawyers on behalf of clients work in a world of industrial espionage and they search for hidden assets in faraway places. Yet, what might appear like a Bond film has turned into a multi-billion-dollar business at the forefront of cybersecurity, compliance, and detection across all sectors.

The key to survival through this changing landscape will be the ability to balance new AI technology with human interaction. One reason for this emanates from the generally accepted notion that all algorithms have limits and despite their ability to cast wide nets in a relatively short period of time, with such high stakes involved it is reconciliation with human intelligence corporate industries will no doubt have to rely on.

Other industries will find that the use of AI comes with its own limitations. It is self-evident that AI shines when processing repetitive data, but it needs to be complemented by the unreplaceable human instinct of ‘gut feeling’ that is just as effective a weapon in an industry where there are many unique data points in play.

There are fears that AI forces the industry to rely on technology that may only be a stop-gap but equally could become a tradable commodity.

The most realistic answer is that AI seems to be a useful tool for the industry, but it needs to be led by the hand into the future by the instincts and abilities of human intelligence.

Three themes encapsulate the influence of AI, machine learning and other technologies for the legal and corporate intelligence communities: First, a growing fear of cyber threats as fraud becomes increasingly online and borderless. Second, cost-effective reliability, even under the global circumstances that we are currently facing, particularly for multi-national corporations. And lastly, a desire for increased AI fraud detection and background checks.

In an ever-changing global landscape, how often investigative experts will be forced to adapt and how they adapt to meet these growing demands remains to be seen.

The Rise of AI

The next decade of investigative advisories, maybe more, has been set by global events and the rise of AI may well help intelligence consultants ready themselves for a new trend in mitigating and preventing corporate fraud.

The key to survival through this changing landscape will be the ability to balance new AI technology with human interaction. One reason for this emanates from the generally accepted notion that all algorithms have limits and despite their ability to cast wide nets in a relatively short period of time, with such high stakes involved it is reconciliation with human intelligence corporate industries will no doubt have to rely on.

Other industries will find that the use of AI comes with its own limitations. It is self-evident that AI shines when processing repetitive data, but it needs to be complemented by the unreplaceable human instinct of ‘gut feeling’ that is just as effective a weapon in an industry where there are many unique data points in play.

There are fears that AI forces the industry to rely on technology that may only be a stop-gap but equally could become a tradable commodity.

The most realistic answer is that AI seems to be a useful tool for the industry, but it needs to be led by the hand into the future by the instincts and abilities of human intelligence.

Three themes encapsulate the influence of AI, machine learning and other technologies for the legal and corporate intelligence communities: First, a growing fear of cyber threats as fraud becomes increasingly online and borderless. Second, cost-effective reliability, even under the global circumstances that we are currently facing, particularly for multi-national corporations. And lastly, a desire for increased AI fraud detection and background checks.

AI: advantages and limitations

AI’s biggest advantage is its ability to analyse mass amounts of data and reveal trends in a fraction of the time it would take a human to do the same job. This is why many, if not all, major companies have invested in some form of machine learning and automated technology.

Even start-ups can offer comprehensive background checking and document verification with relative ease and reliability.

The current pandemic makes such technological advances more appealing, as they are unaffected by travel restrictions and other social distancing measures brought in to
mitigate the spread of the virus. AI-driven investigative products become much more attractive, offering as they do uninterrupted services in fraud detection, internal investigations and more.

AI can not only filter and analyse data quickly but it can monitor data from accounts to social media and public source activity that can automatically alert users, but also recognise patterns and even make predictions of potentially fraudulent activities.

But it’s not all positive.

Cyber defences can be used to great effect to detect and prevent cyber fraud, but criminals are always adapting to new technologies and inventing new and sophisticated ways of scamming people and businesses. This can be done using AI to imitate human activity, making it difficult for counter AI to detect the algorithms.

If AI cannot make these nuanced distinctions, a fraudster pretending to be someone else may also only be stopped by human intervention.

Other limitations to AI include cost, data accuracy, and data access. Each investigation can be unique and require new algorithms to be developed. Therefore, single-use AI detection does not currently represent a cost-effective return.

Perhaps the most severe limitation of AI is that it leads humans and agencies into reliance on the technology and this false sense of security can be exploited by criminals and fraudsters.

While there are no doubts about the usefulness of AI, it should always be treated with an air of caution; when AI has cast its wide net, it is in the murky waters it cannot reach that the true criminals and fraudsters lie waiting to pounce on complacent companies.

Are the old ways still relevant?

AI cannot recreate the creativity, curiosity, and instinct of human investigation. It is bound by the walls of public record and database access and it is perhaps poignant to remember that.

AI can perform roles but lacks the human touch and the instinct to recognise the pitfalls of searching for something as generic as John Smith in California.

There is no doubt that a blend is required when looking into someone’s past, whether it is for an acquisition, a merger, or a joint venture. Someone who looks clean on the surface may not be and it can take a mixture of thorough AI background checks, some hand-pulled records, and a quiet word with a former employee or partner to find the true scope of someone’s past.

Therefore, human intelligence and the curation of facts from all sources still remain a reliable and relevant tool, even in an AI-driven world.

It is perhaps important that we remember that we ourselves, or more specifically, our brains, are the most sophisticated computers of all and behind all the pageantry and automation of a fraudulent money transfer is a human pulling the strings somewhere. It is not the machine or the company or the shell corporation that is pulling off these activities but instead, at the end of the day, a human.

Yet, as people take advantage of our complex and technologically advanced world to put new and modern spins on ancient techniques of fraud and criminal activity, we would be foolish to think that we can counter, identify, and mitigate their elaborate schemes with human power alone.

Local knowledge and the relationships that form between humans are as essential as the ability to trawl through millions of lines of data in an instant and a reason why it seems, for now at least, there will always be the need for human interaction in any fraud case.

The Takeaway

AI will continue to increase in its popularity and will continue to replace certain roles within the investigative world. There needs to be a hybrid approach to corporate intelligence in this new world. The introduction of new technologies is both inevitable and necessary. However, it needs to balance against human intelligence, as usually, it is this human touch that cracks open the most complex of cases.
While AI represents a very accurate way of proving something, a human touch will always be required and it is in the harmonious unionisation of the AI number-crunching skills and the human creativity and intuition that the most intricate of investigations will be unlocked.

Alone, both methods represent a predictable beast that criminals and fraudsters can work around but together they represent a much more comprehensive wall of security to breach. Sidestepping human intelligence is a risk, as is ignoring the power of AI. Therefore, human investigators must use technology to become the best and fastest consultants to lawyers.
It is all about reorganizing and optimizing the IP Department

Protecting value – The Intellectual Property Report 2020/21

By Andreas Bong

Since 2012, KPMG Law has been gathering and evaluating data from the top international Intellectual Property Departments. For the fifth time, “The Intellectual Property Report 2020/21” analyses IP Departments in their activities, structure, costs, performance KPIs, as well as their trends and developments. This analysis has led to in-depth insights regarding the changing priorities of IP Departments, as well as the observation of many trends over the past years. For this article, two main trends will be described: on the one hand, we can see an increasing tendency for the Heads of IP to strengthen their central governance via decentralized units. On the other hand, there is a notable increase in involvement in research and development activities. But first, let us look at the priorities of IP Departments for 2021:

Priorities of IP Departments

Over the past years, the priorities of the IP Department have consistently remained unchanged. In 2021, as in previous years, the top priority remains the improvement of the advising and management of the internal clients, indicating the importance and central role of the IP Department within the wider business.

Handling an increased workload with the same staff is marked as the second-highest priority, followed by cost optimization and cost reduction. These provide a clear indicator of the importance of the work-optimization and increased-efficiency strategies that will continue to dominate the work and organization of the IP Department in the years to come.

Interestingly, for IP Departments of firms headquartered in Germany, strategic law firm management (i.e. selection, performance management, performance assessment, etc.) cannot be found anymore within the top 20 priorities for the upcoming years. Conversely, for participants outside Germany, this still falls within the top 10 priorities.

Increased central governance

The share of firms with a centralized IP Department has clearly been rising over the last few years. This is to be ex-
pected considering the nature of large multinational firms with large patent and trademark portfolios and a high volume of IP-related challenges that require their activities to be bundled. Taking into account the international character of their activities, numerous participants also have several decentralized IP Departments, which increasingly are governed by one main department with either disciplinary or functional control.

As the graphic below visualizes, since 2014 there has been a major change in the manner of structuring leadership, resulting in international IP Departments leading global, decentralized departments under disciplinary control. Implementing this change in leadership, which impacts all areas including HR-related decisions, showed large financial benefits. Besides better transparency and thus better coordination of activities, this setup is expected to save on the total costs compared to those of the same industry that practised a weaker central governance. However, it should be emphasized that this organizational change should only reflect the relevant elements of an international cooperation within a global IP Department, leaving the local advice unchanged in the responsibility of local units.

**Stronger involvement in R&D activities**

Whereas in the past IP Departments typically had a vast amount of prosecution within their daily task portfolio, in recent years they have become increasingly involved in the strategic consulting of the business. In this sense, IP Departments operate more and more proactively and a clear trend towards increased and earlier involvement in R&D activities can be distinguished.

A closer look at this trend leads us to the following interpretation that this increased involvement results in a decreased rejection rate of invention disclosures and proves itself to be more cost efficient, which is shown in the graphic below. Out of the entire database, we selected companies operating within the automotive industry and divided them into two groups. Based on their full time equivalent (FTE) number in the patent and R&D Departments, one group encompasses those with few R&D FTE per patent professional, at an average of 298, and the other with many R&D FTE per professional, at an average of 622. When considering the rejection rate (their share of unfiled invention disclosures) for each of those groups, however, we observed an average of 27% for the first group. Conversely, for the group with many R&D FTE per professional, an average of 39% can be established. The observation that those IP Departments that belong to the group with the lower amount of R&D FTE have a lower
rejection rate, could be explained by the increased possibility of stronger and earlier involvement within strategic decisions. Having more time for each R&D responsible could result in being able to integrate better into the strategic and risk processes and control the R&D activities at an earlier stage and in a comprehensive manner, avoiding superfluous resource investment.

In addition, not only does an earlier and more proactive involvement of the IP Department within the R&D process lead to lower costs per first filing, as the rejection rate can be reduced by an average of 12%-points – the R&D costs per invention disclosure are also significantly lower, as it is expected that there can be a quicker intervention to align the R&D activities in accordance with the company’s IP strategy.

These insights indicate highly promising optimization and cost reduction potential, as the proactive involvement of the IP Department in the development process can lead to the early management of the development focus and strategy of R&D to ensure that the research is targeted.

Shifting away from the traditional thought that a value contribution of the IP Department is e.g. the ability to ensure Freedom to Operate or to gain profit out of licensing, this means that in the long-term, the real untapped added value of IP could lie in its potential to reduce R&D costs.

**Conclusion and outlook**

Increasingly, IP Departments find themselves in a situation where, with the same staff and a dominant budget and cost pressure, they become more and more involved in strategic decisions. Although this results in an increased workload, they are progressively expected to adopt a proactive approach. It will therefore come down to reorganizing and optimizing the IP Department to ensure long-term efficiency gains and cost-savings. The earlier involvement within the R&D process has great potential in terms of achieving this goal and can put the IP Department at the forefront, ensuring that it enables the operating business and creates added value. In order to ensure that the value contribution becomes tangible and is seen throughout the business, a performance assessment of the IP Department with the use of clear KPIs will become crucial. This is the only way to achieve sustainable and long-term growth and involvement of the IP Department.
The Journey and Lessons of an Experienced In-House Lawyer

Interview with Maria Varsellona, general counsel and company secretary of ABB

Earlier this year, ACC Europe changed its 2020 Annual Conference from an in-person event to a virtual experience. Maria Varsellona, general counsel and company secretary at ABB, sat down with Craig Budner (K&L Gates) to kick off the program, sharing her journey from a law student in Italy to CLO of a Swiss-Swedish multinational. Watch the full interview here.

Business Law Magazine: Can you share some highlights of your career up to now?

Maria Varsellona: I have had an interesting career, starting out in a law firm in Italy. If you had asked me in the beginning of my career, I wouldn't have been quite sure what an in-house lawyer did – much less that I would've ended up being an in-house lawyer. I moved to the UK when I was still young, requalified as an English solicitor, and worked for a British-Italian law firm. That's where I started to have interactions with in-house teams.

Around 2001, I decided to go back to Italy. At the same time, I started to look for a role that would be truly global and international. That was when I understood that in those times in Italy there were not many international law firms yet and I joined General Electric (GE). I believe that, as an in-house lawyer, I was formed and learned everything I know there.

It was a fantastic company that had a wonderful legal department. They had specialists and generalists, and I joined as a generalist in the oil and gas business. Thanks to that opportunity, I started to travel all around the world negotiating with oil companies everywhere. The personal aspect is fantastic because, when you have to negotiate a contract, you have to understand the personality of the negotiator that you have in front of you. This is the part of my job that I still enjoy the most today, although I don't do many negotiations at this point and it is now being replaced by the human aspect in leading teams.

I spent several years at GE. After a stint at the Tetra Laval group, I eventually joined Nokia Siemens Networks, a 50/50 joint venture between the two companies. They were considering an IPO, so I was hired to do exactly that. By the time I finished my notice period, Nokia had actually decided to buy out Siemens and going public was off the table. I didn't even know if I would have had the job a few months after being there because in the meantime Nokia sold their device and service business to Microsoft.

I was very happy and humbled that I was eventually selected to become general counsel of Nokia. That was a wonderful opportunity because of the active role I could play in the transformation of the company. Sometimes I felt that every year I worked the same amount that I would have worked in three years at GE. I learned a lot.

Business Law Magazine: Tell us a bit more about your current role at ABB?

Maria Varsellona: ABB is a fantastic company that is also going through both a cultural and a profound business transformation. We have had a new CEO since early 2020 who is driving the company’s further decentralization
with more responsibility shifted to our four business areas. We have now successfully discontinued our long-standing matrix organization and moved operating activities closer to the customer. At the same time, our new operating model called “ABB Way” provides a governance framework of processes and policies, connecting the business areas and divisions to the corporate center.

**Business Law Magazine: What differentiates the role of an in-house lawyer?**

**Maria Varsellona:** I think that the most important differentiator for an in-house lawyer versus an outside counsel is to be a strategic business partner. When I talk to my team, I always try to visualize our role like a triangle. I say we need to be professionals; therefore, we need to know the laws and the regulations that are applicable to our business. If we don’t know, we must find the time to study them because we need to be able to give the answers that the business expects from us.

Second, I say we need to be gatekeepers. Sometimes the business gets excited about things and we always have to help find solutions, but there are times where we have to be able to say no. The good thing is that if you always find solutions, when you say no, the business takes you very seriously. They know it’s a real no and they follow what you’re saying.

I’m not the kind of lawyer who says, on one hand, you can do this; on the other hand, you can do that. You need to choose what you want to do. I like to choose together with the business and to be accepted at the table, you need to understand the business. You need to be a business partner. You need to understand what the drivers and the strategic objectives are. It’s dynamic. So, you need to have a clear risk map of the company.

Personally, I wish I had known these things in the very beginning of my career – it’s very important to have that understanding. So, when you get the video from the CEO who talks about strategy, don’t think that it’s a waste of time. Watch that video!

**Business Law Magazine: How are things changing?**

**Maria Varsellona:** The way we do our job will be very much influenced by the possibility to anticipate issues. Now, our customers in the field do diagnostics with data. We have to look at red flags with data, rather than just trying to resolve issues when it’s too late. That’s definitely an area where I see huge opportunities.

Due diligence is also something that will be much more digitally and data driven. I am convinced that we will be using artificial intelligence more and more as part of due diligence processes.

But it goes farther than that. At Nokia we were already reviewing current customers’ terms and conditions with machine learning tools. There are already tools in the market that highlight the deviations from your standard. So, when you are going to review the contract of your customer to align to your standards, you already find some highlighted parts where the major issues are.

Then there’s compliance. In these last couple of months, regulations have changed once or twice per week everywhere in the world. That has taken it to the next level really and, therefore, I think that regulatory as part of the integrity compliance function is going to be more and more important. The compliance function has been very, very relevant in the past years, but I think it’s going to become more and more so.

**Business Law Magazine: Can you share a bit on how you reacted to the COVID-19 pandemic?**

**Maria Varsellona:** The last time the world saw a pandemic like COVID-19 was 100 years ago.

At ABB, we could learn a lot from the early experiences we had in China. We were monitoring the outbreak from the very start with the health and safety of our people as our most important priority. Since ABB is a provider of critical infrastructure, we could reopen our factories relatively swiftly taking into account all the necessary measures to protect our people and others. That helped us to develop a very good model that we could replicate elsewhere.

I was a member of the global taskforce that we had installed right away. We also had country taskforces that would adopt the global standards we developed. In many places our requirements were actually much more stringent than the local laws.
Our guiding principles were, first of all, we wanted to keep our employees safe. Second, we wanted to ensure business continuity. We had to continue to provide our technologies not only for our customers, but also for the communities in which we live, because people need critical infrastructures such as electricity.

It was a major challenge for my team, but it has had some surprising rewards for the legal department—greater visibility in the company, a stronger sense of mission, and a more visible seat at the executive table.

Editor’s note: Below are a few avenues to help you develop your leadership skills:

- Check out the ACC Leadership Skills Collection, a curated selection of resources, including 10 Skills Today’s Inhouse Counsel Need, and Leveraging Trust in Times of Crisis: Practical Tips for Chief Legal Officers

- To connect and share with other law department leaders on these key topics, exchange with your peers through the ACC Law Department Management Network. The Network is open to all ACC members.

- Explore ACC’s online educational programs on leadership.
Cooperation Partners

Southern African-German Chamber of Commerce and Industry NPC
Cordelia Siegert
Competence Centre: Corporate Social Responsibility, PO Box 87078
Houghton, 2041, 47, Oxford Road, Forest Town, 2193
Johannesburg, South Africa
Phone: +27 (0)11 486 2775
csiegert@germanchamber.co.za
www.germanchamber.co.za

American Chamber of Commerce in Germany
Dr. Hanns Christoph Siebold
c/o Morgan Stanley Bank AG
Frankfurt/Main
hanns.christoph.siebold@morganstanley.com
www.amcham.de/public-affairs/public-affairs-overview/law/

Hilgard-Law
Dr. Mark C. Hilgard
Myliusstraße 29, 60323 Frankfurt/Main
Phone: 0173 1523444
hilgard-law.de
hilgard@hilgard-law.de

ACC Europe – Association of Corporate Counsel
Carsten Lüers
c/o Verizon Deutschland GmbH
Sebrathweg 20, 44149 Dortmund
carsten.lueers@de.verizon.com
www.acce.com