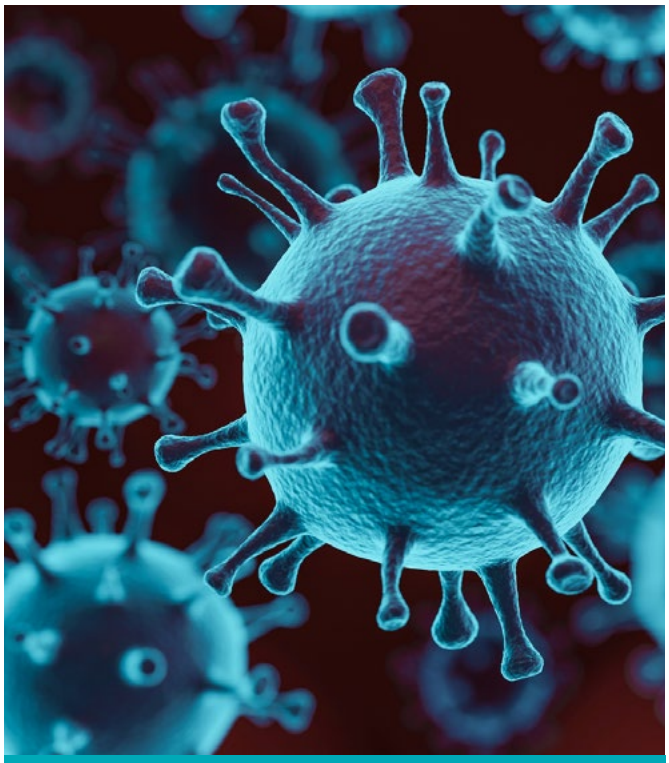
SQUIRE PATTON BOGGS

Coronavirus/COVID-19 Update

Legal Issues in Germany
13 March 2020



In Germany, we have received an increasing number of enquiries about the coronavirus disease 2019 (COVID-19), commonly known as the "coronavirus", and what organisations should be doing to mitigate the impact of the virus on their business, staff, supply chains, etc.

Here is an overview of the key legal issues for businesses in Germany to consider, together with some practical steps for businesses to take.

We will be running a webinar on this topic next week.

COVID-19 and the Costs of Contracts Under German Law

What Role Does "Force Majeure" play?

Although the term "force majeure" is usually a subject matter dealt with in international contracts, it is not found anywhere in the foundation of German contract law, i.e. the German Civil Code (BGB). With the spread of COVID-19, however, it is gaining importance, especially in the cross-border exchange of goods and services. Companies that are unable to fulfil their supply obligations due to restrictions caused by the virus must consider several important points if they intend to successfully invoke force majeure in order to avoid the costs resulting from any failure to comply with contracts that are governed by German law. These days, contractual agreements with insurers should also be examined closely, for example, if trade fairs or other major events, which were planning to be attended, are cancelled.

Applicable Law

As always with cross-border contracts, the most important question is what law applies. Contracts should always contain a choice of law clause in order to clarify this issue. Because Germany is a contracting member state, purchase contracts, which are governed by German law even without an express choice of law according to the rules of private international law, are also automatically subject to the applicability of the United Nations Convention on Contracts for the International Sale of Goods (CISG). Contracts that expressly provide for the applicability of German law, however, often contain an additional provision excluding the applicability of the CISG.

If the CISG applies, there are clear rules for cases of force majeure: According to Art. 79 CISG, a vendor is not liable for an impediment beyond its control. The vendor must prove that the conditions set out in Art. 79 CISG are fulfilled. In this respect, it is recognised that epidemics or the closure of transport routes can represent cases that fall under Art. 79 CISG.

National Legal Basis

If the CISG does not apply, cases of force majeure will be evaluated in Germany according to Section 275 BGB ("Exclusion of the Duty of Performance") or according to Section 313 BGB ("Interference with the Basis of the Transaction"). According to Section 275 BGB, the vendor is released from its duty to perform if the performance is impossible for it or any other person. The party liable may also refuse performance if the performance would require unreasonable efforts. Section 313 BGB provides that the vendor can demand an adjustment of the contract or – as a last resort – withdraw from the contract if circumstances, which became the basis of the contract, have changed to such a serious, unforeseeable extent that it cannot be reasonably expected to uphold the contract.

Force Majeure and Supply Chain Issues

Coronavirus as Force Majeure?

In which cases, therefore, does the coronavirus make the performance under the contract impossible or lead to circumstances under which it cannot be reasonably expected to uphold the contract? If, for example, the vendor's plant in China is closed by an official order, it can be assumed that these conditions are fulfilled in most cases. However, the situation is already different if the plant owner voluntarily decides to close the plant due to the current circumstances.

If a subcontractor of the vendor does not fulfil its supply obligations because it has to close its plant, the question arises for the vendor whether it is possible and reasonable to procure its supply from a different subcontractor. Even if this is associated with additional costs, the vendor will no longer be able to invoke force majeure successfully in many cases. The vendor must accept financial losses, i.e. additional costs due to higher prices, to a certain extent in order to fulfil its supply obligations. Depending on the form of the contract, there are, for example, conceivable constellations in which the vendor is obligated to keep a sufficient quantity of the goods to be delivered on stock in order to be able to bridge any supply bottlenecks for a certain period of time. Finally, the signed contracts should be reviewed again to determine whether they contain any contractual provisions on the duty to perform in the event of force majeure. If such provisions were agreed in general terms and conditions of business, the question is whether these provisions are effective. The conceivable constellations are numerous. Therefore, as is so often the case, the legal classification will depend on the individual case. It is generally recognised that plagues or epidemics can be classified as force majeure, as happened, for example, in the case of cholera or SARS.

Burden of Proof of the Vendor

Whoever wishes to invoke force majeure must prove its existence in the event of a dispute according to the basic rules of German procedural law. The hurdles that exist in this regard are high. First and foremost, the principle of "pacta sunt servanda" (Latin for "agreements must be kept") applies. Therefore, it is advisable to carefully document the relevant facts and make them "fit for court" early on. In addition, the vendor must be able to demonstrate that it made all reasonable efforts – even at the expense of economic losses – to fulfil its supply obligations in accordance with the contract.

What Should the Vendor's Customers Do?

First, customers should request that their vendors make all reasonable efforts to fulfil their supply obligations. What can be specifically demanded will depend on the individual case. If a remedy appears impossible or unreasonable, customers are well advised to inform their own customers of the impending delivery difficulties as early as possible and in a verifiable form. Otherwise, customers may be faced with an increased risk of recourse claims of their own customers. They will then be in the same situation of having to prove the existence of force majeure themselves or ensuring the delivery in another – potentially economically disadvantageous – way.

Event Cancellations

Who Provides Compensation for Damages if a Trade Fair Is Cancelled?

Insurance policies often do not cover losses due to infectious diseases, unless insurance protection has been explicitly agreed for such cases. Even in the case of an explicit agreement, the insurer may only step in if the trade fair or other event is cancelled by official order. However, if the majority of exhibitors withdraw their participation on their own initiative and the organiser cancels the trade fair in response, it will likely be questionable in many cases whether the insurer will cover the resulting damages, and if yes, to what extent. It is, therefore, essential to look at the insurance policy to assess the risks, especially since a number of insurers have been explicitly excluding coverage for damages caused by COVID-19 under certain conditions since the beginning of this year.

Employment

What Are an Employer's Health and Safety Obligations in Relation to Its Staff?

Employers should regularly obtain information on the current status of infection via the websites of public authorities (e.g. Federal Ministry of Health, Robert Koch Institute, Federal Centre for Health Education). Furthermore, the recommendations of the Robert Koch Institute on reducing the risk of infection with COVID-19 at the workplace should be implemented as far as possible and employees should be informed accordingly.

Where applicable, employers should also involve and seek the views of any elected works council in light of their co-determination rights.

Should Employers Place Restrictions on Work-Related International Travel?

If the employment contract contains an obligation for regular business trips, an instruction to travel is basically permitted. However, there are exceptions. If there is a travel warning from the Foreign Office for an entire country or a partial travel warning for a region, the trip can be refused by the employee.

It would be in the interest of most companies to reduce or refrain from travel to high-risk countries to keep the risks for their employees and operational processes as low as possible.

See the German Foreign Office website for the latest information on travel.

In What Circumstances Are Employees Required to Self-Isolate?

Sick employees normally receive an official sick note by a doctor that outlines the period during which the employee is unfit to work.

In cases of suspected infection, the public health authorities may order a ban.

Self-isolation should not be encouraged without advice from a doctor. Employees should visit a doctor or refer to the local branch of the public health department. An employee who self-isolates without medical advice (other than on the instruction of the employer) will not be entitled to be paid during that period.

Employees are obliged to report sick to the employer immediately. The type of illness does not usually have to be reported.

Because the coronavirus is a highly infectious and dangerous disease, the general duty of loyalty under labour law means that employees who are suffering from it should, and even must, exceptionally notify the type of illness, since only in this way can an employer take appropriate protective measures against the spread of the virus.

Do Employers Have to Pay an Employee if They Self-Isolate?

Sick employees normally receive continued payment of their wages by the employer for six weeks per sickness.

However, if there is only a suspicion or fear of infection, and the authorities order a ban on employment or a quarantine, they have no right to continued payment of wages. Instead, employees receive compensation from the state. Although the employer must pay this to staff, it will be reimbursed by the responsible health authority. This is laid down in the Protection Against Infection Act.

How Should Employers Deal With a Member of Staff Who Refuses to Come to Work Because They Are Concerned About the Risk of Infection?

Fear and concerns alone are not enough. If there is no concrete evidence of possible infection, employees must come to the office for the most part. An exception would be if an employer makes an agreement with its employees to work from home.

In cases where it is suspected that an employee is infected with the coronavirus and there is a concrete risk of infection, the employee may work from home. A unilateral instruction to work from home by the employer is not permitted; such measures must always be accepted by both parties, unless agreed otherwise. Employers may instruct employees to stay at home, but must release them from their work duties in cases of doubt.

If an employee refuses to attend work for fear of infection, even though there is no objective basis for fear of infection, employers may first give a warning and, if this happens again, dismiss the employee for conduct-related reasons.

If Staff Say They Want to Wear Facemasks at Work, Are Employers Entitled to Say No?

Employers have a right to direct/issue instructions.

Before refusing an employee consent to wear a mask at work (see France), employers should have taken reasonable steps to persuade the employee of the disadvantages/pointlessness of doing so; but ultimately, such a refusal does fall within the employer's powers of direction.

What Should Employers Do if a Member of Staff Is Confirmed As Having the Virus and Has Recently Been in the Workplace?

Close co-operation with the public health department is strongly recommended.

Furthermore, protective measures should be taken for the rest of the workforce. If other employees report virus symptoms, such as fever, coughs, colds, etc., the employer should send them home and direct them to obtain a medical going one way or the other.

Data protection laws should not be forgotten. Collecting health data from employees, for example, by measuring possible fever when entering company premises, is not admissible without consent. The same applies to informing third parties (particularly other employees, clients and customers) of a possible infection. It remains to be seen how easily employers can reconcile their duties of confidentiality to the (potentially) infected employee with their duties to other colleagues who may have come into contact with them. The employer should refer to the public health department when in doubt.

If the Situation Worsens and Employers Are Considering Closing One of Their Sites, Do Employers Have a Right to Lay Off Staff in These Circumstances? Are Employers Obliged to Continue to Pay Staff?

There are two different situations. If a company closes down as a temporary precautionary measure to protect its employees, then the employer also bears the financial risk. The employees must still be paid.

The situation is different if the company is ordered to close down by the health authorities. Then, in turn, general state compensation regulations take effect. In addition to the above, there is the possibility for an employer to apply for shorttime work (e.g. in case of delays in the supply or production chain due to the virus).

In this case, no "forced vacation" has to be taken because if the employer closes the company on its own initiative and the employee cannot come to work, then the employer is responsible. Employees do not have to take leave for this.

For layoffs, the general principles for redundancy situations apply. A virus outbreak itself will not be sufficient for a layoff. A restructuring due to a materially impacted economic situation in the business, by contrast, may be a sufficient reason for business-related termination.

Data Protection

Home Office

- The spread of the virus has already led to a significant increase in the desire of employers and employees to have options to work from home.
- The data privacy and data security requirements in a home office are generally no different than the requirements at a time when there is "no crisis." However, challenges arise from the request to quickly set up a home office in response to the (COVID-19) crisis, even for those employees who previously only had a stationary place of work. In the case of great time pressure, even smart phones or tablets might, therefore, need to be used on a transitional basis. It should thereby be ensured that suitable apps are used to avoid the undesirable mixing of private and business data under data protection law.
- The same applies if, for example, the private hardware of employees is used (temporarily) due to the lead time required for procuring mobile home office software. Access using virtualization applications (e.g. Citrix) via a remote desktop or VPN Tunnel are also options. A clear "no go" from a data protection standpoint is the (even temporary) use of a private email account of employees.
- The top priority is a clear technical separation between private and business use. Otherwise, the data protection compliance and IT security of the company could be affected by the data collection or security problems caused by private use on the private home network of the employee. If private devices of employees are (or must be) connected, it is strongly recommended to verify their basic security (virus protection, newest versions of security applications, etc.) according to the requirements of the company. If necessary, this can take place remotely using (mobile) device management applications.
- Data protection should also be ensured through clear home office policies. Even those employees who have not been affected up to now must be trained (if necessary, ad hoc) on data privacy and data security, the use of passwords even in a home office, screensavers for the remote desktop, etc.

- Caution: Hastily sending employees to work from home can cause known privacy and security risks associated with the use of USB sticks. The same applies here – data privacy by policy, use of personal data only within the (VPN) secure area, and no giving or taking of personal data by employees on USB sticks to a home office.

Employee Data

- From a data protection perspective, because the coronavirus is a highly contagious disease, it can be justified – on the basis of employment law (duty of loyalty) – that employees, as an exception, should or even must provide notification of the nature of their illness. The employer will be able to take appropriate protective measures against the spread of the virus at its establishment only on this basis.
- This could quickly result in large quantities of personal or personally identifiable data, with and without reference to health or the (physical) location of an employee in an area of risk. The format for collecting the data is generally irrelevant. Personal data, therefore, exists regardless of whether the employee submits a questionnaire, volunteers information or is questioned in person, e.g. by supervisors or HR employees.
- In the case of employee data, the handling of such data for the purposes of the employment relationship is only permitted if this is necessary for the employer in order to exercise rights or fulfill its legal obligations under employment law, social security law or social protection law. Specifically, this can be difficult and raises many problems when making differentiations. What may be unproblematic in the case of confirmed contact of an employee with an infected person or even in the case of a positive COVID-19 test of the employee, can look completely different in the case of groundlessly requesting health data from a large number of employees.
- In difficult times, companies need clarity. For entirely trivial, straightforward information, such as "employee X was once in northern Italy," the processing could take place from a practical standpoint, even with a personal reference, for the purposes of the "elementary" justified interests of the company in the individual case.
- Until it has been clarified how to handle the new "corona data" and until at least the supervisory authorities have taken a position, caution is recommended. This applies above all for the access to data collected in such way, especially data related to health (authorization concept) and its retention. Proven methods, such as pseudonymisation (where possible), and strict retention schedules are recommended.
- On the other hand, the technically possible collection of GPS-supported data on the whereabouts of employees by tracking smart phones and other mobile end devices should not take place. There is no identifiable legal basis for this, at least for companies in relation to their employees. In addition, they would be breaching the transparency requirement under data protection law if this takes place without the knowledge of the employee.
- Due to the gains in terms of certainty under data protection law, it may be appropriate to make separate works agreements on protection against infection. The agreements could form the legal basis for the handling of the data if they meet privacy requirements. Unlike legislative measures or the positioning of supervisory authorities, such agreements can be quickly implemented by parties. Works agreements may be invalid in the case of serious data privacy breaches. However, the parties have a wide margin of discretion in this regard. It terms of data protection, it is important that the works council is also and precisely responsible for safeguarding the personal rights of the employees.

Concrete Operational Measures, in Particular, Entry Controls and Health Checks

- Preventative measures for entry control (combined locks/scanners/thermal imaging camera systems) result in large amounts of personal data. This applies both for employees and for other visitors. The personal reference intensifies if, in suspected cases, for example, an elevated body temperature is manually "re-measured" by the plant security team. Because these measures in relation to the individual concerned appear groundless, this type of data collection is particularly critical.
- Even if no "re-measurements" are taken by the plant security team, a comparison with other data can usually take place, which the company has access to (e.g. card readers, video surveillance with biometric functions, time sheet records, etc.). Based on a practical and realistic point of view, the better arguments are in favor of a personal reference.
- In view of the current doubts of experts as to the informative value of measuring body temperature for containing COVID-19 infections in general (e.g. usually no elevated temperature during the incubation period and many mild cases entirely without a fever), the doubts prevail at present, even with respect to employees, whether the necessity

required to justify temperature controls under employee data protection rules even exists. Furthermore, due to the close proximity to personal rights, there will likely be tangible and often overriding opposing interests of the employees concerned to be spared from "mandatory measurements." Even individual guidelines of the public authorities are not likely to change this in principle.

- This also applies, in particular, for the fact that, under data protection law, such measures may only be performed by (company) medical staff, who, unlike the plant security team, must comply with medical confidentiality.
- The company's options with respect to suppliers, external companies and their members, and other visitors to the business premises are even more limited than in the case of employees. In this regard, the special provisions of employee data protection law naturally do not apply. With respect to third-party visitors, the nature of the data as health data is primarily problematic under data protection law. At present, it appears unrealistic that company entry controls with groundless temperature checks for visitors are permissible, according to the strict exceptions that apply under general data protection law.
- The only possible legal basis for collecting personal data is, therefore, the consent of the data subject. However, such consent is only legally valid if it is given voluntarily. Therefore, it appears problematic for both groups of persons concerned. For employees, their limited negotiating power often opposes the voluntariness. For other visitors, access to the company's premises by consenting to a temperature measurement is typically a passage requirement in order to get to the business premises. For both groups, therefore, solving the problem with consent of the individual does not appear expedient or advisable from today's perspective.
- In the short term, it will make sense to make oral inquiries without collecting any data in those places where controls appear indispensable or provide notification through appropriate posters in the access area that visitors, for example, with typical cold symptoms, returning from risk areas or contact persons of infected persons are not allowed to enter the business premises.
- For employee controls, a works agreement could form the legal basis in the medium term. The concerns expressed recently in this regard with a sweeping reference to the health data are not convincing and are, above all, of no help in practice. Because the works council is also responsible for safeguarding the personal rights of the employees, one may correctly assume that, at least for employees, temperature controls can generally be agreed in the works agreements. This requires careful treatment of the affected personal rights of the employees.
- Even in times of a pandemic, the following applies: the highest principle of data protection is still the principle of prohibition with the reservation of permission or the principle of lawfulness under the GDPR. Everything that is not explicitly permitted is (and remains) prohibited. This particularly applies for health data. Data protection infringements can result in fines being imposed by the supervisory authorities in the amount of up to €20 million or a maximum of 4% of the group's worldwide annual turnover of the prior financial year. It is, therefore, advisable to proceed prudently and, if necessary and possible, in coordination with the competent supervisory authorities.

Further Updates

We will continue to monitor the situation carefully and keep this advice note under review. We have also set up a dedicated resource centre for businesses on the legal, regulatory and commercial implications of coronavirus COVID-19 on our website: https://www.squirepattonboggs.com/en/services/key-issues/coronavirus-covid19

This is to provide you with the very latest guidance on the practical steps to take, given that the situation is an evolving one and the government and health authorities' guidance and advice may well change.

If you would like to discuss any of the issues raised in this advice note, please contact any of our team listed below.

Key websites/sources of guidance

Robert Koch Institute Risk Analysis:
https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Risikobewertung.html

Robert Koch Institute FAQ:
https://www.rki.de/SharedDocs/FAQ/NCOV2019/FAQ_Liste.html

Foreign Ministry Travel Advice:
https://www.auswaertiges-amt.de/de/ReiseUndSicherheit/10.2.8Reisewarnungen

Federal Health Department:
https://www.bundesgesundheitsministerium.de/

Contacts

Horst Daniel
Partner, Frankfurt
T +49 69 1739 2432
E horst.daniel@squirepb.com

Jens Petry
Partner, Frankfurt
T +49 69 1739 2441
E jens.petry@squirepb.com

Tanja Weber
Partner, Berlin
T +49 30 72616 8206
E tanja.weber@squirepb.com

Alper Kaufer
Senior Associate, Frankfurt
T +49 69 1739 2443
E alper.kaufer@squirepb.com

Jörg Staudenmayer
Partner, Böblingen
T +49 7031 439 9632
E joerg.staudenmayer@squirepb.com