SCHWERPUNKT

Datenschutz & Coronakrise: Wie viel Überwachung von Bürgern und Mitarbeitern ist zulässig?

Die COVID-19-Pandemie stellt den Datenschutz auf eine harte Probe. Die Nutzung moderner Technologien zu deren Bekämpfung ist Realität. Wie weit dürfen in der Krise Daten aus Mobiltelefonen über Bürger ausgewertet werden und in welchem Umfang darf der Arbeitgeber Gesundheitsdaten über seine Arbeitnehmer erheben?

RAINER KNYRIM / CLAUDIA GABAUER

A. Einleitung

Die aktuelle Bedrohung durch das Virus COVID-19 veranschaulicht drastisch, dass die Menschheit auch im 21. Jahrhundert trotz der gestiegenen Hygienestandards und des hochentwickelten technischen und medizinischen Fortschritts nicht vor den existenziellen Gefahren einer Seuche gefeit ist. Auch wenn die zentralen Strategien der Infektionsbekämpfung seit Jahrhunderten unverändert geblieben sind,[1] eröffnen sich durch die modernen Technologien nun auch neue Wege zur Bekämpfung der Pandemie. Im Fokus stehen hierbei zunächst das Mobiltelefon und die damit verbundene Möglichkeit zur Sammlung und Auswertung von Daten.

B. Auswertung von Mobilfunkdaten

Die von der Datenschutz-NGO noyb[2] ins Leben gerufene Wiki-Seite GDPRhub[3] gibt einen aktuellen Überblick darüber, in welchen Ländern Projekte zur Bekämpfung von COVID-19 unter Verwendung von personenbezogenen Daten im Einsatz sind. Die Bandbreite reicht von statistischen Auswertungen von Daten von Mobilfunkbetreibern (etwa in Österreich, Deutschland, Italien und der Schweiz) über Self-Assessment-Apps für das Handy (Spanien), grafischen Standortauswertungen (Südkorea) bis hin zu dezentralen Kontakt-Tracking-Apps wie der „Stopp Corona"-App in Österreich und anderen Apps für den privaten Gebrauch (zB Deutschland, Italien, England, USA) oder Regierungs-Apps (zB Island und Irland). Manche Staaten gehen noch weiter und setzen Kontakt-Trackingsysteme ein, die nicht nur Mobilfunkdaten, sondern weitere Datenquellen nutzen, um die Bürger zu überwachen (zB Tschechien und Slowakei). In Israel führt der Geheimdienst die Überwachung durch, in Südkorea werden öffentliche Kameras, Kreditkartendaten und GPS-Daten aus Autos und von Mobilfunktelefonen hinzugezogen.[4] Am weitesten in der EU geht bisher Polen, wo Bürger mittels einer freiwilligen „Home Quarantine"-App in ihrer Quarantäne überwacht werden, die – als Alternative zu regelmäßigen Vor-Ort-Polizeikontrollen – Zugriff auf deren Kamera und GPS-Standortdaten verlangt und die Bürger binnen zwanzig Minuten zur Anfertigung von Fotos aus ihrer Quarantäne-Wohnung auffordert.[5]

Die in Österreich verwendeten bzw in Diskussion stehenden Technologien zur Auswertung von Mobilfunkdaten teilen sich aktuell in drei große Gruppen auf, die unterschiedlich zu behandeln sind.

1. Auswertung von anonymisierten Bewegungsdaten mittels „Big Data"

Thomas Arnolder, CEO von A1 Telekom Austria, erklärte am 26. 3. 2020 in einer Pressekonferenz mit Verkehrsministerin *Köstinger,* dass A1 der Regierung Analyseergebnisse von anonymisierten, aggregierten Bewegungsmustern übermittelt habe. Dies, damit festgestellt werden könne, ob die Maßnahmen der Verkehrsbeschränkung wirken. Man könne dadurch etwa eruieren, ob sich (noch immer) Menschenansammlungen auf Straßen oder Plätzen bewegen.

Dies ist eine bekannte und erprobte Technik zur Seuchenbekämpfung. Schon im Jahr 2015 berichtete *Mila Romanoff,* Rechts- und Datenschutzspezialistin bei UN Global Pulse – einer Big Data Initiative der UNO – in einem Interview, dass Big Data-Auswertungen bei einem Hochwasser-Projekt in Mexiko eingesetzt wurden. Im Rahmen dieses Projekts wurde erforscht, ob anonymisierte Aufzeichnungen einer Handydatennutzung oder von Einzelverbindungsnachweisen zeigen könnten, wie Bevölkerungsgruppen ihre Verhaltensmuster in einer Katastrophensituation verändern.[6]

Ebenfalls eingesetzt wurde diese Technologie von UN Global Pulse während des Ausbruchs der Ebola-Krise in Afrika, um die Fluchtbewegung der Bevöl-

Dr. *Rainer Knyrim* ist Rechtsanwalt und Mitbegründer von Knyrim Trieb Rechtsanwälte OG.

Dr. *Claudia Gabauer,* LL.M., ist Rechtsanwaltsanwärterin bei Knyrim Trieb Rechtsanwälte OG.

1) Vgl *Kopetzki,* Editorial: Corona – Epidemierecht auf Bewährung, RdM 2020/40.

2) noyb.eu.

3) gdprhub.eu.

4) gdprhub.eu/index.php?title=Projects_using_personal_data_to_combat_SARS-CoV-2 (abgefragt am 7. 4. 2020).

5) www.cbsnews.com/news/coronavirus-update-poland-quarantine-app-asks-selfies-to-prove-isolation-social-distancing-police-patients/ (abgefragt am 7. 4. 2020).

6) *Knyrim,* Interview mit *Mila Romanoff,* Wie Big Data Katastrophenhilfe unterstützt, Dako 2015, 50, abrufbar in der RDB oder unter www.kt.at/wp-content/uploads/2020/03/Dako-2015-3_50.pdf.

kerung aus den Ballungszentren in ihre ländliche Heimat in anonymisierter Form „live" zu beobachten und damit vorhersagen zu können, wo Ebola als Nächstes ausbricht.[7)]

Datenschutzrechtlich sind solche Big Data-Auswertungen, wenn sie tatsächlich anonymisiert, dh vor allem ausreichend aggregiert durchgeführt werden, unbedenklich, weil sie mangels verknüpfbaren Personenbezugs aus dem Anwendungsbereich der DSGVO und des Grundrechts auf Datenschutzrecht fallen.[8)] Der Vorgang des Anonymisierens zum Zweck der Durchführung kann als Form der Verarbeitung personenbezogener Daten auf § 7 Abs 1 Z 2 DSG oder Art 6 Abs 1 lit f DSGVO gestützt werden. Sofern die Erstellung von anonymisierten Bewegungsanalysen auf Verkehrs- oder Standortdaten iSd TKG 2003 beruht, richtet sich die Rechtmäßigkeit der Verarbeitung – und damit auch der Anonymisierung – nach den Bestimmungen des TKG 2003, die als leges speciales[9)] der DSGVO vorgehen und eine strenge Zweckbindung normieren.[10)]

2. Private Tracking-Apps

Derzeitige „Stufe 2" der Überwachung in Österreich sind private Tracking-Apps. Private Tracking-Apps, wie die „Stopp Corona"-App des Roten Kreuzes[11)] oder eine weitere in Entwicklung befindliche App des Vereins „Novid20",[12)] sollen von möglichst vielen Österreichern auf freiwilliger Basis genutzt werden. Rechtsgrundlage der Datenverarbeitung im Verhältnis zum Nutzer ist somit deren Einwilligung. Die „Stopp Corona"-App ermöglicht einen „digitalen Handshake", der darin besteht, dass mittels Bluetooth, WLAN, Ultraschall und/oder Google Nearby Mobiltelefone in der Umgebung geortet werden, mit denen sich der Nutzer entweder automatisch oder manuell durch Austausch eines Zifferncodes vernetzen kann.[13)] Dieser „digitale Handshake" soll es ermöglichen, die zuvor vernetzten „Begegnungen" im Fall einer positiven Testung eines Nutzers auf COVID-19 oder im Fall eines Verdachts anonym zu verständigen, dass sie vielleicht ebenfalls infiziert wurden.

Datenschutzrechtlich essentiell bei der Entwicklung solcher Apps ist die Einhaltung der Grundsätze der Datenverarbeitung nach Art 5 DSGVO, insb zur Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung und Integrität und Vertraulichkeit.[14)] Ebenso müssen die konkreteren Vorgaben von „Privacy by Design" und „Privacy by Default" (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) des Art 25 DSGVO berücksichtigt werden. Bei der Entwicklung muss auch darauf geachtet werden, dass die Menge der erhobenen personenbezogenen Daten, der Umfang ihrer Verarbeitung, ihre Speicherdauer und ihre Zugänglichkeit präzise bedacht werden.[15)] Ein Kriterium, das von den Entwicklern der Apps hervorgehoben wurde, ist die lokale Speicherung der Daten auf dem Mobiltelefon des Nutzers. Sicherheitsforscher kritisierten hinsichtlich der „Stopp Corona"-App allerdings, dass die „Handshakes" auch an das Rote Kreuz übermittelt werden.[16)]

Zu bedenken ist auch, dass eine „anonymisierte" Information der Kontaktpersonen letztlich von der Anzahl der Kontaktpersonen abhängt. Laut Datenschutzinformation des Roten Kreuzes werden alle Kontakte der letzten 54 Stunden von einer Infektion informiert.[17)] Angesichts der aktuellen Restriktionen und des angeordneten Social Distancing beschränken sich die sozialen Kontakte und damit auch die Anzahl potenzieller „Handshakes" in der Praxis auf ein überschaubares Maß. Liegt die Zahl der Handshakes der letzten 54 Stunden bei einem Nutzer bei sechs oder weniger, kann nach der bisherigen Judikatur[18)] nicht von einer ausreichenden Aggregierung und Anonymisierung ausgegangen werden. Auch liegt es im Fall eines manuellen „Handshakes" beim Nutzer selbst, über die Zahl der durchgeführten „Handshakes" und damit letztlich auch über die Bestimmbarkeit seiner Kontaktpersonen zu entscheiden.

Ein weiterer heikler Punkt ist die potenzielle Missbrauchsgefahr, die aus falsch-positiven Meldungen resultieren könnte. Die Meldung über eine positive Testung obliegt der alleinigen Entscheidung des Nutzers und ist nicht von einem tatsächlich positiven Testergebnis abhängig. Da eine Information der Kontaktpersonen über eine (vermeintlich) bestätigte Infektion oder über einen Verdachtsfall eines ihrer „Handshake"-Partners dazu führt, dass sich diese regelmäßig in Selbstisolation begeben (müssen), hat es der Nutzer letztlich auch in der Hand, willkürlich

7) www.unglobalpulse.org/2015/03/big-data-innovation-as-part-of-a-data-revolution-in-africa/ (abgefragt am 7. 4. 2020).

8) futurezone.at/netzpolitik/ausgangsbeschraenkung-a1-liefert-bewegungsprofile-an-regierung/400783565 (abgefragt am 7. 4. 2020); *EDSA,* Statement on the processing of personal data in the context of the COVID-19 outbreak (19. 3. 2020).

9) Vgl DSB 7. 3. 2019, DSB-D130.033/0003-DSB/2019; 30. 11. 2018, DSB-D122.931/003-DSB/2018.

10) Vgl § 96 Abs 1, §§ 99, 102 TKG 2003; *Riesz* in *Riesz/Schilchegger* (Hrsg), TKG (2006) § 96 Rz 9, § 99 Rz 18 ff.

11) www.roteskreuz.at/site/faq-app-stopp-corona/ (abgefragt am 7. 4. 2020).

12) www.novid20.org/en (abgefragt am 7. 4. 2020).

13) Status der Stopp Corona-App des Roten Kreuzes am 14. 4. 2020, die eine Vernetzung nun optional auch automatisiert ermöglicht - s www.roteskreuz.at/site/faq-app-stopp-corona/ (abgefragt am 14. 4. 2020).

14) Vgl näher *Hötzendorfer/Kastelitz/Tschohl* in *Knyrim,* DatKomm Art 5 Rz 18 ff.

15) Siehe im Detail auch die Guidelines des EDSA 4/2019 on Article 25 Data Protection by Design and by Default vom 13. 11. 2019 sowie *Hötzendorfer/Kastelitz/Tschohl* in *Knyrim,* DatKomm Art 25 Rz 19 ff und *noyb,* Ad hoc Paper SARS-CoV-2 Tracking unter GDPR (VO.3, 8. 4. 2020), noyb.eu/en/data-protection-times-corona (abgefragt am 11. 4. 2020).

16) *SBA Research,* Stopp Corona App – Technisches Statement www.sba-research.org/wp-content/uploads/2020/03/Technische-Analyse-Stopp-Corona-App_27. 03. 2020_TA.pdf (abgefragt am 7. 4. 2020).

17) www.roteskreuz.at/site/faq-app-stopp-corona/datenschutzinformation-zur-stopp-corona-app/ (abgefragt am 13. 4. 2020).

18) Vgl zum DSG 2000 DSB 30. 3. 2015, DSB-D215.611/0003-DSB/2014; DSK 22. 5. 2013, K213.180/0021-DSK/2013, wonach ein Rückschluss auf bestimmte Personen erst im Fall einer Gruppe von mehr als fünf Personen nicht mehr möglich ist.

über die Bewegungsfreiheit seiner Kontakte zu entscheiden.

Dieses Risiko des Rechtsmissbrauchs wird auch in der Datenschutzinformation der „Stopp Corona"-App berücksichtigt, in der ausdrücklich darauf hingewiesen wird, dass personenbezogene Daten (insb die im Fall einer Infektionsmeldung verpflichtend anzugebende Telefonnummer) im Fall von Anhaltspunkten für ein gesetzwidriges bzw rechtsmissbräuchliches Verhalten auf Grundlage des Art 6 Abs 1 lit f iVm Art 9 Abs 2 lit f DSGVO an die Strafverfolgungsbehörden oder an die Gerichte weitergeleitet werden.

Freiwillige Nutzer der App könnten allerdings auch in eine andere „Straf-Falle" tappen: COVID-19 ist nicht nur hinsichtlich einer Erkrankung, sondern bereits hinsichtlich eines Verdachtsfalls anzeigepflichtig.[19] Wer eine anzeigepflichtige Krankheit hat und vorsätzlich oder fahrlässig andere Menschen gefährdet, macht sich nach §§ 178 f StGB strafbar (bis zu ein Jahr Freiheitsstrafe, bei Vorsatz sogar bis zu drei Jahre). Ein Nutzer der App könnte sich im Fall einer Meldung einer Infektion strafbar machen, wenn er sich trotz Infektion nicht selbst isoliert oder gegenüber Dritten behauptet, kein Verdachts- oder Erkrankungsfall zu sein und damit diese Personen einer Infektionsgefahr aussetzt. Gesundheits- und Strafverfolgungsbehörden hätten in diesem Fall auch Zugriffsmöglichkeit auf die vom Roten Kreuz gespeicherte Telefonnummer als Beweis.[20]

Die mittlerweile veröffentlichte Datenschutz-Folgenabschätzung zur „Stopp Corona"-App listet rd 30 zum Teil hohe Risiken auf, die großteils schwere Auswirkungen auf die betroffenen Personen haben können, sich aber laut den Autoren durch die Ergreifung verschiedenster technischer und organisatorischer Maßnahmen auf mittlere oder geringe Risiken reduzieren lassen.[21]

3. Staatliches Einzeltracking

China, Israel, aber auch europäische Staaten wie die Slowakei oder Tschechien werten im Kampf gegen das Virus personenbezogene Daten einzelner Bürger aus. Auch in Österreich wurde eine gesetzlich verpflichtende Nutzung von Tracking-Apps sowohl politisch als auch medial heftig diskutiert. Nach der geltenden nationalen Rechtsordnung fehlt eine entsprechende Rechtsgrundlage, die eine derartige Maßnahme legitimieren könnte. Laut Europäischem Datenschutzausschuss könnte aber in außergewöhnlichen Umständen und abhängig von den konkreten Maßnahmen der Verarbeitung ein „Tracking" von Einzelpersonen – inklusive der Auswertung von historischen Bewegungsdaten – zulässig sein.[22]

Der Gesetzgeber könnte daher laut dieser Aussage auch in Österreich eine entsprechende Eingriffsnorm in Form eines formellen[23] Gesetzes schaffen. Fraglich ist aber, ob diese Norm den Vorgaben des § 1 Abs 2 DSG iVm Art 8 EMRK entsprechen würde, wonach der Eingriff zur Wahrung wichtiger öffentlicher Interessen „in einer demokratischen Gesellschaft" notwendig sein muss. Die Maßnahme muss zunächst zur Zweckerreichung geeignet sein: Soweit ersichtlich, fehlen bislang valide Studien zur Effektivität von Tracking-Apps bei der Bekämpfung von Epidemien. Zu beachten ist auch, dass der Einsatz von Tracking-Apps eine Ansteckung nicht verhindern kann, sondern lediglich die Eindämmung der Infektionskette durch eine raschere Ermittlung von Kontaktpersonen fördert. Weiters kann der Nutzen einer Tracking-App durch missbräuchliches Verhalten durch den Nutzer torpediert werden, indem er etwa das Mobiltelefon nicht mit sich führt oder falsch-positive Meldungen vornimmt oder eine Infektion nicht meldet. Die Maßnahme muss auch das gelindeste, zur Zweckerreichung geeignete Mittel sein. Dazu müsste – etwa durch Studien, die es, soweit ersichtlich, in Österreich aber noch nicht gibt – untersucht werden, ob der Einsatz einer solchen Tracking-App zur Eindämmung der Pandemie abstrakt geeignet ist und ob gelindere und zugleich effektivere Mittel zur Zweckerreichung in Betracht kommen, wie etwa bereits bestehende Maßnahmen, das Tragen von Schutzmasken im öffentlichen Raum oder verstärkte Schutzmaßnahmen für Risikogruppen. Die Maßnahme muss auch verhältnismäßig im engeren Sinn sein. Je nach Ausgestaltung und den Folgen der Nichteinhaltung einer verpflichtenden Nutzung – zB Koppelung der Teilnahme am öffentlichen Leben an die App-Nutzung, Beugehaft, Quarantäne – wäre eine gesetzliche Regelung mit einer Vielzahl an Grundrechtseingriffen verbunden, die – auch im Verhältnis zu anderen schon verfügten, teils aber auch sehr invasiven Grundrechtseingriffen – einer Rechtfertigung bedarf.[24] Anhaltspunkte für das Ergebnis einer Verhältnismäßigkeitsprüfung und damit für die Frage nach der verfassungsrechtlichen Zulässigkeit einer derartigen Regelung finden sich in der Rsp des VfGH.[25]

19) § 1 Abs 2 EpidemieG iVm V betreffend anzeigepflichtige übertragbare Krankheiten 2020 BGBl II 2020/15; s auch *Soyer/Baier,* Schon Husten kann mit Gefängnis bedroht sein, Die Presse 2020/15/05.

20) *Knyrim,* Staatliche Tracking-App bei Bedarf denkbar, Die Presse 2020/14/04.

21) *Tschohl,* Bericht über die Datenschutz-Folgenabschätzung für die Anwendung Stopp Corona-App des Österreichischen Roten Kreuzes, Version 1.1 vom 10. 4. 2020, www.roteskreuz.at/fileadmin/user_upload/Bericht_Datenschutz-Folgenabschaetzung_OeRK_Stop CoronaAppR1.1_RI_09-04-2020_V1.1_public.pdf (abgefragt am 13. 4. 2020).

22) *EDSA,* Statement on the processing of personal data in the context of the COVID-19 outbreak.

23) Vgl *Ennöckl,* Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung (2014) 196; *Jahnel,* Handbuch Datenschutzrecht (2010) Rz 2/57; *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl,* DSG (2018) § 1 Rz 12.

24) Recht auf Datenschutz (§ 1 DSG, Art 8 GRC), Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK), Freizügigkeit (Art 4 StGG, Art 2 4. ZPEMRK), Persönliche Freiheit (BVG Schutz der persönlichen Freiheit, Art 5 EMRK), Gleichheitssatz (Art 2 StGG, Art 7 Abs 1 B-VG); s auch *Bußjäger/Gamper,* Stellungnahme zur Verfassungskonformität einer verpflichtenden Tracking-App, www.uibk.ac.at/public-relations/presse/archiv/2020/1269/ (abgefragt am 13. 4. 2020); Der Standard, Verwaltungsrichter: App-Pflicht wäre unverhältnismäßiger Eingriff in die Grundrechte, www.derstandard.at/story/2000116805190/vfgh-richter-app-pflicht-waere-unverhaeltnismaessiger-eingriff-in-grundrechte (abgefragt am 13. 4. 2020).

25) Vgl VfGH 11. 12. 2019, G 72/2019; 27. 6. 2014, G 47/2012.

C. Gesundheitsdatenerhebung bei Mitarbeitern

Auch im Arbeitskontext ist die Frage der Zulässigkeit der Überwachung von Mitarbeitern virulent. Arbeitgeber sind aufgrund ihrer Fürsorgepflicht[26] angehalten, geeignete Vorkehrungen zum Schutz der Mitarbeiter zu treffen und Gesundheitsrisiken am Arbeitsplatz auszuschließen.[27] Da bereits Verdachtsfälle von COVID-19 als Gesundheitsdaten iSd Art 4 Z 15 DSGVO einzustufen sind, ist die Verarbeitung dieser Information grundsätzlich verboten, sofern kein Ausnahmetatbestand nach Art 9 Abs 2 DSGVO vorliegt. Hinsichtlich der datenschutzrechtlichen Zulässigkeit der Erhebung von Gesundheitsdaten ist in weiterer Folge je nach Form und Umfang der Erhebung zu differenzieren.

1. Bekanntgabe einer Infektion durch Arbeitnehmer

Als Ausfluss ihrer Treuepflicht müssen Arbeitnehmer grds eigeninitiativ den Arbeitgeber über einen Verdachtsfall oder eine bestätigte Infektion informieren.[28] Für bestimmte Arbeitnehmer in besonders sensiblen Arbeitsbereichen – zB bei der Herstellung, der Kontrolle oder dem Inverkehrbringen von Arzneimitteln – sieht der Gesetzgeber eine ausdrückliche proaktive Meldepflicht von (auch nur beschränkt) anzeige- und meldepflichtigen Krankheiten vor, deren Nichtbeachtung auch verwaltungsstrafrechtliche Konsequenzen nach sich zieht.[29]

2. Befragungen durch den Arbeitgeber

Die allgemeine Fürsorgepflicht erlaubt auch Befragungen durch den Arbeitgeber.[30] Zulässig und zweckmäßig sind Fragen über das Bestehen einer Infektion oder über Kontakte mit infizierten Personen sowie über einen Aufenthalt in einem Risikogebiet. Die Datenverarbeitung stützt sich dabei auf Erfüllung von Verpflichtungen aus dem Arbeitsrecht gem Art 9 Abs 2 lit b iVm Art 6 Abs 1 lit c oder f DSGVO. Bei der Befragung ist besonders auf die datenschutzrechtlichen Grundsätze der Datenminimierung und Zweckbindung Bedacht zu nehmen. Unzulässig wäre etwa ein umfangreicher Fragebogen, der die Angabe von konkreten Aufenthaltsorten oder die namentliche Nennung von Kontaktpersonen fordert. Zu beachten ist, dass mündliche Befragungen in den Schutzbereich des Grundrechts nach § 1 DSG fallen, auch wenn die erhobenen Daten in weiterer Folge nicht verarbeitet werden und daher nicht dem Anwendungsbereich der DSGVO unterliegen.[31]

3. Temperaturmessungen

Viele Arbeitgeber möchten das Risiko einer Infektion und Ausbreitung in ihrem Betrieb durch die Messung der Körpertemperatur ihrer Arbeitnehmer eindämmen. Sofern die Messung digitalisiert erfolgt, liegt eine (zumindest teilweise) automatisierte Verarbeitung personenbezogener Daten vor, die dem Anwendungsbereich der DSGVO unterliegt, auch wenn das Ergebnis dieser Messung in weiterer Folge nicht gespeichert oder dokumentiert wird. Hinsichtlich der Zulässigkeit dieser Maßnahme verweist die DSB in ihren „FAQ zum Thema Datenschutz und Coronavirus“ zunächst darauf, dass es sich hierbei in erster Linie um eine arbeitsrechtliche Frage handle. Gleichzeitig merkt sie jedoch an, dass aus datenschutzrechtlicher Sicht gelindere Mittel für die Erhebung von Gesundheitsdaten bestehen, wie etwa die Befragung der Mitarbeiter, zumal Fieber auch nur eines von mehreren möglichen Symptomen für eine mögliche Ansteckung mit COVID-19 sein könne.[32]

Es ist zutreffend, dass eine Infektion mit COVID-19 nicht zwingend mit Fieber oder mit einer bestimmten Symptomatik einhergehen muss. Die Schlussfolgerung, dass Fiebermessen kein geeignetes und auch nicht das gelindeste Mittel sei, ist für viele Arbeitgeber jedoch unbefriedigend und auch überraschend, zumal die Messung der Körpertemperatur – zusätzlich zur Erhebung der Reisebewegungen und allfälliger Kontakte mit an COVID-19-Erkrankten – vom Gesetzgeber explizit als zulässige medizinische Überprüfung im Rahmen einer verkehrsbeschränkenden Maßnahme gegenüber ein- und durchreisenden Personen normiert wird.[33] Darf daher nur der Staat an der Grenze Fiebermessungen zum Schutz seiner Bürger durchführen, nicht aber ein Arbeitgeber an den Pforten seines Betriebsgeländes zum Schutz seiner Arbeitnehmer?

Die DSB sieht eine derartige Maßnahme nur dann ausnahmsweise als datenschutzrechtlich zulässig an, wenn eine Untersuchungspflicht gesetzlich angeordnet wird. Sie verweist dabei auf Eignungs- und Folgeuntersuchungen und führt bspw § 49 ASchG an, der Gefahren einer Berufskrankheit und somit berufsspezifische und nicht – wie hier aus einer Epidemie resultierende – allgemeine Gesundheitsgefährdungen adressiert. Zu beachten ist, dass dem Arbeitgeber im Fall von Eignungs- und Folgeuntersuchungen nur die Beurteilung über die „Geeignetheit“ mitzuteilen ist,[34] nicht aber das Vorliegen einer Infektion nach COVID-19.

---

26) Vgl § 1157 ABGB, § 3 ASchG, § 18 AngG.

27) Vgl *DSB,* FAQ zum Thema Datenschutz und Coronavirus (Stand 27. 3. 2020), abrufbar unter www.dsb.gv.at/informationen-zum-coronavirus-covid-19-.

28) Vgl auch § 15 Abs 5 ASchG iVm Art 9 Abs 2 lit b DSGVO; *DSB,* FAQ zum Thema Datenschutz und Coronavirus.

29) § 71 Abs 1 AMG iVm Art 9 Abs 2 lit i DSGVO, § 83 Abs 1 Z 7 AMG, wonach die Unterlassung einer unverzüglichen Meldung mit einer Geldstrafe mit bis zu € 7.500,– – im Wiederholungsfall bis zu € 14.000,– – zu bestrafen ist.

30) Vgl *DSB,* FAQ zum Thema Datenschutz und Coronavirus; krit hingegen *Bergauer,* Fragen und Antworten: Gesundheitsdatenerhebungen durch den Arbeitgeber und die Gesundheitsbehörden im Zusammenhang mit dem Corona-Virus (SARS-CoV-2), jusIT digital exklusiv 2020/1, wonach die allgemeine Fürsorge- und Treuepflicht als Rechtsgrundlage nicht den spezifischen Anforderungen der DSGVO entspricht.

31) Vgl *Jahnel,* Handbuch Rz 2/14; *DSB,* FAQ zum Thema Datenschutz und Coronavirus.

32) *DSB,* FAQ zum Thema Datenschutz und Coronavirus.

33) Vgl § 25 EpidemieG iVm § 1 Abs 2 V betreffend medizinische Überprüfungen bei der Einreise iZm dem „2019 neuartigen Coronavirus“ BGBl II 2020/81.

34) Vgl § 52 Z 7 ASchG.

Weitere gesetzliche Untersuchungspflichten finden sich zB für öffentliche Bedienstete im Fall berechtigter Zweifel ihrer gesundheitlichen Eignung[35] sowie für Beschäftigte in Arzneimittelbetrieben,[36] sofern sie mit Arzneimitteln oder mit zur Herstellung von Arzneimitteln verwendeten Behältnissen oder Stoffen in Berührung kommen.

Besteht keine gesetzliche Untersuchungspflicht, bestünde die Möglichkeit einer Einwilligung der Arbeitnehmer, auf die sich der Arbeitgeber idR aber wegen fehlender Freiwilligkeit aufgrund verdünnter Entscheidungsfreiheit der Arbeitnehmer nicht stützen können wird. Dies könnte dadurch entschärft werden, dass entsprechende Informationen zur Verfügung gestellt und Prozesse implementiert werden, die es dem Arbeitnehmer ermöglichen, eine Körpertemperaturmessung durchzuführen (etwa in räumlich abgetrennten Bereichen und durch Arbeitsmediziner) oder aber zu verweigern, ohne dass er mit arbeitsrechtlichen Konsequenzen rechnen muss (zB durch die optionale Möglichkeit der Vorlage eines ärztlichen Attests für die Gewährung des Zutritts auf das Betriebsgelände).

Bei der Implementierung einer verpflichtenden Messung der Körpertemperatur wird es sich regelmäßig um eine betriebsvereinbarungspflichtige Maßnahme handeln.[37] Ob eine Betriebsvereinbarung für sich genommen zugleich eine ausreichende datenschutzrechtliche Rechtsgrundlage begründen kann, ist strittig.[38] Sofern eine Betriebsvereinbarung nicht vorliegt, ist die Pflicht zur Durchführung einer Datenschutz-Folgeabschätzung nach der österr „Blacklist" zu prüfen.[39]

35) § 52 BDG.

36) § 71 AMG iVm Art 9 Abs 2 lit i und Art 6 Abs 1 lit c DSGVO.

37) Vgl § 96 Abs 1 Z 3 ArbVG; für den Fall des Fehlens einer Betriebsvereinbarung ist eine Zustimmung nach § 10 Abs 1 AVRAG erforderlich.

38) Verneinend *Kunnert,* Datenschutz in Fragen & Antworten (2019) Frage 26.A.2. und 5., der § 96 und § 96a ArbVG auf Regelungen der betrieblichen Mitbestimmung beschränkt und ihnen keinen konkreten datenschutzrechtlichen Gehalt zuweist; bejahend *Goricnik* in *Knyrim,* DatKomm Art 88 DSGVO Rz 16, 41 ff (Stand 1. 10. 2018, rdb.at).

39) Vgl § 2 Abs 3 Z 1 und 4 DSFA-V.

SCHLUSSSTRICH

Die Nutzung von Daten aus der Mobilfunktechnologie zur Bekämpfung der COVID-19-Pandemie wäre nur unter genauester Beachtung der Datenschutz-Grundsätze und der Prinzipien von Privacy by Design and Default der DSGVO und bei staatlichen Zwangsmaßnahmen unter Abwägung der verursachten Grundrechtseingriffe und Prüfung des Vorhandenseins gelinderer Mittel umsetzbar. Selbiges gilt für die über bloße Befragungen oder gesetzliche Untersuchungspflichten hinausgehende Erhebung von Gesundheitsdaten von Arbeitnehmern durch Arbeitgeber, wobei diese idR nur bei Schaffung einer echten Freiwilligkeit denkbar ist.

ZIVIL- UND UNTERNEHMENSRECHT
GELEITET VON
G. WILHELM

Zum Haftungsprivileg für Sachverständige

Der OGH judiziert laufend in mehreren Senaten zur Haftung von Sachverständigen. Anhand des vorliegenden Beschlusses des 6. Senats v 27. 11. 2019, 6 Ob 205/19 v, wird die Rsp kritisch hinterfragt. Im gegenständlichen Fall lagen in einem Insolvenzverfahren vom Masseverwalter beauftragte Gutachten zu den Ursachen und dem Zeitpunkt der Insolvenz vor, welche die ehemaligen Organe der Gemeinschuldnerin belasteten.

FELIX MICHAEL KLEMENT

A. Ausgangslage

In dem der Entscheidung (E) zugrunde liegenden Sachverhalt hatte eine Wirtschaftsprüfungsgesellschaft im Auftrag von Masseverwaltern Gutachten erstattet, in welchen sie ua Ursachen und Zeitpunkt der Insolvenz der Gemeinschuldnerin feststellte und analysierte. Die Sachverständigen wurden nicht durch Gerichtsbeschluss des Insolvenzgerichts (§ 81 Abs 4 IO) bestellt.

In den Gutachten wurde festgestellt, dass der Kl Mitverursacher der Insolvenz war und die materielle Insolvenz etwa rund zweieinhalb Jahre vor Insolvenzeröffnung eintrat. Die Aussagen in den Gutachten gaben dem Kl nicht nur Mitschuld an der Insolvenz sondern implizierten darüber hinaus, dass der Kl als Aufsichtsratsvorsitzender der Konzernspitze jahrelang das Vorliegen der materiellen Insolvenz der Unternehmensgruppe nicht erkannte. Die gutachtende Wirtschaftsprüfungsgesellschaft (Bekl) räumte dem Kl bei Erstellung des Gutachtens keine Möglichkeit ein, zu ihren für den Kl negativen Ergebnissen Stellung zu nehmen. Die Gutachten gelangten an die Öffentlichkeit.

RA Dr. *Felix Michael Klement,* MBA, ist Partner bei Wildmoser/Koch und Partner GmbH in Wien (am Verfahren beteiligt).