EVERSHEDS SUTHERLAND

Legal Compass
Datenschutzrecht

März 2020

Q&A: Mögliche datenschutz- und persönlichkeitsschutzrechtliche Probleme im Zusammenhang mit dem Coronavirus – was gilt es zu beachten?

Autoren

Markus Näf
Partner

Dr. Michel Verde
Senior Associate

Trotz der ausserordentlichen Lage gelten die gesetzlichen Bestimmungen für die Bearbeitung von Personendaten weiter. Diese sind bei der Arbeit im Home-Office wie auch im Umgang mit Informationen über eine mögliche Infektion mit dem Corona-Virus (COVID-19) zu beachten. Informationen über den Gesundheitszustand gehören zur Intimsphäre einer Person und stellen sog. besonders schützenswerte Personendaten dar. Informationen darüber, ob eine Person sich mit COVID-19 infiziert hat, sind daher mit der entsprechenden Vertraulichkeit und Zurückhaltung zu handhaben.

Der Datenschutz steht in der aktuellen Situation wohl nicht an erster Stelle, trotzdem gilt es die Regeln zu beachten und als Unternehmen einige organisatorische Vorkehrungen zu treffen.

Bearbeitung von mitarbeiterbezogenen Daten

1. Ist ein Mitarbeiter verpflichtet, den Arbeitgeber über eine potenzielle oder erfolgte Infektion mit COVID-19 zu informieren?

Für den Arbeitgeber ist es wichtig zu wissen, ob sich ein Mitarbeiter mit COVID-19 infiziert hat, da der Arbeitgeber in einem solchen Fall verpflichtet ist, so schnell wie möglich Massnahmen zu Schutz anderer Mitarbeiter zu treffen und sie nötigenfalls über die Ansteckungsgefahr zu orientieren (siehe dazu auch Frage 3). Gegebenenfalls müssen auch Drittpersonen, wie zum Beispiel Kunden, die mit dem betreffenden Mitarbeiter in Kontakt standen, orientiert werden. Der betroffene Mitarbeiter ist daher verpflichtet, seinen Arbeitgeber umgehend über seine COVID-19-Infektion in Kenntnis zu setzen. Diese Pflicht ergibt sich einerseits aus seiner allgemeinen arbeitsvertraglichen Treuepflicht (Art. 321a Abs. 1 OR), andererseits aber auch aus seiner Pflicht, die Gesundheit von anderen Menschen nicht zu gefährden.

Eine Informationspflicht besteht auch dann, wenn der Mitarbeiter Symptome einer Ansteckung aufweist oder wenn er sich einer konkreten Ansteckungsgefahr ausgesetzt hat. Letzteres ist vor allem dann der Fall, wenn der Mitarbeiter in direktem physischen Kontakt zu einer Person stand, die sich mit COVID-19 angesteckt hat oder zumindest Symptome einer Ansteckung aufweist, oder wenn eine im gleichen Haushalt lebende Person sich einer konkreten Ansteckungsgefahr ausgesetzt hat. Hingegen begründet das gegenwärtig in der Schweiz bestehende allgemeine Risiko, sich im öffentlichen Raum mit COVID-19 anzustecken, keinen Verdachtsfall, über den zu informieren wäre.

2. Kann der Arbeitgeber Mitarbeiter auffordern, sich auf COVID-19 untersuchen zu lassen?

Für einen Arbeitgeber kann es von eminenter Wichtigkeit sein, zu wissen, ob ein Mitarbeiter, bei dem der Verdacht besteht, dass er sich mit COVID-19 angesteckt hat (namentlich, wenn Krankheitssymptome auftreten), tatsächlich infiziert ist. Eine Ungewissheit über eine mögliche Ansteckung kann zur Stillegung ganzer Betriebsteile führen. Der Arbeitgeber ist daher im Prinzip berechtigt, den betreffenden Mitarbeiter aufzufordern, sich auf eine COVID-19-Infektion untersuchen zu lassen sowie mitzuteilen, ob das Testresultat positiv oder negativ ausgefallen ist. Allerdings gilt es zu beachten, dass der Arbeitgeber den Mitarbeiter nicht zu einer Untersuchung zwingen kann. Verweigert sich der Mitarbeiter einer zumutbaren Untersuchung, könnte er jedoch allenfalls schadenersatzpflichtig werden, wenn die Ungewissheit über eine COVID-19-Infektion des Mitarbeiters dazu führt, dass sich andere Arbeitnehmer in Selbstisolation begeben müssen und infolgedessen nicht arbeiten können. Dabei gilt es zu berücksichtigen, dass der Mitarbeiter nur beschränkten Einfluss darauf hat, ob er tatsächlich getestet wird, da der Entscheid über die Notwendigkeit eines Tests schlussendlich beim Arzt liegt, was der Arbeitgeber hinzunehmen hat.

3. Was muss der Arbeitgeber hinsichtlich des Umgangs mit Informationen über eine COVID-19-Ansteckung von Mitarbeiter beachten?

Grundsätzlich gilt das Datenschutzrecht auch bezüglich der Bearbeitung von Personendaten in Zusammenhang mit dem COVID-19. Die allgemeinen Grundsätze des Schweizer Datenschutzrechts und – sofern überhaupt anwendbar – der EU Datenschutz-Grundverordnung («DS-GVO») sind daher weiterhin einzuhalten.

Die Information, dass sich ein Mitarbeiter mit COVID-19 infiziert hat, gehört zu den sog. besonders schützenswerten Personendaten im Sinne des Datenschutzgesetzes sowie der DS-GVO. Wie oben erwähnt (siehe Fragen 1 und 2), ist der Arbeitgeber zwar grundsätzlich berechtigt, diese Information zu erfahren, um die Gesundheit der anderen Mitarbeiter sowie von Drittpersonen zu schützen (vgl. Art. 13 Abs. 1 DSG; Art. 9 Abs. 2 DS-GVO). Indes gilt es in diesem Zusammenhang folgende, nicht abschliessende Punkte zu beachten:

- Die Information, dass sich ein Mitarbeiter mit COVID-19 infiziert hat, darf nur mit denjenigen Personen geteilt werden, die diese Information zwingend benötigen. Dies trifft namentlich auf die HR-Verantworliche und gegebenenfalls auf den Vorgesetzten zu. Bezüglich den anderen Mitarbeitern im Betrieb, die allenfalls angesteckt worden sein könnten, genügt in der Regel die blosse Information, dass sie einem Ansteckungsrisiko ausgesetzt waren und entsprechende Vorkehrungen treffen müssen (z.B. beobachten, ob sie Krankheitssymptome entwickeln, Selbstisolation, etc.); die Offenlegung der Namen von infizierten Arbeitskollegen wird daher für gewöhnlich nicht gerechtfertigt sein. Auch die Weitergabe von nicht-anonymisierten Informationen über eine COVID-19-Ansteckung an andere Konzerngesellschaften zwecks Ressourcenplanung wird normalerweise mangels Notwendigkeit nicht rechtmässig sein.
- Die Information über eine COVID-19-Ansteckung darf nur so lange aufbewahrt werden, wie dies für den Schutz der Gesundheit der Mitarbeiter notwendig ist.
- Der Arbeitgeber hat die Mitarbeiter darüber zu informieren, wie er mit den Informationen über eine COVID-19-Infektion umgeht. Dies beinhaltet namentlich eine Information über den Zweck der Bearbeitung, über die Empfänger der Information sowie über die Aufbewahrungsdauer, wobei die letztgenannte Information unter dem geltenden Schweizer Datenschutzrecht nicht zwingend ist.

Vorgenanntes gilt sinngemäss auch in Bezug auf Informationen über eine konkrete Ansteckungsgefahr, der sich ein Mitarbeiter ausgesetzt hat (siehe dazu auch Frage 1). Falls ein Mitarbeiter den Arbeitgeber darüber orientiert, dass er Kontakt zu einer Person hatte, die sich (möglicherweise) mit COVID-19 angesteckt hat, sollte der Mitarbeiter die betroffene Person (zum Beispiel die Ehefrau) über diese Orientierung informieren, sofern die Anonymität nicht gewahrt werden kann.

4. Kann der Arbeitgeber die Mitarbeiter auffordern, ihre Temperatur zu messen?

Die Messung der Körpertemperatur kann allenfalls eine Massnahme sein, um die Ansteckungsgefahr im Betrieb zu reduzieren. Allerdings dürfte nur eine Selbstmessung durch den Mitarbeiter im Sinne einer Selbstkontrolle rechtmässig sein. Dabei ist sicherzustellen, dass der Arbeitgeber keine Messdaten speichert.

5. Darf der Arbeitgeber bei besonders gefährdeten Personen Informationen zum Grund ihrer besonderen Gefährdung bearbeiten?

Artikel 10c der COVID-19-Verordnung 2 vom 13. März 2020 auferlegt dem Arbeitgeber besondere Pflichten gegenüber Mitarbeiter, die besonders gefährdet sind. Er muss ihnen ermöglichen, von zu Hause aus zu arbeiten, oder, wenn dies nicht möglich ist, ihnen gegenüber mit geeigneten organisatorischen und technischem Massnahmen die Empfehlungen des Bundes betreffend Hygiene und sozialer Distanz umsetzen. Sollte dies nicht machbar sein, muss er die betreffenden Mitarbeiter unter Lohnfortzahlung beurlauben. Gemäss Artikel 10b Absatz 2 der COVID-19-Verordnung 2 geltend Personen über 65 sowie Personen, die an Bluthochdruck, Diabetes, Herz-Kreislauf-Erkrankungen, chronische Atemwegserkrankungen, Krebs oder einer krankheits- oder therapiebedingten Immunsystemschwäche leiden, als besonders gefährdet. Abgesehen des dem Arbeitgeber ohnehin bekannten Alters des Mitarbeiters hat der Arbeitgeber im Hinblick auf seine vorgenannten Pflichten jedoch kein Anspruch darauf, Informationen darüber zu erhalten und zu bearbeiten, aus welchem Grund ein Mitarbeiter der Kategorie der besonders gefährdeten Personen angehört. Stattdessen muss sich der Arbeitgeber grundsätzlich mit einem ärztlichen Attest begnügen, dass die Zugehörigkeit des Mitarbeiters zu dieser Personenkategorie bescheinigt.

Datenschutz und Home-Office

Der Arbeitsplatz hat sich für viele Mitarbeitende aufgrund der aktuellen Situation nach Hause ins Home-Office verlagert. Dies erfordert neben den technischen Voraussetzungen auch eine klare Instruktion an die Mitarbeitenden.

6. Technische und Organisatorische Massnahmen (TOM)

Es gelten bei der Datenbearbeitung im Home-Office grundsätzlich die gleichen Regeln, wie für die Datenbearbeitung in den Geschäftsräumen. Der Arbeitgeber hat mit der Erlaubnis der Heimarbeit sicherzustellen, dass diese in einem sicheren Umfeld möglich ist.

Am klarsten kann diese bei der Verwendung von Remote Access Lösungen gelöst werden, wo die Mitarbeitenden über eine sichere Verbindung auf einem Profil wie im Unternehmen arbeiten und lokal keine Daten gespeichert werden. Dabei können auch lokale Speicher, Druckfunktionen oder das Einlesen von Daten gesperrt oder kontrolliert werden.

Die Überwachung von Mitarbeitenden im Home Office mittels Tools ist genauso unzulässig, wie sie dies in den Geschäftsräumlichkeiten ist.

7. Datenablage und Nutzung von Collaborative-Tools

Mitarbeitende sollten die Daten grundsätzlich nur in den firmeneigenen Dateiablagen speichern und nicht auf externen Datenträgern (Memory-Sticks) oder lokal auf dem Rechner; ist dies dennoch erforderlich, sollten der Rechner oder externe Datenträger verschlüsselt sein. Die Speicherung von Geschäftsdaten auf privaten Rechnern sollte ausgeschlossen werden.

Bei der Nutzung von im Internet verfügbare Online-Tools, wie Dropbox oder W-Transfer sind deren Datenschutzbestimmungen zu beachten. Diese übermitteln und speichern die Daten oftmals irgendwo im Ausland und es ist nicht immer klar, inwieweit Dritte darauf Zugriff haben. Mitarbeiter sollten nur vom Unternehmen autorisierte Tools verwenden und auf den Einsatz solcher Freeware verzichten.

Ebenfalls dürfen keine geschäftlichen Daten für die Bearbeitung auf private E-Mail Adressen von Mitarbeitenden übermittelt werden.

8. Einsatz von Video-Conferencing

Bei der Nutzung von Videoconferencing-Tools sind die Datenschutzbestimmungen der jeweiligen Anbieter zu beachten. Generell kann man davon ausgehen, dass kostenlose Tools meist einen tieferen Datenschutzstandard haben als kostenpflichtige Unternehmenslösungen.

Aber bei pratkisch allen Lösungen wie Zoom, Skype oder Teams ist zu berücksichtigen, dass die Daten meist in den USA bearbeitet werden. Datenschutzrechtlich stellt dies eine Datenübermittlung ins Ausland dar. Damit muss ein Anbeiter in den USA sich zur Einhaltung der europäischen oder schweizerischen Datenschutzbestimmungen verpflichten (zum Beispiel mit dem Privacy Shield-Abkommen) oder es muss eine Einwilligung der betroffenen Person vorliegen. Bei der Bearbeitung von besonderen Kategorien von Personendaten oder von Daten, die einem Berufsgeheimnis unterliegen, ist die Übermittlung ins Ausland nur mit Einwilligung zulässig.

Wir empfehlen bei der Verwendung dieser Tools eine entsprechende Datenschutzinformation vorzuschalten, welche die Verwender wenn möglich vorgängig akzeptieren müssen. Wir stellen gerne ein solches Muster zur Verfügung.

9. Arbeitsmittel und Entschädigung

Grundsätzlich hat der Arbeitgeber den Mitarbeitenden die notwendige Arbeitsinfrastruktur zur Verfügung zu stellen und allfällige Spesen im Zusammenhang mit der Arbeit zu entschädigen.

Wenn der Mitarbeiter seinen privaten PC oder das Mobilephone nutzt (BYOD), kann der Arbeitgeber dies mit Auflagen erlauben. Eine Entschädigung für Strom- oder Telefonkosten ist durch den Arbeitgeber geschuldet, wenn die Home-Office Arbeit im Interesse des Arbeitgebers erfolgt. Diese kann mit einer Pauschale, wie zum Beispiel die Entschädigung für die private Nutzung des Telefons, geregelt werden.

Eine Entschädigung für die Nutzung eines Arbeitsplatzes zu Hause ist hingegen nicht geschuldet, soweit der Arbeitnehmer auch einen Arbeitsplatz im Unternehmen zur Verfügung hat.

Wir empfehlen, diese Puntke transparent zu regeln.

10. Sorgfältige Instruktion der Mitarbeitenden

Die Mitarbeitenden sind in Bezug auf den Datenschutz im Home-Office sorgfältig daüber zu instruieren, dass:

- die vom Arbeitgeber bereitgestellte IT-Infrastruktur nicht privat genutzt wird (keine Vermischung von privaten und geschäftlichen Daten) und keine Dritten darauf Zugriff haben (zum Beispiel Hausaufgaben der Kinder);
- ein sicheres, passwortgeschütztes WLAN verwendet wird;
- bei der Verwendung eines privaten Computers dieser mit einer aktuellen Virenschutzsoftware versehen ist und über die aktuellste Software-Updates verfügt;
- keine Speicherung von Geschäftsdaten auf privaten Rechnern;
- der Computer stets gesperrt wird, wenn man den Arbeitsplatz verlässt;
- keine Übermittlung von Geschäftsdaten auf private E-Mail-Adressen des Mitarbeitenden;
- vertrauliche Telefonate nur in abgeschlossenen Räumen ohne unbefugte Mithörer geführt werden;
- Unterlagen mit personenbezogenen Daten oder Geschäftsgeheimnissen nicht offen herumliegen und von Dritten eingesehen werden können; diese Unterlagen sind unter Verschluss aufzubewahren;
- nicht mehr benötigte Unterlagen fachgerecht entsorgt werden (nicht offen im Haushaltsmüll);
- festgestellte Datenschutzverstösse unverzüglich gemeldet werden.

Wir empfehlen, eine beidseitige Vereinbarung zwischen Arbeitgeber und Mitarbeitenden zur Arbeit im Home-Office in einem Formular festzuhalten und darin die anwendbaren Regeln klar zu definieren. Es können darin auch Fragen der Erreichbarkeit und der Entschädigung geregelt werden. Gerne unterstützen wir Sie dabei.

Ihr Kontakt für Daten- und Persönlichkeitsschutz

Daniel Bachmann
Partner

T: +41 44 204 90 90
daniel.bachmann@eversheds-sutherland.ch

Markus Näf
Partner

T: +41 44 204 90 90
markus.naef@eversheds-sutherland.ch

Dr. Michel Verde
Senior Associate

T: +41 44 204 90 90
michel.verde@eversheds-sutherland.ch