COVID-19 is disrupting supply chains worldwide, has rocked stock exchanges, and can lead to business closures being ordered as a result of quarantine measures. Even though the situation is developing very dynamically and reliable forecasts are difficult to make, it is important for all companies to prepare themselves for potential scenarios by means of goal-oriented crisis management, and thus to preserve the trust of their employees, business partners and customers.

But how do you guarantee goal-oriented crisis management? What is decisive for this is well-founded, efficient action, built on the following cornerstones:

- install a crisis team
- carry out an individual, ordered risk analysis
- use sound knowledge and professional expertise.

I. Crisis team:

In order to be able to act as efficiently and swiftly as possible, it is vital to form a crisis team. You should assign (not just invite) people in charge from all relevant departments to that crisis team. These are *inter alia* personnel, sales, marketing and finances. Schedule meetings (telephone conferences) at short regular intervals, in order to be able to react appropriately to the rapid developments.

Allocate powers! Who issues invitations? Who may inform the employees, customers and/or suppliers? And definitely avoid conflicts of interest! Such a conflict situation exists, for example, if the responsibility and monitoring for a subject area is allocated only to one person.

Document the crisis meetings! By doing so, you will have evidence that you have done everything conceivable in the circumstances to manage the crisis. Afterwards, you will thus be able to prove fulfilment of your duties of care and avert administrative fines or recourse claims. At the same time, you will be ensuring that if members of the crisis team are absent due to illness, new members can be seamlessly brought in to carry out their predecessors’ activity.

II. Risk analysis:

The crisis team should conduct an individual risk analysis at the beginning of its activity. The risk analysis will assist you in a structured manner to identify what has to be done and what measures are essential, and when, and what risks there respectively are.

The creation of a risk table has proven itself in practice here. Our organisation consultants recommend ideally a classification of the risks into four levels (low, medium, high, and very high). Of course you can use more levels here in the framework of your analysis, but this tends to make the risk analysis disproportionately more complex. It's better to think in simple, good and easily-comprehensible structures. We set out below a risk table as an illustration of a possible layout:

Risk level	When does this level apply?	Gravity and probability of the impacts for your company	Measures which you have provided for in this respect	Communication which you effect in this respect
Low	▪ Latent threat ▪ No cases of the infection at the company or in the neighbourhood	Low to insignificant impacts, but high probability	Preventative measures, e.g. ▪ hygiene plans ▪ procurement of disinfectants ▪ recommendation to postpone business trips and events with larger numbers of attendants ▪ preparing the IT infrastructure for decentralised work	▪ Hygiene training for all employees ▪ Putting up instructions
Medium	Suspected cases or infection cases in the direct vicinity of the company or company employees.	Noticeable effects, increasing probability in the course of the proliferation in the population.	▪ Prohibition against business trips ▪ Personnel crisis plan: spatial/temporal separation of shifts/teams/groups ▪ Where applicable, special prevention for key personnel ▪ IT crisis plan ▪ Cancellation of events	▪ Explanation to the employees about the spreading and risks of the infection ▪ Appeal for protection of vulnerable people ▪ Obligation to comply with all prevention measures
High	Suspected cases or infection cases at the company. Closure of departments or shutdown of individual departments, whose activities can be covered by someone else, however.	High impacts – low probability (to be regularly reassessed).	▪ Ordering home office work ▪ Implementation of personnel crisis plan and IT crisis plan ▪ Information about state aid and other financial stabilisation measures	▪ Communication to all relevant stakeholder groups
Very high	Shutdown of production or parts thereof which cannot be covered by others.	Existential impacts, very low probability (to be regularly reassessed).	▪ Activation of state aid, insurance policies ▪ Personnel measures	▪ Communication to all relevant stakeholder groups ▪ Where applicable, communication to the press

Note: the measures outlined are to be defined depending on the company, and are only given as examples.

III. Knowledge – make use of expert know-how, notifications by public bodies, etc.

Don’t reinvent the wheel in this crisis situation – use the following as sources of knowledge:

- notifications by public bodies, such as the Federal Government, the states, recommendations issued by the Federal and state offices, etc.,
- the expertise of your employees/external advisors (e.g. data protection officers, IT security officers), and
- obtain expert advice on individual issues if needed.

The following information is intended to offer you a first overview of individual sources of knowledge and subject areas, but makes no claim of completeness. Particularly in light of the sources given and notifications made by public bodies, new ones are being added daily; we are endeavouring to update this regularly. Legal topics can only be noted here – please see the recommendations made by your legal advisors. You can find information about employment-law issues **here**.

1. Announcements made by public bodies - as of 18 March 2020:

Federal Republic of Germany	
German Federal Office of Civil Protection and Disaster Assistance	Handbook Company Pandemic Planning (Betriebliche Pandemieplanung)
BfDI – the Federal Commissioner for Data Protection and Information Security	Data protection-law information regarding the processing of personal data by employers in connection with the corona virus pandemic (Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie)
Data Protection Authority Baden-Württemberg	FAQs regarding the subject of the corona virus
Federal Minstry for Work and Social Affairs	Corona virus: employment-law impacts - FAQs

European Union and Other European States	
Denmark	
Datatilsynet	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/hvordan-er-det-med-gdpr-og-coronavirus/
Finland	
TT – Tietosuojavaltuutetun toimisto	https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-ja-koronaviruksen-leviamisen-hillitseminen
France	
CNIL - Commission Nationale de l’Informatique et des Libertés	Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles
Hungary	
NAIH - A Nemzeti Adatvédelmi és Információszabadság Hatóság	https://naih.hu/files/NAIH_2020_2586.pdf
Iceland	
PV – Persóna Vernd	https://www.personuvernd.is/personuvernd/frettir/covid-19-og-personuvernd
Ireland	
DPC – Data Protection Commission	Data Protection and COVID-19
Italy	
Garante per la protezione dei dati personali	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117

Luxembourg	
CNPD – Commission nationale pour la protection des données	https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html
Netherlands	
AP – Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/mijn-zieke-werknemer
Poland	
UODO – Urząd Ochrony Danych Osobowych	https://uodo.gov.pl/pl/138/1456
UK	
ICO – Information Commissioner’s Office	Data protection and coronavirus: what you need to know

2. Data protection-law information – as of 18 March 2020:

Data protection-law concerns arise particularly with regard to your employees. Here, always follow the principle that the employee should remain the “master” of their own data, even in crisis situations. This is even more the case because in this particular crisis health data will be involved to a high degree.

As a matter of principle, an employee does not have to provide their employer with any specific details about their own health. In suspected cases, however, there can be an obligation to have a medical examination carried out by a health authority. There can also be an obligation, due to returning from a trip or due to illnesses in personal vicinity, to provide information about places the employee has been or people the employee has had contact with, in order to enable you as the employer to assess health risks for the person affected and other employees.

Permissibility of processing employees’ health data

Whether it is permissible to process employees' health data or not is determined pursuant to Article 9 of the GDPR and Article 88 of the DSGV in conjunction with § 26.3 of the BDSG. Pursuant thereto, processing sensitive data such as health data for purposes of the employment relationship is permissible if *inter alia* this data is necessary for the fulfilment of the employer’s legal obligations arising out of employment law, and if there is no reason for assuming that the protection-worthy interest of the person affected in excluding the processing prevails.

The legal obligation consists here of fulfilling the provisions of § 618.1 of the BGB in conjunction with § 3 of the ArbSchG. In principle, an employer is obliged pursuant to the German Occupational Safety Act to appraise the risks to its employees’ safety and health in the workplace (so-called risk assessment) and to derive measures therefrom.

There is a conflict here: on the one hand, an employer must fulfil its duty of care by protecting the employees from infection, but on the other hand the employer may not breach the employees' data-protection and personal rights.

Whether a measure is permissible is determined authoritatively in this context pursuant to the criterion of necessity. In the framework of ascertaining the necessity for processing, the conflicting positions of employer and employee are to be weighed up. The employer’s interest in the processing must be carefully balanced with the employee’s personal right. This rather theoretical definition ultimately means that the interests of both parties must be weighed up, that the means for the goal being pursued must be suitable, and that no milder means with the same effect is available.

Something else to be borne in mind in this context is the principles of data protection law arising out of Article 5 of the GDPR. In particular, the principles of fairness and transparency pursuant to Article 5 paragraph 1 a of the GDPR as well as the principle of data minimisation pursuant to Article 5 paragraph 1 c of the GDPR come into effect in the framework of weighing interests up. Pursuant thereto, data processing must be foreseeable for the data subjects, they must be informed about the type and scope of the data processing, and the data processing must be limited to the minimum necessary to achieve the purpose pursued. If all of this is well-implemented, this has a positive influence on the weighing up in the framework of the necessity review.

What may you do? What not?

This is currently difficult to assess finally – things are happening so fast and there is not yet a unified policy by the European data protection supervisory authorities. For this reason, the following is only a provisional first appraisal:

Permissible measures	Impermissible measures
Collecting information whether an employee was in a risk area or has had direct contact with an ill person, e.g. asking people returning from holiday whether they were in a risk area	You may not specifically name a certain employee who has become ill with the virus to the employees, because knowledge that an employee has the corona virus can lead to enormous stigmatisation for that person. Instead, measures are to be taken in a department-related or team-related manner without specifically naming the person(s). Employees who have had direct contact with the infected person(s) should be warned and temporarily released from their obligation to perform work.
Upon request by the health authorities: transmission of data concerning ill employees, about employees who have been in risk areas or have had contact with infected people	General enquiries of all employees about travel destinations, particularly without specific indications or trips.
Collection of voluntary information or questionnaires regarding places people have been and regarding symptoms	General enquiries of all employees about their health status (e.g. about flu symptoms).
In the event of a positive finding regarding an employee (by an official body) or even in the event of confirmed contact with a person who has tested positive, information concerning the employee affected can be processed, e.g. the point in time and people they have had close contact with, as well as measures taken (see French data protection authority)	A registration obligation for employees if a co-worker shows symptoms (see Italian data protection authority).
With the employee’s consent: collection of the current private mobile telephone number(s) or other contact details for information about closure of the business or in similar cases (see handbook concerning company pandemic planning (*Betriebliche Pandemieplanung*) German Federal Office of Civil Protection and Disaster Assistance)	Employees having a mandatory temperature test at the entrance to business premises or similar medical measures (e.g. throat swabs for saliva tests). This measure might be permissible in individual cases => this requires the interests of all of the parties involved to be weighed up carefully.

3. Information regarding data and information security – as of 18 March 2020:

Check critically the risks of data and information security *inter alia* in connection with the following measures:

Measure	Remark
Home office	Set up VPN; use company equipment; home office/remote-working policy
Video conferences & co.	Selection of provider; any necessary agreement regarding order processing
Blocking access to sensitive areas	Permissible? Necessary? Possible?
Limiting access options	Permissible? Necessary? Possible?

4. Employment-law information – as of 18 March 2020:

You find information on employment law from TIGGES Rechtsanwälte **here**.

We are endeavouring to keep this information as current as possible. You will find the updates on our website at www.tigges-dco.de in the “News” section.

We would be pleased to assist you – please do not hesitate to contact us.

Your TIGGES DCO team!

TIGGES DCO GmbH
Zollhof 8 | 40221 Düsseldorf | Germany
info@tigges-dco.de