Briefing December 2020

Update: COVID-19 and its Privacy Implications

The exponential spread of COVID-19 has forced companies to take strict measures to prevent the spread of the virus and strike a balance between their duty of care and keeping their businesses running. This Bär & Karrer Briefing describes certain measures that companies have implemented during this pandemic, describes the implications that these measures have from a privacy perspective and provides guidelines on how to handle the current situation in a data protection compliant manner.

Measures Implemented by Companies Due to COVID-19

Employers have to walk a fine line between their duty of care, their employees' duty of loyalty, and keeping their businesses running. Certain companies have implemented, in particular, the following measures:

– Increased working from home.

– Return to work protocols including, for example, medical checks of their employees and the installation of thermographic cameras.

– Placing a duty on employees to report a COVID-19 infection or any contact with an infected person, for example, by encouraging employees to download the governmental COVID contact tracing app.

– Introducing a duty to report any travel abroad or even limiting travel to a certain extent.

Privacy Implications

General data protection implications

The potential measures taken all entail various privacy implications that must be considered – even during a pandemic.

To protect public health during these unusual circumstances, more health data is being processed than usual. This concerns not only public but also private institutions and employers. Health data is considered sensitive personal data under data protection law, and individuals must at least be informed of the processing at the point of collection of their health data. Consent may even be needed for certain processing activities, i.e. the disclosure of the data to third parties.

Working from Home

Increased working from home may have implications on data protection. While working, employees who may be processing personal data have to respect

data protection law and the company's privacy policies as well as IT security and professional secrecy, regardless of where they are working.

Risk of Illegitimate Employee Monitoring

However, there are certain specific considerations that apply to data protection when working from home. For example, the employer needs to be careful when applying measures to control their employees' working habits (e.g. the implementation of software or tools that take pictures of the employee during the workday or apps that control activities on the computer, i.e. by recording all key-strokes etc.), as such measures could be qualified as illegitimate employee monitoring. Any measure to monitor employees needs to be carefully assessed before its implementation for that reason.

Security Measures and Policies

There should be clear policies, procedures and guidance on the accessing, handling and disposing of personal data, established by the employer for staff who are working from home. Remote access solutions should be up to date, staff should be reminded to use unique and complex passwords, and where possible and practical, multi-factor authentication should be configured. Any remote access within Switzerland or from outside of Switzerland needs to be established through a secure connection, preferably using infrastructures of the employer via VPN or VMWare.

Specific safety concerns have to be addressed with cloud storage and potential attacks on remote desktops and with regard to the remote applications used.

Furthermore, the data protection of physical documents or work-related calls is also different: the employee must be aware that they ought to keep members from the household from seeing their work, their computer screen, or listening in on work-related calls.

Cross-Border Data Disclosures (Working from Abroad)

When employees use remote access from a foreign country to work, this can be deemed a "cross-border data disclosure" according to Swiss data protection law. The disclosure of personal data is only permitted if the country receiving the data is considered providing an adequate level of data protection. If this is not the case, other reasons to justify the transfer need to apply.

If a company decides to use remote access, it needs to inform its clients that their data may be transferred to third countries due to personnel working from abroad, for example by a statement on the employer's website, a privacy policy or through e-mail.

Return to Work Protocols

When a company wants their employees to return to work and this is combined with certain health checks or the requirement to download corporate contact tracing apps or the filling out of questionnaires and providing their health data, this should preferably only be done on a voluntary basis (i.e. by giving employees the option between working from home or in another isolated environment, so as to not expose other employees to any health risks, or returning to work but then complying with the company's safety measures). If a voluntary basis is not desirable or possible, the return to work protocol should be accompanied with measures like temperature checks and health questionnaires that are least invasive to the employees' privacy, which will be discussed in more practical detail further below.

The company also has a duty to take the necessary measures to protect the employees' health. In particular, the company must ensure that the employees can comply with the rules regarding hygiene and social distance.

Implications for Employees' Privacy

Within the employment relationship, certain privacy invading measures may be justifiable to comply with the employer's duty of care. Employees must abide by certain standards due to their duty of loyalty and the employer's right to direct and instruct. However, employers may only process personal data of employees insofar as such data is necessary for the performance of the employment contract. Within this context, the general data protection rules apply. This can mean the following:

– Due to the employers' duty of care towards their employees, employers may require employees to stay home when they feel sick, or impose medical checks on employees, such as the taking of temperature (preferably allowing employees to take their temperatures themselves), health questionnaires or the installation of thermographic cameras. Such measures must always be executed as carefully and proportionally as possible and it must be ensured that only the least invasive measures that lead to the required results are implemented, e.g. choosing temperature checks over installing thermographic cameras, asking employees to assess how they are feeling rather than asking them specific health questions etc. However, this must be assessed on a case-by-case basis.

– The employees' duty to disclose a COVID-19 infection or any contact with an infected person to the employer can be in line with employment law, due to the employer's duty of care, i.e. the duty to protect the health of other employees who may have been in contact with that person or who belong to a so-called "risk group".

– Measures that limit the employees' freedom outside of work, e.g. requiring employees to download governmental or even corporate COVID-19 contact tracing apps or limiting personal travel, have to be carefully evaluated according to the same principles. For example, a policy could be adopted that requires employees to report their travel plans to the HR department, so that they can assess whether the employee may return to work or should quarantine or isolate after travelling.

Guidelines

Even during a pandemic, privacy laws apply and personal data should be processed in compliance with applicable data protection law, respecting the general principles of proportionality, purpose limitation and transparency. Thus, the following guidelines should be followed when taking and executing the measures mentioned above:

– Only personal data that is necessary to contain and prevent the spread of COVID-19 may be processed, and the processing must always be kept to the minimum necessary. Therefore, only health data related to the virus may be processed when testing persons, e.g. temperature may be taken but not a full health check-up. Such data should only be processed if considered necessary to protect the health of others. In the context of an employment relationship, whenever possible, appropriate data on flu symptoms such as fever should be collected and passed on by the affected employees themselves.

– As far as possible, the information collected should be shared in an aggregated and anonymized form. For example, companies should record and store health data such as the employees' temperature on a pass or fail basis and, whenever possible, keep that data anonymous.

– Health data is considered sensitive personal data. Employers may not process health data of their employees against their will as it is, in general, not strictly necessary for the performance of their contract.

– Health data may only be shared with third parties if the person has consented to the sharing or if an overriding private or public interest, such as public health, safety, or a legal obligation requires such disclosure.

– If a person's personal data is going to be shared with third parties, they must be transparently informed about this. For example, companies must inform their employees that if an employee opts to be tested for COVID-19, the employer may disclose the results, if possible, on an anonymized basis or subject to the infected employee's consent, to other employees for their safety.

– Personal data should only be stored for as long as necessary to fulfil the purpose it was collected for Personal data on persons that have or had COVID-19 should be immediately deleted, especially by employers, once this pandemic is

over, unless a statutory storage duty applies. Furthermore, the data collected in connection with COVID-19 should not automatically added to the employee's personnel file.

– It is beneficial to be clear, open and honest with the employees about their data. In the ideal scenario, employer and employee work together to ensure everyone's safety during the pandemic while respecting personal data. Keep in mind too that employees have certain rights (e.g. right to access, erasure or rectification) in relation to their personal data which they must be able to exercise.

Key Contacts

Dr. Corrado Rampini
Partner
M: +41 58 262 52 83
corrado.rampini@baerkarrer.ch

Dr. Rehana Harasgama
Associate
M: +41 58 262 54 51
rehana.harasgama@baerkarrer.ch

Seline Amstutz
Junior Associate
M: +41 58 262 52 57
seline.amstutz@baerkarrer.ch

Further Contacts

Dr. Jan Kleiner
Partner
M: +41 58 262 53 84
jan.kleiner@baerkarrer.ch

Dr. Jonas Bornhauser
Associate
M: +41 58 262 54 13
jonas.bornhauser@baerkarrer.ch