Dr. Matthias Lachenmann

Datenschutz vs. Corona-Virus – Handlungsempfehlungen für Unternehmen bei Schutzmaßnahmen

Das neuartige Corona-Virus („Sars-CoV-2“) sorgt aktuell auf der Welt für gravierende Probleme. Die Weltgesundheitsorganisation (WHO) hat am 11.3.2020 die Situation zu einer Pandemie erklärt. Aufgrund der schnellen Ausbreitung des Virus ist die Situation schwer kontrollierbar. Die stetig wachsende Zahl der Infizierten verlangt, dass geeignete Abwehrmaßnahmen zum Schutz der Mitarbeiter/-innen und des Unternehmens getroffen werden. In diesem Beitrag soll kurz dargestellt werden, in welchem Umfang Unternehmen Gesundheitsdaten zu Schutz- und Präventionsmaßnahmen verarbeiten dürfen.

Die Qualifizierung als Gesundheitsdaten

Informationen, die bei Maßnahmen zum Schutz vor dem Corona-Virus erhoben werden, sind meist als Gesundheitsdaten zu klassifizieren, so dass ihre Verarbeitung besonders hohen Anforderungen unterliegt. Speichert ein Unternehmen z. B. die Information, dass ein Mitarbeiter Symptome des Virus zeigt oder gibt ein Mitarbeiter den Namen einer möglicherweise infizierten Person an das Unternehmen weiter, handelt es sich dabei um Gesundheitsdaten nach Art. 4 Nr. 15, Erwägungsgrund 35 DSGVO. Daten, die das Unternehmen durch Selbstauskünfte oder Fragebögen der Mitarbeiter oder Externer erhält, um den aktuellen Gesundheitsstand abzufragen, stellen ebenso schützenswerte sensible Daten dar.

Demgegenüber handelt es sich nur um „reguläre“ personenbezogene Daten, wenn anlassbezogene Befragungen nach Dienstreisen oder Erhebung von Kontaktdaten und -personen zur Information über eine Infektion durchgeführt werden. Ein manueller Fiebertest ohne weitere Verarbeitung von Informationen würde hingegen bereits keine Verarbeitung personenbezogener Daten darstellen (kann für Arbeitnehmer aber von § 26 Abs. 7 BDSG erfasst sein).

Mögliche Rechtsgrundlagen bei der Verarbeitung von Gesundheitsdaten

Gesundheitsdaten unterliegen dem Verarbeitungsverbot gem. Art. 9 Abs. 1 DSGVO, der strengere Anforderungen als der für reguläre Datenverarbeitung geltende Art. 6 Abs. 1 DSGVO zur Folge hat. Die Fälle, in denen eine Verarbeitung zugelassen ist, sind in Art. 9 Abs. 2 DSGVO normiert. Als Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten im Zusammenhang mit Maßnahmen zum Schutz vor Corona Virus kommen verschiedene Erlaubnistatbestände des Art. 9 Abs. 2 DSGVO in Betracht.

Der deutsche Gesetzgeber hat allerdings von den in Art. 9 Abs. 2 DSGVO gegebenen Möglichkeiten, spezielle Gesetze zum Schutz vor Epidemien/Pandemien zu erlassen und dazu Unternehmen eine Verarbeitung von Gesundheitsdaten zu gestatten, keinen eindeutigen Gebrauch gemacht (auch nicht strengere Vorgaben nach Art. 9 Abs. 4 DSGVO). Es wurden lediglich im nationalen Recht eine Konkretisierung verschiedener Vorschriften vorgenommen. So wurde in § 22 BDSG i. V. m. Art. 9 Abs. 2 lit. g DSGVO die Möglichkeit vorgesehen, Gesundheitsdaten zu verarbeiten. Unternehmen, die als nichtöffentliche Stellen zu qualifizieren sind, können unter bestimmten Voraussetzungen ihre Datenverarbeitung auf § 22 Abs. 1 Nr. 1 BDSG stützen.

Soweit Gesundheitsdaten der eigenen Mitarbeiter verarbeitet werden, sind § 26 Abs. 3 BDSG i. V. m. Art. 9 Abs. 2 lit. b DSGVO einschlägig; bei sonstigen Daten insbes. Art. 6 Abs. 1 S. 1 lit. b, c und f DSGVO. Maßnahmen gegenüber Besuchern können bei regulären Daten auf Art. 6 Abs. 1 S. 1 lit. f DSGVO gestützt werden. Soweit Gesundheitsdaten von Nicht-Beschäftigten verarbeitet werden, kann Art. 9 Abs. 2 lit. i DSGVO i. V. m. § 22 Abs. 1 Nr. 1 lit. c BDSG als Rechtsgrundlage herangezogen werden.

Konkrete Maßnahmen

Fragebögen und Selbstauskünfte

Unternehmen können durch Selbstauskunfts- oder Fragebögen zum Aufenthaltsort und zu Symptomen die entsprechenden Daten ihrer Mitarbeiter erheben und speichern. Zunächst können Daten erhoben werden, die den Aufenthaltsort oder die Kontaktpersonen betreffen (z. B. zu Zeitpunkt, Orten und Kontaktpersonen des Bezugs, sowie die Kontaktdaten). Die Rechtsgrundlage zur Erhebung dieser Daten, die nicht als Gesundheitsdaten zu klassifizieren sind, ist Art. 6 Abs. 1 S. 1 lit. f DSGVO. Fragt das Unternehmen demgegenüber explizit nach dem Gesundheitszustand der betroffenen Person (z. B. „Haben Sie Symptome, und wenn ja, welche?“) handelt es sich um eine Verarbei-

tung sensibler Daten, die sich nur über Art. 9 Abs. 2 lit. g DSGVO i. V. m. § 26 Abs. 3 BDSG rechtfertigen lässt.

Im Falle eines positiven Befunds bei einem Mitarbeiter (durch eine offizielle Stelle) oder sogar bei einem bestätigten Kontakt zu einer positiv getesteten Person muss es zulässig sein, Informationen über den betroffenen Mitarbeiter zu verarbeiten, z. B. Zeitpunkt und enge Kontaktpersonen sowie ergriffene Maßnahmen. Das Statement der Datenschutzkonferenz (siehe auch der Beitrag „Aktuelles aus den Aufsichtsbehörden", S. 98 – in diesem Heft) macht deutlich, dass die Verarbeitung von Gesundheitsdaten von Beschäftigten, zur Eindämmung und Bekämpfung der Corona-Pandemie, als datenschutzrechtlich legitimiert betrachtet werden können. Hierzu gehören insbesondere Informationen in den Fällen, in denen eine Infektion festgestellt wurde oder in denen ein Aufenthalt in einem Risikogebiet stattgefunden hat. Es dürfte daher zulässig sein, von allen Mitarbeitern verpflichtend die Information von Reisezielen und Gesundheitszustand abzufragen (eine andere Auffassung vertritt jedoch die französische Aufsichtsbehörde CNIL).

Veröffentlichung der Namen Infizierter

Die Offenlegung von Gesundheitsinformationen von Infizierten oder Verdachtspersonen, um Mitarbeiter zu informieren, kann nur rechtmäßig sein, wenn die Kenntnis der Identität für die Mitarbeiter unerlässlich ist. Wird ein Mitarbeiter eines Unternehmens positiv getestet, dürfte es für den Arbeitgeber verpflichtend sein, die bekannten Kontakte zu informieren.

Kann in einem Unternehmen nicht mehr festgestellt werden, mit wem Kontakt bestand, müssen im Zweifel alle Kollegen/-innen informiert werden. Die Informationen sollten per E-Mail oder auf sonstigen persönlichen Wegen erfolgen, nicht über Aushänge am „schwarzen Brett" od. ä. Soweit keine konkrete Namensnennung erforderlich ist – insbesondere bei klar getrennten Abteilungen oder einer schon erfolgten Aufteilung in verschiedene Teams – dürfte es ausreichen, die Mitarbeiter ohne Nennung der Identität des Infizierten über die Situation zu informieren und weitere Vorsichtsmaßnahmen zu treffen.

Fiebermessungen

Die Fiebermessung von Mitarbeitern am Eingang des Betriebsgeländes und sonstige ärztlich empfohlene medizinische Maßnahmen (z. B. Inspektion des äußeren Gesundheitszustandes auf Schwitzen oder Husten) können unter engen Voraussetzungen mit § 26 Abs. 3 BDSG gerechtfertigt werden. Eine Fiebermessung kann durchaus als zulässig angesehen werden, wenn die Ergebnisse nur für eine Einlasskontrolle mit Entscheidung Zutritt ja/nein genutzt werden oder wenn die Maßnahmen rein freiwillig ohne Nutzungsverpflichtung sind.

Kritisch wäre es zu bewerten, wenn eine verpflichtende Fiebermessung für alle Mitarbeiter durchgeführt würde und eine festgestellte hohe Temperatur zu sofortigen Maßnahmen wie Freistellung od. ä. führen würden (schon allein, da die Temperatur kein definitives Kriterium zur Feststellung einer Infektion ist). Solche Maßnahmen mit weiterer Datenverarbeitung können vor allem gerechtfertigt sein, wenn Mitarbeiter spezielle Bereiche betreten, in denen eine Weitergabe der Infektion möglicherweise zum Stillstand des Unternehmens führen würde (z. B. Vorstandsetage, Produktionsstraßen). Die Zulässigkeit dieser Maßnahmen wird man wohl auch im Bereich der Lebensmittelproduktion od. ä. bejahen können.

Home Office

Immer mehr Arbeitgeber fordern ihre Mitarbeiter auf, von zu Hause aus zu arbeiten. Datenschutzrechtliche Risiken bestehen im Hinblick auf unerlaubten Zugriff durch Dritte und eine nicht ausreichende IT-Sicherheit. Die Übertragung der Daten von den Heimarbeitsplätzen muss mittels verschlüsselter elektronischer Kommunikationswege stattfinden, z. B. VPN-Verbindungen oder über ein zur Verfügung gestelltes Portal mit Authentifizierung über Sicherheitstoken.

Weiterhin sollten die Laptop-Festplatten verschlüsselt sein, Zugriffe auf das VPN protokolliert und eine Home Office-Vereinbarung mit den Beschäftigten getroffen werden, die den Rahmen festlegt. Beschäftigte sollten zusätzlich verpflichtet werden, Zugriff auf Unternehmensinformationen durch Dritte zu unterbinden und unbenutzte Arbeitsmittel sicher zu verstauen. Bei zeitweisem Verlassen des Arbeitsplatzes ist der Laptop zu sperren, generell ist eine automatische Sperrung nach kurzer Zeit mit Passwortschutz beim Zugriff zu gewährleisten.

Handyortung von Infizierten

Diskutiert wird zudem die Handyortung von Infizierten, um Kontaktpersonen besser ermitteln zu können, oder die Nennung konkreter Adressen von Infizierten zu ermöglichen. Diese Maßnahme könnte allerdings nur durch den Staat durchgeführt werden und nicht individuell durch einzelne Unternehmen.

Das European Data Protection Board (EDPB) äußerte sich zur Verarbeitung von mobilen Standorten am 16.3.2020 dahingehend zutreffend, dass aufgrund nationaler Gesetze die Standortdaten vom Betreiber nur verwendet werden dürfen, wenn die Zustimmung der betroffenen Personen eingeholt wurde oder die Daten anonymisiert erhoben werden. Behörden sollen zunächst eine anonymisierte Verarbeitung der Daten anstreben, um beispielsweise die Konzentration von mobilen Geräten an einem bestimmten Ort festzustellen.

Das EDPB sieht Art. 15 der Datenschutzrichtlinie für elektronische Kommunikation als Rechtsgrundlage für die Mitgliedsstaaten nationale Regelungen zu erlassen, die der Gewährleistung der nationalen und öffentlichen Sicherheit dienen. Diese Form der Notstandsgesetzgebung kann unter den Voraussetzungen möglich sein, dass sie eine notwendige, angemessene und verhältnismäßige Maßnahme innerhalb einer demokratischen Gesellschaft darstellt. Aus grundrechtlichen Erwägungen heraus sind solche Maßnahmen aber sehr kritisch zu betrachten.

Maßnahmen gegen Besucher des Unternehmens

Unternehmen können sich bei Maßnahmen gegen Besucher oder sonstige Externe nicht auf § 26 Abs. 3 BDSG stützen. Maßnahmen, die nicht dazu führen, dass Daten verarbeitet werden (z. B. mündliche Befragung über den Gesundheitszustand, manuelle Fiebermessung) sind möglich. Weiterhin bleibt dem Unternehmen stets, die Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO der Betroffenen einzuholen, die freiwillig sein und konkreten Bezug auf die Verarbeitung von Gesundheitsdaten nehmen muss.

Nach dem Statement der DSK, das durch die neueste Aussage des EDPB vom 16.3.2020 gestützt wird, sind auch weitergehende Maßnahmen gegen Besucher zulässig. Danach sind Maßnahmen, die zu einer Verarbeitung von Gesundheitsdaten von Besuchern führen, gerechtfertigt, insbesondere, wenn festgestellt werden soll, ob jene infiziert sind oder sich in einem Risikogebiet aufgehalten haben. Zur Feststellung einer Infizierung gehören auch Maßnahmen der Fiebermessung oder der Ausfüllung eines Fragebogens, sodass diese ohne Einwilligung möglich sein müssen, wenn der Zweck der Eindämmung und Bekämpfung des Corona-Virus erfüllt werden soll.

Unternehmen können im ersten Schritt Maßnahmen ergreifen, die keine Datenverarbeitung darstellen und daher keinen besonderen Vorgaben, nur z. B. dem Hausrecht oder Arbeitsrecht unterworfen sind. Dazu können die Einschränkung von Besuchsmöglichkeiten, Hinweisschilder, strengere Hygienevorschriften oder konkrete Handlungsempfehlungen zum Schutze Aller gehören.

Formale Vorgaben nach der DSGVO

Bei der Verarbeitung der Gesundheitsdaten trotz der Ausnahmesituation sind die formalen Vorgaben der DSGVO zu beachten. So müssen betroffene Personen nach Art. 13 DSGVO über den Zweck der Verarbeitung und die rechtliche Grundlage informiert werden. Insbesondere bei der Verarbeitung von Besucherdaten sollten entsprechende Datenschutzerklärungen vorbereitet werden. Dort ist auch aufzuführen, wie lange die Daten gespeichert bleiben sollen und welche weiteren Maßnahmen, z. B. ggf. Weitergabe der Daten an Behörden, erforderlich werden können.

Zudem müssen die neuen Vorgänge über die Aufzeichnungen in Zeiten der Corona-Krise in das Verarbeitungsverzeichnis nach Art. 30 DSGVO aufgenommen werden. Weiterhin ist zu bedenken, dass in verschiedenen Fällen eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchgeführt werden muss, die aber ggf. zum jetzigen Zeitpunkt kürzer ausfallen kann.

Im Ausgleich für eine Einschränkung von Betroffenenrechten aufgrund der Extremsituation sind die personenbezogenen (Gesundheits-)Daten grundsätzlich in gesonderten Datenbanken zu speichern, die einem speziellen Zugriffs- und Berechtigungskonzept unterliegen und eine zeitnahe Löschung nach Zweckerreichung gewährleisten können. Höhere IT-Sicherheitsmaßnahmen können unerlaubte Zugriffe auf sensible Daten verhindern.

Fazit

Unternehmen können und sollen zur Eindämmung der Pandemie geeignete Abwehrmaßnahmen treffen. Dies kann insbesondere in Form von Fragebögen zur Kontaktaufnahme oder Feststellung einer möglichen Erkrankung erfolgen. Dabei sollten die verarbeiteten Daten in getrennten Datenbanken/Akten gespeichert werden, um eine zeitnahe Löschung zu ermöglichen.

Eine Einschränkung der datenschutzrechtlichen Problematik kann erreicht werden, wenn Kontrollen ohne Datenverarbeitung durchgeführt werden. Dazu können z. B. zählen eine mündliche Befragung oder lediglich manuelle Fiebermessung, ohne Speicherung der Daten. Die Sensibilisierung der Mitarbeiter, die Einrichtung von Kommunikationskanälen, sowie Hinweisschilder mit Handlungsempfehlungen und Hygienevorschriften bleiben praktikable und effektive Schutzmaßnahmen.

Autor: **Dr. Matthias Lachenmann ist Rechtsanwalt und Partner bei der Kanzlei BHO Legal PartG mbB in Köln. Er ist auf die Beratung im Technologie- und Datenschutzrecht spezialisiert, insbesondere mit Fokus auf internationalen Konzerndatenschutz, Beschäftigtendatenschutz und Industrie 4.0**