Baker McKenzie.

# Compliance and Investigation Trends in Germany in 2020

# Contents

# Introduction

In this publication, our lawyers from different practice groups discuss the trends in compliance and investigations of 2020 in Germany. We take a look at the most important developments and court decisions of 2020. Discussing these trends will help companies doing business in Germany to grasp the developments in the area of compliance and investigations in the future. After providing a general overview and presenting the highlights of the developments in the last year, each practice group will outline the developments in their respective practice areas in greater depth.

2020 was overshadowed by the COVID-19 pandemic. Of course, this has also left its mark in the area of compliance. To name just one key development: In spring 2020, shortly after the pandemic began to spread in Germany, the German Federal Government issued an export ban on facemasks and other medical protective equipment to all countries outside of Germany. The introduction of such a broad, far-reaching and unexpected ban caught many companies by surprise, and they consequently faced challenges to adjust to the unannounced governmental measures which had a significant impact on their supply chains and led to government investigations.

## Corporate Liability Act

One of the most important developments in summer 2020 has been that the German Federal Ministry of Justice and Consumer Protection published its draft law for a Corporate Liability Act. For the first time in Germany, this draft law sets out to introduce a corporate criminal liability and to define "corporate crimes" (Verbandstaten). The legal framework currently in force only provides for a criminal liability of individuals. Corporations so far can only be liable for the commitment of administrative offences (Ordnungswidrigkeiten). Administrative liability under the current legal framework provides for a monetary fine of up to EUR 10 million. The new draft law on corporate criminal liability would also raise the upper limit to 10% of the worldwide turnover of the corporate group. The draft, however, also introduces and codifies new elements to be taken into account for the calculation. Following a decision by the German Federal Court of Justice (Bundesgerichtshof), the draft law stipulates that the existence and quality of an internal compliance system must be taken into account as a mitigating factor when determining the extent of the criminal liability as a result of corporate infringements of the law.
The judgment and its codification provide an even greater incentive for companies to continuously work on their compliance systems.

## Highlights of 2020 in the different practice areas:

### General Corporate Compliance and COVID-19

In 2020 the world and global business were dominated by the COVID-19 pandemic. Businesses had to adapt to the pandemic in many and often dramatic ways, which also affected corporate compliance. The challenge for corporate compliance systems in 2021 will be to review how the pandemic was handled and prepare for the "new normal" to come.

### Anti-Bribery and Corruption

Although the year 2020 did not bring any significant legal changes or court decisions in the area of anti-bribery and corruption, it did set an important course for the future. Companies based in Germany should review their compliance management system (CMS), as the implementation and effectiveness of a CMS can lead to more lenient penalties. A crucial component of an effective CMS is a whistleblowing tool. When implementing a whistleblowing tool and dealing with whistleblowers, the requirements that the forthcoming national Whistleblower Protection Act will place on companies must be taken into account.

### Antitrust

2020 has seen competition authorities targeting the digital economy and attempting to find suitable approaches towards the challenges of a global pandemic. While traditional anticompetitive agreements (e.g. in the automotive or healthcare sector) still play a role, the investigation of digital business models by Amazon, Facebook, Apple & Co. has long become the most visible area of antitrust enforcement. Amidst a modified regulatory environment in Germany, competition law must be an integral part of every compliance lawyer's agenda in the months to come.

## Data Protection

From a data protection law perspective, we have seen in particular the following developments: The German data protection authorities imposed several high fines, including one concerning video surveillance of employees. There were also a number of noteworthy developments regarding international data transfers following the so-called "Schrems II" decision of the European Court of Justice of the European Union. Since the Whistleblowing Directive must be implemented into national law, it is also expected that Germany will have specific whistleblowing legislation in the near future.

## Money Laundering

Anti-money laundering stays high on the agenda in 2021 and beyond. While the implementation of the 5th Money Laundering Directive (MLD) in January 2020 led to considerable tightening of customer due diligence obligations, the recent implementation of the 6th MLD in February 2021 significantly facilitates the criminal prosecution of money laundering offences by German enforcement authorities. Overall, increased enforcement action must be expected in the near future.

## Labour Law - False Employment

A key compliance trend in German employment law is the increase of law enforcement when it comes to the use of misclassified independent contractors. German authorities are applying more scrutiny and are less tolerant towards misclassification. This collides with headcount restrictions which oftentimes result in the temptation to fill talent-gaps with independent contractors. Lacking a robust compliance system can result in very significant penalties, includingcriminal sanctions, for the responsible management.

## International Trade Law

Over the course of the past year, globally operating companies with complex supply chains were subjected to a major stress test as a result of the COVID-19 pandemic. In light of the magnitude of the challenges not only stemming from the pandemic, but also Brexit and trade wars, global supply chains generally showed resilience. New export restrictions on, for example, protective gowns and medical equipment, as well as economic sanctions and a strengthened foreign investment review regime, show that German companies need to be on top of regulatory developments to ensure they comply with a set of continuously changing obligations governing their exports, trade transactions and foreign investments.



# Outlook for 2021

In 2021, the regulatory developments will be dominated by the parliamentary elections in the fall. The legislative projects currently underway will be pursued and completed in the run-up to the elections. This relates in particular to the above-mentioned Corporate Liability Act, but also to the Supply Chain Act which is currently under discussion within the German government.

We are happy to discuss the developments outlined below in greater detail. You may find our contact details at the end of this publication.

Best regards,

**Anahita Thoms, LL.M.**
Partner
Dusseldorf

+49 211 3 11 16 121
Anahita.Thoms@bakermckenzie.com

# Contributors

**Dr. Nicolai Behr**
Partner

**Sina Buhl**
Associate

**Dr. Christian Burholt, LL.M.**
Partner

**Alexander Ehrle, LL.M.**
Associate

**Dominik Guttenberger**
Associate

**Dr. Robin Haas, LL.M.**
Senior Associate

**Dr. Nicolas Kredel, LL.M.**
Partner

**Dr. Andreas C. Lohner**
Partner

**Dr. Manuel Lorenz, LL.M.**
Partner

**Dr. Holger Lutz, LL.M.**
Partner

**Dr. Michaela Nebel**
Partner

**Dr. Steffen Scheuer**
Partner

**Dr. Anika Schürmann, LL.M.**
Counsel

**Anahita Thoms, LL.M.**
Partner

1.0

# General Corporate Compliance

Dr. Andreas C. Lohner and Dr. Robin Haas, LL.M

In 2020 the world and global business were dominated by the COVID-19 pandemic. Businesses had to adapt to the pandemic in many and often dramatic ways. As governments and business alike were taken by surprise by the virus all of this happened very quickly. Changing the way business work had an effect on the risks companies face, which naturally affects corporate compliance. Changing business also means that some of the corporate compliance measures of pre-COVID-19 times were not designed to work in an environment in which a large part of the work force stayed at home. The pandemic will not go away in 2021. The challenge for corporate compliance systems in 2021 will be to review how the pandemic was handled by the respective compliance management system and prepare for the "new normal" to come.

2020 brought a number of significant challenges to the corporate compliance arena, in particular:

- A completely new layer of compliance rules relating to the pandemic was created and had to be observed by companies. These Corona specific rules included for example measures according to the Infectious Diseases Protection Act (Infektionsschutzgesetz, "IfSG") or the statutory ordinances issued in accordance with the IfSG. In addition to sanctions against the persons acting in each case, violations of measures pursuant to the IfSG may under certain circumstances also lead to fines against the company pursuant to the Act on Regulatory Offenses.

- In addition to the Corona specific compliance risks described above, the ongoing economic crisis poses further compliance risks for companies. In times of crisis, employees are under great economic pressure. Orders may have been cancelled or postponed. Routine procedures and standard processes may have no longer been followed as usual. There may have been a growing temptation to be less strict about complying with internal rules and legal regulations or to enter into business transactions that would normally be avoided. Non-compliant behavior typically increases when companies and/or their employees seek to:
  - Speed up processes that may be stalled and/or delayed due to a crisis, e.g. customs clearance.
  - Shift to alternative business partners (e.g. suppliers) that were less affected by the crisis but that may have higher risk profiles, or without sufficient time to conduct due diligence to evaluate their risk profiles.
  - Make false representations when applying for government grants and subsidies, especially with respect to Corona related relief funds.

However, external factors such as an economic crisis are generally not considered by regulators and law enforcement agencies as effective justification for non-compliant behavior.

- The COVID-19 pandemic also changed business models, traditional work routines and had a significant impact on standard compliance routines:
  - Online activity increased significantly with an effect on for example fraud or data security risks.
  - Significant parts of the work force worked from home increasing compliance risks (data security) and impairing traditional compliance oversight as well as typical internal investigation measures.
  - Many companies were under cost pressure, which also often led to cost cuts with regard to non-urgent compliance projects. In particular, the audit and update of compliance programs including risk analysis projects were a lot less frequent than in previous years or at least delayed significantly.
  - In person compliance trainings were over large parts of 2020 practically impossible. Depending on how much online training companies already had in place, the effects of this varied from company to company. In companies with less developed online training, it is likely that 2020 saw significantly less training than in previous years.
  - The pandemic also had a significant impact on the investigation of alleged wrongdoing. In person interviews of employees in the context of internal investigations were rare. Quite often interviews were online. In addition, it seems that the number of investigation handled externally may have gone down. Compliance teams may have investigated more in-house and/or less allegations were investigated.

The above outlined challenges will not have affected all companies the same way and some companies may have had other pandemic related challenges. Irrespective of this, the challenges of 2020 should lead to a thorough review of corporate compliance in 2021.

Such review should look in particular at the following:

- Update risk assessment: Is the risk assessment of the company still valid or does it need an update? New rules, new business models (online), new business partners and new ways of working may result in a different look at the risk environment the company faces. As good corporate compliance is always based on solid risk assessment, this should be a top priority in corporate compliance in 2021. This should also be considered in companies that only have undergone a risk assessment in late 2019 or early 2020 and planned to only update in 2022. The dimension of changes in 2020 were rather dramatic. Review circles should at least be questioned.

- (Selective) review, if the above outlined Corona specific compliance challenges were met through specific compliance measures and audits.

- Fresh look at technology: The pandemic forced companies to speed up the digital transformation. Meetings, interviews and phone calls were within weeks replaced by Zoom, Microsoft Teams or other virtual platforms. These technologies also provide opportunities for corporate compliance. A good example for this is compliance training. In the past, training was either in person or online. In person training is often perceived as "expensive" and online training as "not interactive". If board meetings, shareholder meetings and school classes can be conducted virtually it should also be possible to keep or include virtual trainings as part of the compliance training plan. Risk assessments and compliance audits also often include interviews with employees. These were in the past primarily in person and over the last year mostly virtual. What seemed to be a "second best option" has in the meantime changed into the normal way to operate and proven to work. Virtual meetings are less expensive and often easier to organize. With the exception of interviews in internal investigation (potentially only "critical interviews") virtual meetings can be as effective as in person meetings. Companies can and should explore, if remote/ virtual training, onboarding, audits should be added to the standard compliance toolbox.

1.0

- Companies should also take a critical look which compliance measures were postponed or delayed in 2020. If any were postponed or delayed, it should be reviewed, if and how these should be redone or replaced.
- Renew tone from the top: 2020 was a year of crisis, challenges and uncertainties. This may be a good time to renew the tone from the top to affirm that there are no uncertainties about the importance of compliance.
- Most companies are already preparing for the new normal. It is likely that some of the changes to business models or work routines that were initially driven by the pandemic will stay. Given the above outlined significance of these changes on corporate compliance it seems advisable for companies to already include compliance functions into the teams planning the new normal.
- As employees more regularly work remotely from home, companies should ensure that their internal policies on the use of personal devices are up to date and facilitate and not hinder compliance oversight and internal investigations.

If one looks at lessons learned from the pandemic, it could be to value the importance of compliance culture. Given the speed things changed in the pandemic, it is clear that not all new developments were immediately reflected in the rules of the company. If the compliance culture in a company extends beyond what is explicitly included in the code of conduct it may be able to deal with exceptional situations like the pandemic better than others.

**Dr. Andreas C. Lohner**
Partner
+49 89 5 52 38 263
Andreas.Lohner@bakermckenzie.com

**Dr. Robin Haas, LL.M.**
Senior Associate
+49 89 5 52 38 273
Robin.Haas@bakermckenzie.com



2.0

# Anti-Bribery and Corruption

Dr. Nicolai Behr, Dominik Guttenberger and Sina Buhl

Large corporations are embracing the fight against corruption. To date, 97% of companies with more than 10,000 employees have implemented a compliance management system (CMS) and most companies identify the fight against corruption as one of the main objectives of their CMS. Since the Federal Court of Justice has ruled that the (non-)implementation and effectiveness of a CMS can lead to more severe or more lenient penalties, companies have a great interest in modeling their CMS at best practice.

While there have not been any legal developments or landmark court decisions, some developments have been noteworthy.

## Anti-corruption in Germany

### Whistleblower protection

A very important part of the CMS is a whistleblowing system and a process to encourage employees to take action against misconduct. Whistleblower reports are often a significant source for uncovering misconduct. To protect whistleblowers, the EU Whistleblowing Directive came into force in December 2019. This directive must be implemented into national law by 17 December 2021. The German government is currently working on a draft whistleblower protection law. The draft as it currently stands would invert the burden of proof, that means the company would have to prove that no retaliation took place and may be fined for retaliation against whistleblowers.

### Competition register

In Germany, a competition register has been introduced. In the future, it will be mandatory to consult the competition register prior to awarding public contracts above EUR 30,000. The competition register will not only be populated by public contract-related information, but also with information regarding any sanction proceedings against such companies. In all likelihood, a "negative" entry in the register will lead to the exclusion of such company for future public awards. To conduct future business with the public sector, companies listed on the competition register have to carry out so-called self-cleaning measures to reduce the registration period to a minimum. Such self-cleaning measures regularly require the company to cooperate with the investigating authorities and to compensate for the damage incurred.

2.0

### Digitizing investigations
Today, many crimes are committed via the internet. Therefore, investigators and forensics professionals need to understand in-depth network security and software systems that underpin, for example, expense reports, payroll, procurement and electronic banking.

For companies, it is important that compliance and internal audit teams understand these topics well, in particular communication flows, to properly conduct an internal investigation.

It is essential to identify and work with experts, especially in IT and information security, to gather evidence and to identify responsible parties for data protection documentation (e.g. when and what data is transferred between the company and third parties).

## European developments

### European Public Prosecutor's Office
Since 2020, the European Public Prosecutor's Office, supported by 22 member states (including Germany), has the power to investigate, prosecute and bring to justice crimes detrimental to the European Union budget, such as fraud, corruption or serious cross-border VAT fraud. This will entail a new type of investigation and require new approaches to criminal law advice.

### European Production and Preservation Order (to be expected in 2021)
The draft regulation of the European Production and Preservation Order defines two instruments. Each instrument imposes a direct obligation on a provider abroad without having to approach — through a mutual legal assistance request or by means of a European Investigation Order (EIO) — authorities of the state in question.

- European Production Order (EPO): An EPO obliges service providers to hand over data requested by authorities within 10 days. The deadline is shortened to 360 minutes for urgent cases due to an imminent threat to life and limb or critical infrastructure. The request for subscriber data and access data applies to any criminal offense; for other data, it applies only to serious criminal offenses with a sentence of three years or more.
- European Preservation Order (EPrO): The EPrO is intended to prevent the deletion or overwriting of existing data to allow for later requests for mutual legal assistance, an EIO or an EPO.
- Authorities of the member state in which the provider is located must assist authorities of the requesting state to enforce the requests.
- A company must also be able to respond appropriately to such requests and ideally implement processes in advance.


**Dr. Nicolai Behr**
Partner
+49 89 5 52 38 204
Nicolai.Behr@bakermckenzie.com

**Dominik Guttenberger**
Associate
+49 89 5 52 38 156
Dominik.Guttenberger@bakermckenzie.com

**Sina Buhl**
Associate
+49 89 5 52 38 208
Sina.Buhl@bakermckenzie.com




3.0

# Antitrust

Dr. Nicolas Kredel, LL.M., Dr. Christian Burholt, LL.M. and Dr. Anika Schürmann, LL.M.

2020 has seen competition authorities targeting digital economy and attempting to find suitable approaches towards the challenges of a global pandemic. Looking ahead, competition law compliance merits particular attention of compliance lawyers from digital businesses and traditional industries alike. While the specific implications of the revised German competition law (10th Amendment) will only come to show in the next few months, this section provides an outline on the most relevant changes and illustrates noteworthy enforcement activities in Germany and the EU.

## Important regulatory developments

In January 2021, the 10th amendment to the German Act against Restraints of Competition has taken effect ("ARC"). The new law entails a number of noteworthy changes from a compliance perspective:

### Calculation of the administrative fine
When calculating the administrative fine, the Federal Cartel Office ("FCO") will need to evaluate adequate and effective compliance measures conducted prior to the infringement by the undertakings concerned to prevent and detect competition law infringements (cf. § 81d para. 1 No. 4 ARC).

### Competition in the digital economy
§ 19 para. 1 No. 4 ARC clarifies that the refusal by a dominant company to grant access to data can be abusive, if such access is objectively necessary to operate on one of the relevant upstream or downstream markets, and the refusal to grant access restricts effective competition on that market.

Introduction of § 19 a ARC, which addresses "undertakings with paramount significance for competition across markets", providing for the possible prohibition of certain practices listed in the new § 19 a para. 2 ARC (e.g. self-preferencing measures, measures to restrict access to markets, pre-installation of own software or leveraging of market power to neighboring markets).

### Increase of turnover thresholds for merger control
Domestic merger control turnover thresholds were significantly raised from EUR 25 million to EUR 50 million (first domestic turnover threshold) and from EUR 5 million to EUR 17.5 million (second domestic turnover threshold).

3.0

### "Remondis-clause"
Enabling the FCO to counteract market concentration tendencies for transactions and parties falling short of the jurisdictional thresholds. This requires a prior sector inquiry of the relevant market(s). The FCO will then under certain conditions be entitled to require an undertaking to notify all future acquisitions in the relevant market.

### Implementation of ECN+ perspective
The implementation of the ECN+ Directive (EU) 2019/1, legally anchors the leniency program of the FCO in relation to cartels and implements further changes. In addition, the FCO will be entitled to request information and the release of documents not only from the undertakings concerned but also from individuals even if the information discloses facts able to bring about a prosecution of a criminal or an administrative offence. However, to preserve the nemo tenetur principle, this information may only be used against that individual and her or his immediate family if the individual agrees.

## Important decisions

The importance of having in place an effective compliance system was once again underlined by the antitrust enforcement in the past year. In 2020, the FCO imposed fines amounting to EUR 358 million on a total of 19 companies and 24 individuals. The sectors concerned included plant protection products, vehicle registration plates and aluminium forging companies. The European Commission ("Commission") has inter alia imposed a fine of EUR 260 million on three ethylene purchasing companies, setting the record in 2020 for the highest fine in a single case among leading enforcement jurisdictions.

In the **aluminium sector**, the FCO imposed fines amounting to EUR 175 million on five aluminium forging companies and ten employees. Representatives of the fined companies had formed the so called "Aluminium Forging Group" and informally exchanged information inter alia on costs incurred in the procurement processes and on increased costs for sourcing aluminium and energy. In addition, the Group discussed strategies to pass on cost increases to their customers.

The **ethylene cartel**, fined by the Commission, comprised of four companies colluding on ethylene purchase prices (Case AT.40410). By jointly influencing monthly pricing negotiations and exchanging price-related information, the cartelists aimed at buying at the lowest possible price. One cartelist received full immunity under the 2006 leniency notice, as it revealed the cartel to the Commission.

In 2020, the Commission also added EUR 18 million to the list of fines against automotive parts manufacturers (Case AT.40299). After a leniency application in 2015, the Commission found two separate infringements in the automotive closure systems branch, covering products such as door modules, window regulators and latching systems. The case must be seen in the context of the Commission's series of major investigations in the **car parts sector**. Since 2013, the fines imposed within this series have added up to EUR 2.17 billion, with notable cases like automotive air conditioning, lighting systems and seat belts. So far, the Commission has closed 14 cases in the automotive parts sector.

The antitrust case against **hotel group** Melia embodies the Commission's latest pursuit of restrictions on cross-border trade (Case AT.40528). In February 2020, the Commission fined Melia EUR 6.7 million for including restrictive clauses in agreements with tour operators that limited active and passive sales of hotel accommodation. In particular, Melia's general terms and conditions contained a clause that artificially divided the single European market. Accordingly, the contracts concluded only applied to reservations made by consumers residing in certain countries. As a result, Melia prevented tour operators from freely offering hotel accommodations throughout the EEA and responding to direct requests from consumers residing outside the countries specified in the clause.

In the pharmaceutical industry, the Commission imposed fines amounting to EUR 60.5 million on two companies for engaging in **pay-for-delay agreements** regarding Modafinil, a drug used for the treatment of sleep disorders (Case AT.39686). Pay-for-delay agreements between drug patent holders and generic drug manufacturers have been occupying the Commission for some time. These are settlements in patent disputes in which a generic drug manufacturer agrees not to enter the market. In return, a patent holder offers monetary or other commercial benefits.

Early in 2020, the European Court of Justice ("ECJ") already delivered a preliminary ruling on **pay-for-delay agreements** (C-307/18 – Generics (UK) and others): Having regard to Art. 101 TFEU, the ECJ emphasized the requirement of at least potential competition between the parties of such agreements. It must first be demonstrated, whether there are real and concrete possibilities of market access by the generics manufacturers. In order to find a sufficient degree of harm for an object restriction under Art. 101 TFEU, it is necessary to show that such agreement can have no other explanation than the commercial interest of the parties not to compete on the merits. If the adverse effects of such conduct exceeds the specific effects of the agreement, it may also qualify as an abuse of dominance under Art. 102 TFEU. In particular, this may be the case if it results in foreclosure effects, reserving the market to the drug patent holder and if such conduct cannot be outweighed by efficiencies or consumer benefits.

## Trends & Developments

In 2020, competition authorities in Germany and Europe continued their focus on the **Digital Economy**, the **Automotive industry** and the **Healthcare and Life Sciences industry**, sectors very familiar to the antitrust community. Having turned the global economy upside down, the ongoing **Corona-pandemic** caused a number of new challenges for antitrust compliance and will likely continue to do so for some time. Disrupted workflows, short-term cooperation between companies, cut back of M&A activities and altered timelines are only a few effects compliance lawyers will need to have an eye on.

### Corona-pandemic
At an early stage of the pandemic, competition authorities acknowledged in a joint statement by the European Competition Network ("ECN") the economic consequences triggered by the pandemic. Short-term cooperations between undertakings may be necessary to ensure security of supply in certain branches. The ECN emphasized not to actively intervene against such measures, but clearly expressed its readiness to take action against companies taking advantage of the situation by cartelising or abusing their dominant position.

### Automotive
In addition to the Commission imposing fines upon car parts manufacturers, the FCO announced sector inquiries into the publicly accessible charging infrastructure for electric cars. The aim is to identify competition problems concerning the supply of such facilities, e.g. regarding prices and conditions.

The FCO accepted temporary measures in the automotive sector to overcome the current COVID-19 crisis.[1] Measures include, especially, a limited data sharing to coordinate the restart of production and to allow a quick restructuring for economically troubled businesses. However, the FCO announced its intention to reassess the measures, e.g. in cases of complaints.

1 Read more **here**.

3.0

## Digital Economy

Challenges in the realm of the digital economy have been at the center of the **International Competition Network's ("ICN")** annual conference in 2020. The ICN exchanged views on topics such as abuse of dominance in digital markets, effective competition enforcement in the digital economy, merger investigations in the digital sector and digital readiness of competition authorities.

The FCO initiated a second abuse investigation into **Facebook**. While challenges against the FCO's decision on Facebook's alleged abuse in the context of collection and use of data are still pending before the Higher Regional Court Dusseldorf, the FCO now focuses on virtual reality activities: The proposed linkage of virtual reality products to Facebook's social network may constitute an abuse of dominance.

The FCO also launched a sector inquiry into **messenger services** in late 2020. In particular, the FCO intends to evaluate the protection of personal data to assess possible violations of consumer rights.

The Commission sent a statement of objections to **Amazon** regarding its use of non-public marketplace seller data. As provider of a marketplace and as a retailer on the same platform, the usage of non-public seller data may allow Amazon to avoid the normal risks of competition in the retail sector and leverage its marketplace dominance. In addition, the Commission launched an investigation into Amazon's practice of allegedly favoring its own offers and those offers using Amazon's logistics over others.

The Commission also launched an investigation into **Apple**'s App Store rules. Following complaints, the investigation aims to focus on the mandatory use of Apple's own in-app purchase system and restrictions on developer's ability to inform users of alternative purchasing possibilities. A second investigation into Apple was opened to assess competition concerns regarding Apple Pay. This investigation focuses on a potential distortion of competition by Apple Pay's terms and conditions, as well as Apple Pay being the sole mobile payment solution to be able to access the NFC technology on iOS devices.

In this context, it is interesting to note that **Apple** now officially considers antitrust law to be a significant business risk and in early 2021 announced the introduction of an **antitrust compliance program.**

## Healthcare and Life Sciences

The Commission published a **Temporary Framework Communication**[2] in response to the coronavirus outbreak in April 2020. Thereby the Commission addressed the general supply shock following the pandemic and in particular the risk of shortages in critical medical goods. The framework's objective is to provide guidance to companies intending to temporarily cooperate and coordinate business activities aimed at increasing production. In substance, the Commission outlines and explains its approach towards such cooperations under antitrust law.

Medicines for Europe made use of the **comfort letter** option under the Commission's temporary framework. The option is part of a temporary process set up by the Commission to provide ad-hoc feedback on the legality of specific cooperations under antitrust law. In particular, this comfort letter dealt with a specific voluntary cooperation among pharmaceutical producers targeting the risk of shortage of critical hospital medicines for the treatment of coronavirus patients. Having regard to the objective and safeguards put in place, the Commission found such cooperation justifiable under the special circumstances of the COVID-19 pandemic.

2 Access **here**.



# Looking ahead: Antitrust compliance in 2021

Taking into account the developments of 2020, antitrust compliance will remain crucial in the year ahead. The changing regulatory environment, the ongoing COVID-19 pandemic, multiple sector inquiries and Post-Brexit Europe will have compliance lawyers face a number of challenges. Here are our key takeaways for 2021:

## Regulatory changes:

- Check your Compliance System: When calculating a fine in infringement proceedings, the FCO will need to evaluate adequate and effective compliance measures conducted prior to and after the infringement. Effective compliance systems can pay off.
- Use the "Comfort Letter" option: Companies can require the FCO to assess an envisaged cooperation with a competitor. Such assessments, formerly only granted on an exceptional basis, can increase legal certainty in complex cooperation projects, or joint bid scenarios.
- Analyze Data Sets: Data sets can become subject to access requests by suppliers, customers, or even competitors. Companies should carefully analyze their data sets as they explore options for data monetization in light of potential 3rd party access rights. Vice versa, access to 3rd party data might represent an interesting course of action for companies.
- Consider new "Remondis-Clause": Companies that are subject to a sector inquiry by the FCO should be aware: There is a risk that the FCO might require certain companies to notify all significant future acquisitions in a specific industry.

## COVID-19 Pandemic

- Make sure any pandemic-related business disruptions do not affect the efficiency of your compliance mechanism.
- Screen any short-term cooperation for competition concerns and make use of the possibility to consult the FCO in the event of doubt.

## Post-Brexit

- Pay attention to both competition law regimes: Important for UK companies to remain compliant with EU competition law when undergoing business activities within the EU. On the other hand, companies active within the UK need to comply with the UK regime, bearing in mind personal risks for executives.


**Dr. Nicolas Kredel, LL.M.**
Partner
+49 211 3 11 16 1327
Nicolas.Kredel@bakermckenzie.com

**Dr. Christian Burholt, LL.M.**
Partner
+49 30 2 20 02 81 756
Christian.Burholt@bakermckenzie.com

**Dr. Anika Schürmann, LL.M.**
Counsel
+49 211 3 11 16 128
Anika.Schürmann@bakermckenzie.com

4.0

# Money Laundering

Dr. Manuel Lorenz, LL.M. and Dr. Anika Schürmann, LL.M.

There is no standstill in German anti-money laundering law and the future will see further important developments. 2020 saw the implementation of the fifth Money Laundering Directive (5MLD) into German law effective 1 January 2020. Key changes included a focus on cryptocurrencies and regulating crypto-trading and crypto-custody and a focus on the real estate sector. Both areas have been identified as posing additional money laundering risk. A further focus in 2020 was the Transparency Register (register of beneficial owners) which is now open to inspection by the public and the competent supervisor has engaged in significant enforcement activity.

A key event in 2021 will be a radical conceptual change in the definition of the crime of money laundering as a result of the implementation of the sixth Money Laundering Directive (6MLD). In addition, 2021 will also see further changes being made to the rules of the Transparency Register, since the initial German approach to de-bureaucratize the obligations of German companies has lead to chaos and confusion. There can also be little doubt that regulators and law enforcement authorities will clamp down further on enforcing AML-laws and prosecuting money launderers in 2021.

## AML and Cryptocurrencies

A significant money laundering risk is created by the rise of cryptocurrencies and "token" and it is an open secret that cryptocurrencies are used for purchasing drugs, weapons and other illicit goods in the DarkNet. Moreover, crypto currencies can be used for money laundering given that the flow of funds is possible in complete anonymity, even across borders, without any physical transport of bank notes. This is because transfers of cryptocurrencies occur outside the financial system and are completely anonymous. Cryptocurrency transfers are recorded in a blockchain using the distributed ledger technology and based on encryption. The publicly available blockchain data will provide a trail of each transaction, but the sender and receiver is only a wallet address. The identity of the holder of the wallet is not known. The only means of access to the wallet is a cryptographic key in the hands of the wallet holder.

Consequently, 5MLD imposes a registration requirement for crypto currency traders and wallet providers, because these service providers are important entry and exit points for the holding and transferring of crypto assets. In addition, 5MLD makes these companies "obligated persons" under applicable AML law. As a consequence, crypto traders and wallet providers must identify their clients before entering into a business relationship with them, thus removing the anonymity of crypto trading.

When implementing 5MLD, Germany went one step further and created a financial services license requirement: Crypto traders and wallet providers (crypto custodians) are treated as investment firms and will have to apply for a license under the German Banking Act. According to the view of the German regulator BaFin (stated for the first time in 2011), cryptocurrencies come under the definition of financial instruments under the Banking Act as "Units of Account" and therefore, the exchange of fiat currencies into cryptocurrencies and vice-versa was viewed as trading in financial instruments subject to a license requirement under the Banking Act. This had been disputed by the Higher Regional Court of Berlin in a criminal case in 2019, which, however, did not prompt BaFin to change its view. The issue has now been clarified in the implementation law for 5MLD.

Given that crypto traders and crypto custodians perform regulated activities, they automatically became subject to the AML obligations under the German Money Laundering Act. In addition, it is now clear that also the exchange of cryptocurrencies into another cryptocurrency is also crypto trading that requires a license. Originally, the draft law did not allow the combination of crypto custody activity with any other regulated financial services. This limitation was removed in the final law.

It should be noted that the issuance of token as a corporate finance instrument continues to be an unregulated activity and token issuers are not subject to any AML obligations. Most public sales of tokens nevertheless are in practice conducted with money laundering checks, since most subscribers of token will open wallets with a crypto custodian and token issuers need to control the nationality and residence of the subscribers to avoid breaching local securities laws.

## Real Estate Sector

Another major concern for money laundering in Germany is the real estate sector. In its national risk analysis, Germany has acknowledged that proceeds from crime are often reinvested in real estate. In a spectacular action, German law enforcement authorities confiscated a large number of properties held by family members of a "clan" accused of numerous organized crimes. As a consequence, Germany used the opportunity to increase AML obligations surrounding real estate transactions. Not only must real estate brokers have risk management including group-wide procedures to combat money laundering in place, but a new notification regime was created in connection with real estate transactions.

A suspicious activity report to the relevant Financial Investigation Unit (FIU) must be made by lawyers and notaries, auditors and tax advisors for transactions closely related to particular high-risk countries regarding one of the participants or beneficial owner or the object of the transaction or where a participant or a beneficial owner is on a sanctions list. Further reporting obligations arise in case of participants who fail to fulfill their obligations to provide information under the applicable money laundering rules or if there is reason to believe that the information is false.

4.0

A report must also be made:

- in case a trust relationship is used if the trust has no evident economic or other legitimate purpose;
- if one of the participants or beneficial owner is subject to criminal investigations or convictions;
- in case there is reason to believe that the transaction value is grossly disproportionate to the legitimate income or assets of the seller, purchase or beneficial owner;
- if the beneficial ownership goes through a company in a third country and this interposition of the company has no evident economic or other legitimate purpose;
- if the transaction carries hallmarks under the Directive dealing with cross border tax schemes ("DAC6") and a reporting obligation under such Directive applies;
- where there are deficiencies or peculiarities with any power of attorney used, including where the power of attorney was notarized by a German consular official in a third country;
- in case of cash payment or payment in cryptocurrencies;
- in case of gross deviations from the fair market value or;
- in case of payment to a party otherwise not related to the transaction;
- in case of a resale within three years at a significantly different price if there is no apparent reason for the price deviation or if the real estate is sold back to the original seller for no apparent reason.

This drastically increases the compliance obligations of the professionals involved in the transaction.

In addition where in a real estate sale or purchase (including by share deal) involving companies, foundations or trusts, the obligations of the recording notary have been increased: The notary must obtain a documentation of the ownership and control structures in text form and perform a plausibility check. On demand, such documentation must be shared with the FIU.

5 MLD also brought additional AML obligations for dealing in art. This is also driven by intelligence that art works, particularly stolen art, serve as collateral in drug trafficking and other illegal trades.

## Register of Beneficial Owners

Another new feature of 5MLD is that the register of beneficial owners of German companies (Transparency Register), which was implemented with 4MLD, has been opened for inspection by the general public without any need to demonstrate a legitimate interest. Under 4MLD, only obligated persons and persons with a legitimate interest could get access to the Transparency Register. At the same time, the obligations of companies to make own inquiries regarding their beneficial owners have been strengthened.

In this context, the Federal Administrative Office as the competent authority for enforcing the obligations of companies to provide information to the register has started to launch investigations into situations where there are actual or perceived inaccuracies in the information provided and levied administrative fines in case of non-compliance. The disclosure obligations of companies are complicated by the de-bureaucratization approach taken by the German legislator: Under the law it is not necessary to provide information to the Transparency Register where the information on the ultimate beneficial owners is already visible from other public registers and such information is complete. As a result, companies need to make a complex analysis on whether they need to make a filing or not. It is highly recommended that companies fully document their analysis and their efforts to determine their beneficial owners. Otherwise, there is a risk that such companies will be sanctioned by the Federal Administrative Office.

## Enforcement in the Financial Sector

A further area of enforcement activities is directed against banks and other financial sector companies. Banks are increasingly the subject of dawn raids based on suspicions that bank employees were assisting bank clients in money laundering activities. Moreover, supervisory authorities keep a closer eye on money laundering compliance and react with harsh measures in case of findings of perceived deficiencies in proper performance of customer due diligence. If banks are not vigorously pursuing remediation projects (including "backward" identification of clients), the supervisory authority will exercise further pressure and in several cases it has appointed special representatives that shall monitor the remediation measures from inside the bank.

## Criminal Law Enforcement

Whereas the implementation of the 4MLD and 5MLD led to considerable tightening of customer due diligence obligations, the implementation of the 6MLD in 12 February 2021 will facilitate prosecution of money laundering offences by the German enforcement authorities.

In this respect, the most important change will be the complete elimination of an exclusive list of predicate offences, which might trigger money laundering allegations. Under previous law, a money laundering offence required the relevant asset to be derived from either crimes (offences with a minimum term of imprisonment of one year) or from certain other enumerated offences, which usually required commission on a commercial or gang basis. In future, it will be sufficient for an asset to be derived from any criminal offense and regardless of whether it was committed on a commercial or gang basis. Obviously, this significantly expands the scope of the German money laundering prohibition, which, going forward, will apply regardless of the predicate offense by which the assets were acquired and regardless of whether the predicate offense was committed intentionally or negligently. In the areas of tax and customs offenses, e.g., unlawfully obtained tax refunds will be caught in future even in case of a one-time offence. Although, the court will still be obliged to establish that the relevant assets originate from a criminal offence, this task will naturally be easier if the court does not have to specify the predicate offence. Overall, the implementation by the German legislator goes considerably beyond the requirements of the 6MLD, which only requires that assets be included that originate from offences with a minimum sentence of six months.

4.0

On the other hand, in the future, there will be no more criminal liability in case an employee negligently fails to recognize that the asset originates from a criminal offense. The German money laundering offense would otherwise have had an almost boundless scope of application. Thus, in future, the offender needs to positively know or at least accept that an object originates from some criminal offence. It remains to be seen how the requirement of intent will play out in practice. It should not always be easy for the courts to prove intent with regard to the illegal origin of the assets, however.

In addition, the scope of the German money laundering prohibition has also been extended territorially. While, in the past, the prohibition would only apply to assets derived from outside Germany where the predicate offence was punishable both in Germany and at the place of the offence, criminal liability at the place of the offense is no longer relevant for certain offences mentioned in the European Conventions and Framework Decisions. This inter alia concerns corruption offences.

Finally, the implementation of the 6MLD provides for an increased penalty risk (imprisonment from three months to five years) for money laundering offenses committed by obligated persons according to the 4MLD (such as credit institutions, financial services institutions, insurance, auditors, estate agents, etc.). Consequently, the number of suspicious activity reports should further increase in future and it remains to be seen how this will be dealt with by the authorities, considering their already current overload in processing suspicious activity reports.

## Outlook

As an outlook on enforcement trends in 2021, it is clear that the competent supervisory authorities, including the bar associations, notary associations and other professional bodies are under pressure to ensure that financial sector companies and processional firms fully comply with their AML obligations and in case there are deficiencies they will apply sanctions. Therefore, increased enforcement action must be expected in the near future.

At the same time, it is to be expected that the risk for companies who have not complied with their obligations to provide information on their beneficial owners to the Transparency Register continues to increase. A further tool has been introduced by 5MLD; the so-called discrepancy notice. If obligated persons identify a client, they need to cross-check the beneficial owner information with the information in the Transparency Register and if the information does not match, they are obligated to report this to the operator of the Transparency Register. This new tool will increase the detection risk for false or missing reports.

In early 2021, the Government presented a draft to the German Parliament to make a significant conceptual change to the information contained in the Transparency Register. The current approach under which companies and other associations do not have to make a filing to the Transparency Register if the beneficial owner is visible from other publicly accessible registers has lead to confusion and chaos: For example it remains unclear whether the lack of an entry for a specific company means that the beneficial owner information could be retrieved from other register (eg. because the managers are considered the "fictitious UBOs" or whether companies had simply failed to comply with their filing obligations. The current German approach also creates an obstacle for interlinking the various UBO registers at European level. Under the proposed law, each German company and association would have to submit UBO information to the Transparency Register, even if this information can already be gathered from other public registers. Certain further measures will also be taken with this proposed law, such as better access to account data from banks to comply with the Financial Information Directive (Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences).

Currently, enforcement of AML obligations in the financial sector is in the hands of national authorities. Recent cases of cross-border money laundering which involved foreign branches of banks have shown that national supervision has its limits. Consequently, there are plans at the EU level to create a European supervisory authority to improve the supervision and enforcement of AML obligations across borders in the EU.

From a criminal law perspective, the scope of the money laundering prohibition has considerably been expanded by the elimination of the predicate offence catalogue. For companies this means that should criminal offences be established in the course of an internal investigations, the company must closely examine whether individual assets obtained as a result of these offences might be suitable money laundering objects which should therefore be isolated and ring-fenced from other assets. Overall, companies should assume that German enforcement authorities will have to initiate more criminal proceedings into alleged money laundering offences than in the past. Whether such allegations may then be upheld by the authorities remains to be seen. It is not unlikely, however, that allegations will often lack the necessary proof of intent.

**Dr. Manuel Lorenz, LL.M.**
Partner

+49 69 2 99 08 506
Manuel.Lorenz@bakermckenzie.com

**Dr. Anika Schürmann, LL.M.**
Counsel

+49 211 3 11 16 128
Anika.Schürmann@bakermckenzie.com

5.0

# Data Protection

Dr. Holger Lutz, LL.M. and Dr. Michaela Nebel

Compliance and internal investigations typically come along with the processing of personal data at various stages, e.g. if a company operates a whistleblowing scheme in order to detect misconduct within the company or in case of a suspicion that an employee committed a criminal offence and the company wants to review emails of that suspect in order to further investigate the suspicion.

It goes without saying, that also in these particular cases, German companies must comply with the General Data Protection Regulation ("GDPR") and the Federal Data Protection Act ("FDPA"). The below outlines some general data protection law considerations regarding internal investigations (A.) and whistleblowing schemes (B.), as well as developments in 2020 in this regard and an outlook (C.).

## Processing of personal data in connection with internal investigations

### Is there a statutory permission?

The question on whether a statutory permission applies must be assessed on a case-by-case basis. Regarding personal data of employees, the following statutory justifications are typically relevant in connection with internal investigations:

- Pursuant to Sec. 26 para. 1 sentence 2 FDPA "employees' personal data may be processed to detect crimes, if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason." Although at first sight, this legal basis seems to fit to internal investigations, the scope of this legal basis is quite narrow and it is in practice typically of minor relevance.

- In case of a serious contractual violation, a company may be able to rely on Sec. 26 para. 1 sentence 1 FDPA, i.e. "for carrying out or terminating the employment contract".

- In many cases companies will rely on Art. 6 para. 1 lit. f GDPR which allows for a processing of personal data "if and to the extent the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (...)". This statutory permission requires a balancing of interests between the interests of the company and the interests of the data subject, such as the suspect. Although the balancing test conveys legal uncertainty, this statutory permission is quite relevant in practice.

In any case, companies must check, whether the processing of personal data is "necessary" ("data minimization") and "proportionate".

### Could companies also rely on consent?

Consent might also be an option. However, a company that wants to carry out data processing activities in connection with internal investigations, such as an email review, must carefully consider beforehand, whether to obtain consent of the respective employee(s):

- In case the employee already cooperated and indicated to further cooperate, obtaining consent might be feasible. However, there is a risk that consent is deemed invalid in the employment relationship, because consent in the employment relationship generally raises doubts as to whether it is freely given.

- If the employee refuses consent or withdraws consent, asking for consent may also be counterproductive: In such case, the company cannot/can no longer rely on consent. Even more so, relying on another legal basis as a fallback-solution very likely does not work, since the data protection authorities are of the opinion that the legal basis must generally be established prior to the processing activity, i.e. a company cannot swap from consent to another legal basis.

### Is it required to inform data subjects involved?

The transparency requirement is one of the processing principles of the GDPR. Thus, in general, data subjects must be informed about the processing of their personal data pursuant to Art. 13/14 GDPR, unless an exception applies.

The GDPR and the FDPA provide for a few exceptions from the requirement to inform, e.g. in case (i) providing information about the planned further use would interfere with the establishment, exercise or defence of legal claims, and the company's interests in not providing the information outweigh the interests of the data subject, (ii) if providing information about the planned further use endangered a confidential transfer of data to public bodies, or (iii) if meeting this obligation disclosed information which by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. However, the scope of the exceptions is rather narrow. It must be assessed on a case-by-case basis (e.g. towards every involved data subject), whether an exception applies.

### What else must typically be considered in internal investigations?

**Are employees permitted to use company IT systems for private purposes?**

In case a company has permitted its employees to use email or IT systems for private purposes (to a limited extent), additional issues need to be taken into account:

- Pursuant to the (still) prevailing opinion under German law, a company permitting its employees the private use of the company's IT and communication systems qualifies as a provider of telecommunication services. To the extent the emails and information reviewed are protected by the telecommunication secrecy, it is in principle prohibited to access and review the emails/information. In order to mitigate the risk of a breach of the telecommunications secrecy, a waiver of the telecommunications secrecy/consent may be obtained. In the employment context, there is, however, a risk that a consent given by an employee is deemed to be invalid.

- If IT systems are used for private purposes, it is likely that data to be reviewed during an investigation also contains sensitive personal data. The processing of sensitive personal data is subject to further requirements and permitted in very limited cases only.

**Are third party processors involved?**

If a company involves a third party service provider in the EU/EEA with the investigation, e.g. regarding the imaging of hard disks or/and reviewing emails, it is often required to conclude a data processing agreement pursuant to Art. 28 GDPR with the respective third party.

In case such third party service provider is located outside of the EU/EEA and outside a country that the European Commission has regarded as providing an adequate level of data protection (such as Japan or Argentina), the requirements for international data transfers must also be complied with, e.g. Standard Contractual Clauses must be concluded and potentially supplementary measures must be taken.

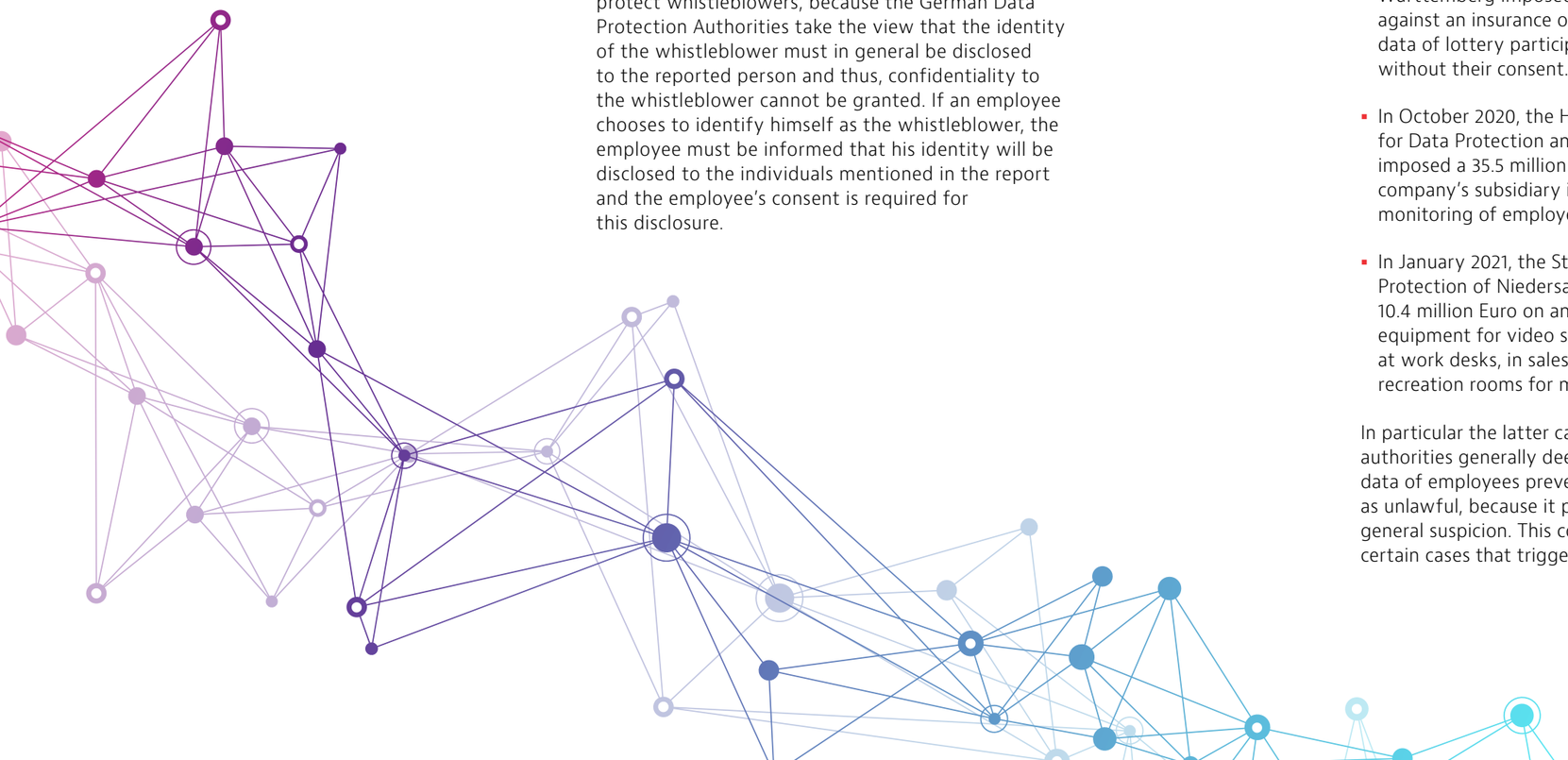
5.0

**Other considerations to mitigate the risks of a violation of German data protection law**
In addition to the above requirements, companies should, for example, also consider the following, in order to mitigate risks of a violation of German data protection law: (i) involving the company's data protection officer, (ii) carrying out a data protection impact assessment, and (iii) limiting the number of persons involved in the processing activities and ensuring that they are committed to confidentiality/ the data secrecy. Depending on the individual circumstances, additional mitigating measures may be advisable.

## Whistleblowing Schemes

Internal investigations are often triggered via whistleblowing schemes, e.g. hotlines or online intake forms. When setting up whistleblowing schemes, it is prudent to comply with the guidelines on whistleblowing published by the Art. 29 Working Party in 2006 as well as with the guidance issued by the German Data Protection Authorities in January 2018. Both take a rather narrow approach regarding the types of misconduct that may be reported via a whistleblowing scheme: (1) behavior that infringes a criminal provision, that protects business interests, such as fraud in respect of accounting or auditing practices or insider trading, and (2) behavior that violates human rights or environmental interests. Behavior that is merely in non-compliance with internal codes of conduct may generally not be reported.

In this regard it should be noted that the guidance issued by the German Data Protection Authorities in January 2018 significantly deviates from previous guidance: it encourages anonymous reporting to protect whistleblowers, because the German Data Protection Authorities take the view that the identity of the whistleblower must in general be disclosed to the reported person and thus, confidentiality to the whistleblower cannot be granted. If an employee chooses to identify himself as the whistleblower, the employee must be informed that his identity will be disclosed to the individuals mentioned in the report and the employee's consent is required for this disclosure.



## Developments in 2020 and outlook

### Enforcement actions with high fines

In 2020 and early 2021 the German data protection authorities continued to impose several high fines. Following the fine of the Berlin Commissioner for Data Protection and Freedom of Information in October 2019, who imposed a fine of 14.5 million Euro against a real estate company for violating data retention requirements, and the fine of the Federal State Data Protection Commissioner, who imposed a fine of 9.5 million Euro against a telecommunication company for insufficient authentication procedures in the customer call center, the Regional Court of Bonn significantly reduced the fine of the Federal State Data Protection Commissioner to EUR 900,000 (judgement of November 11, 2020, file number 29 OWi 1/20). However, the following high fines have also been imposed:

- In June 2020, the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg imposed a fine of 1.2 million Euro against an insurance organisation for using personal data of lottery participants for advertising purposes without their consent.
- In October 2020, the Hamburg Commissioner for Data Protection and Freedom of Information imposed a 35.5 million Euro fine on a global fashion company's subsidiary in Germany for comprehensive monitoring of employees.
- In January 2021, the State Commissioner for Data Protection of Niedersachsen imposed a fine of 10.4 million Euro on an online shop for electronic equipment for video surveillance of its employees at work desks, in salesrooms, the warehouse and recreation rooms for more than two years.

In particular the latter case shows that data protection authorities generally deem a collection of personal data of employees preventively without a suspicion as unlawful, because it puts every employee under general suspicion. This could in particular be relevant in certain cases that trigger internal investigations.

### International data transfers

There were a number noteworthy developments regarding international data transfers in 2020 which may also impact internal investigations and/or whistleblowing schemes.

- In July 2020, the Court of Justice of the European Union ruled in its so called "Schrems II" decision (July 16, 2020, C-311/18) that the EU Commission decision regarding the EU-U.S. Privacy Shield is invalid and that the EU-U.S. Privacy Shield can no longer be used as a transfer mechanism to the US. The Court of Justice of the European Union further ruled that the EU Commission decision regarding standard contractual clauses remains valid, however, the data exporter and the data importer must assess in the individual case, whether supplementary measures are required.
- In November 2020, the European Data Protection Board published two guidelines concerning the Schrems II decision, containing information on (i) what steps companies need to take before transferring personal data outside of the EU/EEA, (ii) examples for supplementary measures, and (iii) what to consider, when assessing the laws of a "third country" (i.e. a country outside of the EU/EEA and a country for that the European Commission has not issued an adequacy decision).
- Also, in November 2020, the European Commission published a draft of updated standard contractual clauses. Once the updated standard contractual clauses are finalized, it is expected that companies must use the updated versions going forward and that companies have a grace period to replace standard contractual clauses that were already concluded before that date.

Since the exceptions of Art. 49 GDPR remain unaffected by the Schrems II decision and its interpretation of the European Data Protection Board, explicit consent, where feasible, could provide for an alternative to justify an international data transfer, if any, in connection with internal investigations.

5.0

### Case law on right of access

The scope of the right of access is still debated in Germany. There were a number of decisions on the scope of the right of access that were not related to internal investigations. For example, the Regional Court of Heidelberg (judgement of February 6, 2020 - file number 4 O 6/10) denied a claim of a former board member against his former employer to provide copies of email correspondence, whereas the Regional Court of Cologne (judgement of November, 11 2020 – file number 23 O 172/19) ruled that an individual has a right of access to all personal data relating to him/her against his/her insurer, including conversation notes and call memos.

According to a press release from September 2020, the case concerning the scope of the right of access in connection with whistleblowing and internal investigations that triggered the decision of the State Labour Court of Baden-Württemberg on December 20, 2018 has been settled. In that case an employee exercised his right of access and requested data resulting from internal investigations initiated via the internal whistleblowing scheme. The court ruled that the secrecy of the source of information may generally constitute a legitimate interest, if the employer has granted anonymity to its whistleblowers. However, the court further ruled that it is not sufficient that the company makes a general reference to the need for protection of whistleblowers, instead, the court requires that the company outlines the related facts, the incident, the topic in terms of time and location, and the acting persons in that regard.

Thus, it remains to be seen which view becomes established case law in Germany.

### New whistleblowing legislation

Regarding whistleblowing schemes it is expected that Germany will have specific whistleblowing legislation in the near future. According to press releases in December 2020, the Federal Ministry of Justice already presented a draft implementation act for Germany. On December 16, 2019, the so called "Whistleblowing Directive" entered into force. It intends to strengthen the protection of whistleblowers against retaliation. Member States have two years to implement the Whistleblowing Directive into national law, i.e. until December 17, 2021. Pursuant to the Whistleblowing Directive, the requirements of the GDPR remain unaffected. It is currently unclear, how the requirements of the GDPR, in particular, in light of the interpretation of the German Data Protection Authorities, will be aligned with the protection of whistleblowers granted under the Whistleblowing Directive. As mentioned above, the German Data Protection Authorities are of the opinion that there is generally a disclosure obligation regarding the identity of the whistleblower which contradicts the confidentiality obligation under the Whistleblowing Directive and potentially also the implementation act in Germany.


**Dr. Holger Lutz, LL.M.**
Partner
+49 69 2 99 08 508
Holger.Lutz@bakermckenzie.com

**Dr. Michaela Nebel**
Partner
+49 69 2 99 08 368
Michaela.Nebel@bakermckenzie.com




6.0

# Labour Law - False Employment

Dr. Steffen Scheuer

The need for flexibility, effective cost management and a trend to manage daily operations on a project-by-project basis continues to create high demand for external staff. Simultaneously, the talent pool for highly qualified employees - in particular in the IT environment - still falls short of the increasing demand.

At the same time, the legislator and law enforcement have taken steps to fight misclassification and illegal labour leasing. The notion being that such relationships create a class of individuals unprotected by employment laws and social security and further deprive the government of social security contributions.

The simultaneous increase in demand and law enforcement require a well-thought-through strategy and intelligent concepts. The lack of a compliance organization controlling the use of freelancers or other external staff can result in substantial economic and legal risks.
In addition to back pay obligations regarding social security contributions and wage tax as well as severe fines, managing directors, board members and other executives may also face criminal consequences.

Having a powerful compliance system in place is therefore essential.

6.0

# False self-employment

Whether the use of external staff results in false self-employment or illegal labour leasing depends on the individual case. Unfortunately, it is often difficult to reliably assess the correct classification. According to case law, whether an occupation is carried out on an employed or self-employed basis is decided within the framework of an overall assessment. (BSG, dec. of 29.8.2012 - B 12 KR 25/10 R, NZA-RR 2013, 252)

In the case of false self-employment or illegal labour leasing, there is a risk under labour law of a fully effective employment relationship.

## Criteria

A false self-employment resulting in an undesired employment relationship is deemed to exist if the contractual agreement provides for the obligation to perform work in personal dependence, subject to instructions and supervised by the employer.

The contractual arrangement and description of the activities in the contract is one important piece of classifying the contractual relationship, but not the decisive element. Rather, what is decisive is how the contractual relationship is implemented in practice (Sec. 611a para. 1 s. 6 of the German Civil Code). (BAG, dec. of 27.6.2017 - 9 AZR 851/16, NZA 2017, 1463)

Freelancers are treated as employees if in the actual execution of their work certain criteria are fulfilled such as:

- integration of freelancer into the business unit of the customer (BSG, dec. of 9.12.2003 - B 7 AL 22/03, NZS 2004 548)
  - close collaboration with employees of the business unit
  - working together as team members of the employee;
- working on-site;
- using/working with operating material of the customer; (BAG, dec. of 31.03.2015 - B 12 KR 17/13 R, BeckRS 2015, 70638)
- remuneration per time and not per product; (LSG Baden-Württemberg, dec. of 30.7.2014 - L 5 R 3157/13, BeckRS 2014, 72689)
- giving or receiving instructions from employees of the customer; (BSG, dec. of 4. 6.2019 - B 12 KR 14/18 R, BeckRS 2019 25023);
- doing work which is usually done by the customer's employees; daily business work;
- freelancer is engaged because of capacity bottlenecks (such as seasonal demand, employees on sick or parental leave, interim position); work product of the freelancer cannot be distinguished from work product of the customer and/or its employees.

## Labour leasing

Not only the engagement of freelancers can have significant legal consequences for the company, but also illegal labour leasing (under certain circumstances even the same consequences).

In 2017, substantial changes to the existing legal framework regulating the use of temporary workers were enacted stipulating that temporary workers must be explicitly stated in the statements of work between customer and service provider. If the parties mistakenly believed that their arrangement is qualified as a service contract, but it turned out to be a labour lease contract, such contract is considered as an illegal agreement of the use of temporary workers. In order to determine, whether the contract between customer and service provider is a real service contract or a labour lease contract, the criteria mentioned under lit. a) apply accordingly, in particular, the integration of the personnel into the business unit of the customer.

In case of misclassification, the deployed personnel is deemed to be employed by the customer. Both service provider and customer are jointly liable for social security contributions and income tax (Sec. 28e Social Code IV (SGB IV)). If the individual worker was not engaged by the service provider as an employee, but as a self-employed subcontractor, the qualification as an employee under the Personnel Leasing Act (AÜG) has the same consequence for both the customer and service provider, as if one of them has hired him directly as a misclassified freelancer (Zieglmeier, NZS 2017, 321).

# Risks

There are significant risks associated with false self-employment or illegal labour leasing.

## Social security contributions, wage tax and late payment fees

Having used the services of a misclassified employee, the company must pay social security contributions and withhold wage tax for the future and also for the past. For illegal labour leasing this only applies, if the used personnel have not been engaged as employees (in this case, the service provider has usually withhold and paid income tax and social security contributions), but as freelancers.

For previous periods, late payment fines amounting to 1 per cent of the outstanding amount apply for each commenced month, Sec. 24 (1) Social Code and Sec. 240 of the German Fiscal Code (AO), BSG, dec. of 12.12.2018 - B 12 R 15/18 R, BeckRS 2018, 40201).

Depending on how many misclassified employees the company employed and over what period of time this occurred, the retrospective payments can jeopardise the liquidity or even the entire existence of the company.

If the company does not pay wage tax and social security contributions, managing directors, board members and other executives of the company may also be liable to prosecution. In particular if a company's business model or staffing practice depends on the use of (misclassified) freelancers, it is typically very difficult to convince a public prosecutor that management was unware of the issues and did not act intentionally.

6.0

### Input tax to value added tax (VAT)

In addition, if the freelancer was subject to payment of VAT, the company typically carried out an input tax deduction for VAT which retrospectively qualifies to have been unauthorized (Obenhaus, BB 2012 S. 1130). If this VAT deduction is not immediately corrected, this results in an oftentimes overlooked risk of criminal liability for tax evasion according to Sec. 370 of the German Fiscal Code (AO).

### Violation of the Temporary Employment Act

Depending on the violation of the law, these can amount to up to EUR 500,000 in the case of illegal labour leasing under the German Personnel Leasing Act (Sec. 16 para. 2 AÜG).

### Labour law: employment relationship, leave payment, protection against dismissal

In terms of labour law, there is a risk that an "unwanted" employment relationship may arise between the company and the external staff, including all employee rights such as protection against dismissal, entitlement to paid leave and continued payment of wages in the event of illness (BAG, dec. of 26.6.2019 - 5 AZR 178/18, NZA 2019, 1558).

## Solutions

In order to avoid such legal risks, a legally compliant concept for the use of external staff is nowadays a necessity for every company's internal compliance management.

### Status assessment procedure

One still widely applied means of avoiding misclassification risks the so-called "status assessment procedure" according to Sec. 7a Social Code IV (SGB IV) may be considered (BeckOK SozR/Rittweger, SGB IV § 7a Rn. 15 ff.).

The status assessment procedure is an official procedure offered by the German Pension Insurances Association which evaluates the status of a particular individual upon request and arrives with a binding assessment based on the facts the parties provided.

Whereas in 2007, the German Pension Insurance Association determined employment subject to social insurance in only 21.2 per cent of the cases examined in voluntary status assessment procedures, ten years later, in 2017, the rate has increased 40.3 per cent (vgl. BT-Drs. 18/11982; BT-Drs. 19/749 v. 14.02.2018).

Although the status assessment procedure is the "safest" solution to determine the status of the freelancer, the system is prone to contradictory decisions. Depending on the department or even the officer determining the status (freelancer or employee), the decisions may vary even if the underlying facts are virtually identical. The lack of predictability can leave companies in a dilemma: If one decision states that the freelancer is not self-employed, does this reasoning also apply to similar cases? And if this is the case: Does the managing director become liable for continuing business with freelancers doing the similar job? Such questions are difficult to answer and raise doubts about the reasonableness of this statutory concept.

### Compliance Concept

If - due to the lack of predictability - an employer does not make use of the status assessment procedure, it is in any case obliged to establish an equivalent (or even better) compliance management. An uncontrolled use of external staff by directs and departments is very risky, as the management cannot excuse missing compliance by saying that they have not been aware of any wrongdoings. The opposite is the case: Not implementing a robust compliance system is a serious breach of the management's statutory duties.

A comprehensive compliance system is therefore a must-have for companies: It enables them to meet the legal requirements. They keep the associated risks of false self-employment or illegal labour leasing as low as possible. The goal of a compliance system is to avoid legal violations, when using external staff and to protect against criminal liability should a legal violation occur.

Despite a compliance system, it happens in many cases that an external employee is accidentally integrated into a company. As long as this happens unintentionally and it can be proven that the compliance system is well implemented and functioning, this usually leads to lower penalties and no or only minor consequences under criminal law.

- Preventive measures that prevent legal violations

  In order to prevent legal violations when using external workforce, companies should introduce guidelines that apply to the entire company. External staff may not - like own employees - be employed and subject to directives or integrated into the company's operational organisation.

  A policy is only as effective as the employees comprehend it. Therefore, it is important to train all employees of a company who come into contact with external staff assignments with regard to the requirements of the guidelines.

- Measures that monitor whether the compliance system is being observed

  A compliance system can only be effective if its observance is also monitored. Otherwise it will not be able to withstand official audits. Regular, traceable controls are necessary. The monitoring measures should also be supplemented by a whistleblowing system that has been reviewed under data protection law.

- Measures to verify whether the compliance system is effective

  In the daily operation of a compliance system, it is important to permanently verify the effectiveness of the compliance system. This enables companies to identify gaps in the system as quickly as possible and take appropriate countermeasures. In order for this to be effective, the compliance department must be informed about the ongoing operations and the risk potential.

**Dr. Steffen Scheuer**
Partner

+49 89 5 52 38 241
Steffen.Scheuer@bakermckenzie.com

### In individual cases: Hybrid model (Rittweger, FS Plagemann, S. 210)

In individual cases, the so-called hybrid model can also be considered if the parties do not want to conclude an employment contract but at the same time want to avoid the legal risks of misclassification.

In this case, a free service contract is agreed upon and practised under labour law. Under social security law, on the other hand, it is assumed that the employment relationship is subject to social security contributions. For tax purposes, the employment relationship is treated as a self-employed activity.

This model combines the special features of the case law of the Federal Labour Court, the Federal Social Court and the Federal Fiscal Court. In fact, however, this model will only be considered for highly specialised professions.

## Conclusion

a) The use of misclassified freelancers or unlawful labour leasing is real and can be a threat to the company's existence.

b) The complexity involved with the appropriate use of freelancers requires a robust compliance system producing clear guidance to the business and is being continuously monitored.

c) If a company discovers potentially misclassified employees, it is necessary to investigate the matter and to rectify misclassified freelancers. "Looking the other way" can result in criminal liability.

7.0

# International Trade Law

Anahita Thoms, LL.M. and Alexander Ehrle, LL.M.

Over the course of the past year, globally operating companies with complex supply chains were subjected to a major stress test as a result of the COVID-19 pandemic. In light of the magnitude of the challenges not only stemming from the pandemic, but also Brexit and trade wars, global supply chains generally showed resilience. New export restrictions on, for example, protective gowns and medical equipment, as well as economic sanctions and a strengthened foreign investment review regime, show that German companies need to be on top of regulatory developments to ensure they comply with a set of continuously changing obligations governing their exports, trade transactions and foreign investments.

## What do companies need to look out for when exporting goods or technology?

- The COVID-19 pandemic has affected the regulatory framework for export controls directly. In spring 2020, during the first wave of the pandemic, the German Federal government issued an export ban on facemasks and other medical protective equipment encompassing all exports, even including deliveries to other EU countries. That initial ban was soon replaced by an EU Regulation prohibiting the export of medical gear to states outside of the EU. The ban was later lifted, but showed that the German government and EU institutions were quick to act and amend the regulatory framework for export controls in a situation of crisis. The enforcement of these provisions was also firm. Customs authorities initiated several investigations in cases in which they suspected infringements of the export ban. Violating an export ban is punishable by German law with high sanctions up to imprisonment of the exporting company's responsible employees and a fine for the company.

- Brexit also has significant implications for exports controls, since the UK now is considered a third country from an EU perspective. This means that deliveries to the UK are no longer regarded as transfers, but now qualify as export like it would to any other third country. This results in new licensing and authorization obligations. These changes are particularly relevant with respect to the export of dual-use items, certain firearms and related ammunition and reloading equipment, and goods covered by the EU anti-torture regulation, as well as trade and brokering transactions, and technical assistance, all of which are subject to licensing requirements under EU law. Furthermore, due to Brexit, export licenses granted by UK authorities for these types of transactions are no longer valid in other EU Member States. The transactions may therefore be subject to additional licensing requirements in the EU. Exports made without a required license qualify as unauthorized and may entail the liability of the individuals and corporations involved. This could result in significant sanctions such as monetary fines and imprisonment.

- There is no guarantee that the export control regimes of the EU and the UK will continue to be aligned. As a result of Brexit and the UK's autonomy over their foreign trade law, the structure and implementation of export licensing regimes are likely to change, possibly diverging from those under EU law. As the EU intends to reform its own export control regulations, it seems very likely that the relevant provisions in the UK and the EU will differ in the future. A proposal for such a reform at EU level has already been drafted.

- The EU has reached an agreement on a reform of the EU Dual-Use Regulation, which has in its current form essentially been in force since 2009. One of the central objectives of the reform efforts is to take human rights considerations into account in the regulatory framework. New criteria to be introduced are supposed to ensure that items likely to be used in violation of human rights, such as surveillance and intrusion technologies, are subject to heightened scrutiny and stronger export control restrictions. Other objectives are the reinforcement of cooperation between EU Member States through various improvements, the rationalization of the authorization regime and the introduction of new types of authorizations aimed at best serving the exporting industry's interests. Unauthorized exports are punishable under German law with up to five years in prison for the responsible individuals.

## Supply chain laws: Between corporate responsibility and liability risks

- The German government intends to introduce a supply chain law. Other European countries, e.g. France, have already introduced such laws. While both political parties in the Federal German government agree in principle on the adoption of such a law, there have been considerable differences regarding the scope and the design of liability clauses. The draft law both sides have agreed on is supposed to apply to companies with more than 3,000 employees. It does not contain a civil liability clause. Instead, companies failing to duly assess their supply chain are to be fined. While the exact wording and provisions of the draft law may still be changed before the law is passed, larger companies should nevertheless start preparations by scrutinizing their direct suppliers for human rights compliance, as this obligation will most likely be found in the German supply chain law.

- In addition to the German legislative initiative, the European Commission is planning to propose a similar law in the first half of 2021. The European Parliament has already passed a resolution that calls for civil liability of companies and demanding extended liability obligations not only to direct, but also to indirect suppliers along the supply chain. It can therefore be expected that the EU bill will include such provisions and exceed the scope of the prospective German law. However, it remains to be seen how the European law will hold companies accountable for the actions of indirect suppliers and what requirements will need to be fulfilled to avoid liability. Thus, we advise companies to closely follow the upcoming developments.

7.0

## Threat of violating sanctions regulations

- Multinational companies find themselves in a conflict between the US secondary sanctions regarding Iran and the EU blocking statute that prohibits EU companies from aligning with the extraterritorial US sanctions. A German regional court lodged a request for a preliminary ruling before the ECJ regarding a pending case between Deutsche Telekom and Bank Melli Iran for the termination of their contractual relationships due to the re-imposed US secondary sanctions. Deutsche Telekom had abruptly ended their services for Bank Melli Iran, as it feared violating the US secondary sanctions. The Bank Melli Iran consequently referred to the EU Blocking Regulation in their legal argument. The EU's plan to establish the special purpose vehicle INSTEX in order to facilitate trade between the EU and Iran has not been successful, as only one transaction has been carried out via INSTEX since the entity has been established in 2019.

- US secondary sanctions also remain a threat to companies working on completing the final parts of the Nord Stream 2 pipeline across the Baltic Sea, even though courts of EU Members States will not enforce those secondary sanctions. This was recently shown by a French court ruling in December 2020 deciding that US secondary sanctions do not form part of the French ordre public. The judgment reinforces the EU's opinion that US secondary sanctions violate both the sovereignty of EU Member States and international law because of their extraterritoriality.

- German companies need to keep in mind that exports from the UK are subject to the UK sanctions regime since 1 January 2021. This currently does not result in significant additional requirements for companies as the UK Sanctions Act simply incorporated the existing EU regimes into UK law. However, companies will have to be prepared to comply with possibly diverging UK sanctions in the future.

## Tightening of current foreign investment laws

- At the same time as restricting foreign trade by means of sanctions and export control regulations in order to preserve the world order and prevent human rights abuses, the EU also increases the scrutiny of foreign investments into the EU internal market. The EU Screening Regulation aims at protecting the EU and its Member States from negative impacts on their public order and security from foreign investments.

- The EU introduced a White Paper on Foreign Subsidies showing that it pays attention to various types of adverse external impacts on the EU internal market and that it deems it necessary to deter them from affecting the internal market.

### EU Screening Regulation

- The EU Screening Regulation entered into force on 11 October, 2020. In its current form, it provides a first step toward an EU-wide regulatory framework for the scrutiny of foreign investments. For the time being, the obligations provided for largely relate to the implementation of foreign investment scrutiny measures and standards at the domestic level and to the coordination on foreign investments between the EU Member States' authorities and the EU Commission. It can already be observed that Member States are reacting to the increased amount of shared information, resulting in slight delays in the handling of transaction reviews.

- Since the adoption of the EU Screening Regulation in 2019, Germany has made several changes focusing on strengthening and broadening its foreign investment review regime at the domestic level. The Foreign Trade and Payments Act (Außenwirtschaftsgesetz - AWG) as well as the Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung - AWV) have undergone several legislative amendments as a result. The changes include lowering the standard required for a formal review and for the imposition of restrictions on foreign investments from a threat to a presumable impact on the public order and security of Germany or another EU Member State. The catalog of industries and business segments considered particularly sensitive was extended. This trend is expected to be continued. In light of the COVID-19 pandemic, an amendment was made to the Foreign Trade and Payments Ordinance in 2020, adding companies to the list of sensitive businesses that develop or produce medical protective equipment, medicinal products and pharmaceuticals for the containment of highly infectious and life-threatening diseases, or in vitro diagnostic medical devices. The statutory limitation period in which the competent authorities can investigate a transaction if they subsequently become aware of it is five years. Moreover, transactions in sensitive sectors are subject to an enforcement prohibition until the German Ministry for Economic Affairs issues a clearance. A violation of this prohibition can be punished with up to five years of imprisonment.

### White Paper on Foreign Subsidies

- The European Commission adopted a White Paper suggesting instruments to contain the adverse impacts of foreign subsidies on the EU, the EU Member States and their economies. The White Paper identifies that foreign subsidies may have adverse impacts and may be used strategically by foreign powers in a way similar to foreign investments and calls for the adoption of new tools addressing the regulatory gap currently existing in this regard and dangers following from it. The White Paper could result in binding legislation introduced in 2021.

## Developments in international trade relations

Some of the EU's most important international trade relationships seemed particularly fragile in 2020 with a no-deal Brexit scenario only nearly avoided and US president Trump repeatedly threatening tariffs on European goods. However, in the end the EU's international trade relationships have risen to the new challenges and the EU remains a strong trade partner. In addition to achieving an agreement on a Brexit deal, the EU and China have concluded negotiations on an agreement on investment, the relationship with the new US administration is likely to improve, and the EU has continued trade talks with other large industrialized countries around the world.

### Brexit deal

- Shortly before the expiration of the transition period, the EU and UK managed to conclude a trade agreement. The EU-UK Trade and Cooperation Agreement prevents the establishment of a hard border between Ireland and Northern Ireland, as Northern Ireland remains in the European single market. Instead, the customs and regulatory frontier runs in the Irish Sea and goods are checked when being transported from Northern Ireland to the British mainland or vice versa.

### EU-China Agreement on Investment

- Regardless of the trade war between the US and China in 2020, the EU and China stayed committed to finding common ground for an agreement on trade and investment. In late December, they concluded the negotiations for a Comprehensive Agreement on Investment (CAI). The negotiators agreed on rules against the forced transfer of technology, obligations for the behavior of state-owned enterprises, comprehensive transparency rules for subsidies and commitments related to sustainable development. The agreement still needs to pass the European Council and European Parliament before entering into force.

7.0

### Other EU trade agreements

- The EU continues to be engaged in trade talks with other growing economies in Asia and South America. The free trade and investment protection agreement between the EU and Vietnam entered into force in 2020. This is especially advantageous for Germany as Vietnam's largest trading partner within the EU.

- Moreover, the EU and Mexico concluded negotiations for a new trade agreement, which is currently pending signature and ratification. Under the new agreement, practically all goods between the two states will be duty-free. The trade agreement also, inter alia, seeks to effectively implement the principle of sustainable development and the targets adopted in the Paris Climate Agreement.

## Conclusion

The regulatory landscape governing exports, foreign trade transactions and investments applicable to companies remains highly complex and dynamic in its development. Brexit has already shown, and will continue to do so, that German and EU companies, especially those having business in the UK, will have to make large efforts to adapt to the new situation, particularly regarding compliance with a possible new distinct legal framework. At the same time, the EU lowers direct and indirect barriers to international trade by negotiating trade instruments with several third countries and regions of the world finding common ground on trade standards. Companies in the EU will benefit from improved access to foreign markets. At the same time, they must continuously comply with an ever more complex framework of export control and sanctions laws. This task requires comprehensive compliance efforts and measures. The legal framework on foreign investments is also expected to expand in scope and strengthen in scrutiny at the EU level as well as domestically with further legislative proposals already underway. Companies should carefully consider all foreign investment law requirements when buying or selling shares in companies established in the EU. It is also important to be aware that violations of these requirements can result in significant penalties including imprisonment.

**Anahita Thoms, LL.M.**
Partner
+49 211 3 11 16 121
Anahita.Thoms@bakermckenzie.com

**Alexander Ehrle, LL.M.**
Associate
+49 (0) 30 2 20 02 81 626
Alexander.Ehrle@bakermckenzie.com

# Contacts


**Dr. Nicolai Behr**
Partner
+49 89 5 52 38 204
Nicolai.Behr@bakermckenzie.com

**Sina Buhl**
Associate
+49 89 5 52 38 208
Sina.Buhl@bakermckenzie.com

**Dr. Christian Burholt, LL.M.**
Partner
+49 30 2 20 02 81 756
Christian.Burholt@bakermckenzie.com

**Alexander Ehrle, LL.M.**
Associate
+49 (0) 30 2 20 02 81 626
Alexander.Ehrle@bakermckenzie.com

**Dominik Guttenberger**
Associate
+49 89 5 52 38 156
Dominik.Guttenberger@bakermckenzie.com

**Dr. Robin Haas, LL.M.**
Senior Associate
+49 89 5 52 38 273
Robin.Haas@bakermckenzie.com

**Dr. Nicolas Kredel, LL.M.**
Partner
+49 211 3 11 16 1327
Nicolas.Kredel@bakermckenzie.com

**Dr. Andreas C. Lohner**
Partner
+49 89 5 52 38 263
Andreas.Lohner@bakermckenzie.com

**Dr. Manuel Lorenz, LL.M.**
Partner
+49 69 2 99 08 506
Manuel.Lorenz@bakermckenzie.com

**Dr. Holger Lutz, LL.M.**
Partner
+49 69 2 99 08 508
Holger.Lutz@bakermckenzie.com

**Dr. Michaela Nebel**
Partner
+49 69 2 99 08 368
Michaela.Nebel@bakermckenzie.com

**Dr. Steffen Scheuer**
Partner
+49 89 5 52 38 241
Steffen.Scheuer@bakermckenzie.com

**Dr. Anika Schürmann, LL.M.**
Counsel
+49 211 3 11 16 128
Anika.Schürmann@bakermckenzie.com

**Anahita Thoms, LL.M.**
Partner
+49 211 3 11 16 121
Anahita.Thoms@bakermckenzie.com

## Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

**bakermckenzie.com**