Kapellmann
Rechtsanwälte

Corona-Krise – Pause für den Datenschutz? Was sagen die Aufsichtsbehörden? Was ist zu beachten?

02. April 2020

In den vergangenen Tagen haben sich die deutschen Datenschutzaufsichtsbehörden verstärkt zu Wort gemeldet und mahnend an die Einhaltung datenschutzrechtlicher Pflichten erinnert. Zahlreiche Behörden und andere Stellen haben eine Fülle an Handlungsanweisungen und FAQs zum Umgang mit personenbezogenen Daten in der Krise veröffentlicht. Auch mit den aktuellen Diskussionen um die Einführung einer Tracking-App zur Erkennung von Corona-Infektionsketten, die Zulässigkeit der seitens einiger Unternehmen eingeführten Pflicht zum Fiebermessen vor Arbeitseintritt sowie mögliche Datenschutzverstöße bei Nutzung bestimmter Videokonferenzlösungen rückt der Datenschutz wieder verstärkt in den Fokus.

Wenngleich der Schutz der Gesundheit der Bevölkerung ohne Frage Vorrang hat und – wie es die brandenburgische Datenschutzaufsichtsbehörde formuliert – „der Datenschutz aktuell nicht die Hauptsorge aller Beteiligten sein dürfte", sind Einschränkungen des Datenschutzes und die Vernachlässigung damit verbundener Pflichten nur im absolut notwendigen Umfang hinnehmbar. Datenschutzrechtliche Versäumnisse, die mit der gezwungenermaßen schnellen Umstellung auf Remote-Arbeit einhergegangen sind, sollten daher schnellstmöglich ausgeräumt werden.

Der nachstehende Überblick gibt wichtige Hinweise, wie die Aufsichtsbehörden mit datenschutzrechtlichen Versäumnissen umgehen und was bei Homeoffice-Arbeit, dem Einsatz von Videokonferenzsystemen und in der Personalarbeit in diesen besonderen Zeiten zu beachten ist.

1. Auswirkungen der Corona-Pandemie auf die Arbeit der Datenschutzaufsichtsbehörden

Angesichts der gegenwärtigen Pandemie-Entwicklung haben auch die deutschen Datenschutzaufsichtsbehörden auf einen Notbetrieb umgestellt. Deshalb kann es bei den Behörden ebenfalls zu Verzögerungen bei der Bearbeitung von Anfragen und Beschwerden kommen. Allerdings betonen die Behörden, dass sie ihren Aufsichts- und Kontrollaufgaben nach wie vor nachgehen werden und selbst – oder vielmehr gerade – in gesellschaftlichen Ausnahmezeiten wie der aktuellen Corona-Pandemie Datenschutz und Datensicherheit – nicht zuletzt auch angesichts des steigenden Risikos von Cyberangriffen und anderer Datenschutzverletzungen – nicht vernachlässigt werden dürfen.

Gleichwohl haben einige Behörden mitgeteilt, Verständnis für verlängerte Reaktionszeiten bei Unternehmen zu haben und bestehende Fristen – soweit die DS-GVO dies zulässt – derzeit aufgrund der Covid-19-Pandemie im erforderlichen Umfang großzügiger zu bemessen. Für die Meldung von Datenpannen und Datenschutzverletzungen hat der Hamburgische Datenschutzbeauftragte etwa verlautbart, dass der Wortlaut des Art. 33 Abs. 1 DS-GVO, wonach erforderliche **Meldungen von Datenschutzverletzungen** „unverzüglich" und „möglichst" binnen 72 Stunden erfolgen müssen, eine Berücksichtigung pandemiebedingter Einschränkungen der Arbeitsfähigkeit grundsätzlich zulasse. Wichtig ist jedoch, dass etwaige Sicherheitslücken unverzüglich geschlossen werden und dass erforderliche Meldungen an die Aufsichtsbehörde nicht unnötig verzögert werden. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) betont ebenfalls, dass die Pflicht zur unverzüglichen Meldung von Datenschutzverletzungen auch in der derzeitigen Krisensituation wichtig sei, da nur so wirksame Folgemaßnahmen zum Schutz der Betroffenen aber auch der Allgemeinheit gewährleistet werden könnten (vgl. › **hier**). Auch in der aktuellen Lage ist es deshalb wichtig, Datenschutzverletzungen möglichst sofort nachzugehen und zu prüfen, inwieweit betroffenen Personen ein Schaden oder sonstige Nachteile drohen (z.B. bei Verlust von Kreditkartendaten). Eine Ausnahme von der Meldepflicht besteht dabei nur, wenn die Datenschutzverletzung „voraussichtlich" nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen

führt (vgl. Art. 33 DS-GVO).

Die für die **Erfüllung der Betroffenenrechte (z.B. Auskunft- oder Löschersuchen)** geltenden starren Fristen der DS-GVO bieten indessen weniger Flexibilität. Betroffene Personen haben – auch in Krisenzeiten – beispielsweise das Recht, von jedem Verantwortlichen binnen eines Monats Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten (Art. 12 Abs. 3 DS-GVO). Eine Verlängerung ist nach dem Wortlaut der DS-GVO nur ausnahmsweise möglich, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Allerdings hat jedenfalls der Hamburgische Datenschutzbeauftragte angekündigt, im Rahmen seines Einschreiteermessens einzelfallbezogen von einer Verfolgung pandemiebedingter Fristversäumnisse abzusehen. Bei der Beurteilung werde es, so die Aussage, entscheidend auf die Länge der Überschreitung sowie die Unternehmensgröße und die damit verbundene berechtigte Erwartung an die Professionalität des Verantwortlichen ankommen.

Demgegenüber sollen seitens der Aufsichtsbehörden z.B. **in laufenden aufsichtsbehördlichen Verfahren gesetzte Fristen** für Stellungnahmen während der Zeit der Pandemie jedoch nach Angaben der hamburgischen Aufsichtsbehörde großzügiger bemessen werden. Es ist davon auszugehen, dass die Aufsichtsbehörden in anderen Bundesländern gleichermaßen verfahren werden. Für in Bayern ansässige Unternehmen hat das BayLDA sogar eine generelle Verlängerung bis zum 20.04.2020 für solche aufsichtsbehördlich gesetzten Fristen bewilligt, die früher ablaufen würden. Darüber hinausgehende Fristverlängerungen können mit entsprechender Begründung beantragt werden (vgl. › **hier**).

Und auch von dem **Erlass von Bußgeldbescheiden wegen Datenschutzverstößen** will die Hamburger Aufsichtsbehörde zur Entlastung von Unternehmen und Gewerbetreibenden während der Corona-Krise absehen. Inwieweit andere Behörden diese Haltung teilen, ist jedoch nicht bekannt.

2. Was ist bei der Verwendung von Videokonferenz-Tools zu beachten?

Aufgrund des deutschlandweit geltenden Kontaktverbotes und der Umstellung zahlreicher Unternehmen auf Homeoffice hat die Arbeitswelt in den letzten Wochen eine rasante Digitalisierung erfahren, die gewissermaßen über Nacht zum Umdenken und Schaffen schneller Lösungen zur bestmöglichen Aufrechterhaltung des Daily Business gezwungen hat. Um den persönlichen Kontakt zu Kollegen und Geschäftspartnern beizubehalten und wichtige Meetings auch weiterhin Face-to-Face durchführen zu können, wird verstärkt auf Videokonferenzsysteme gesetzt. Vor-Ort-Schulungen werden abgesagt, an deren Stelle treten Webinare. Das gemeinsame Feierabend-Bier wird durch das virtuelle Bier ersetzt. Dies alles geschieht unter Zuhilfenahme verschiedener externer Anbieter.

Angesichts der kurzen Reaktionszeit und dadurch bedingten Notwendigkeit zu schnellem Handeln verwundert es nicht, dass datenschutzrechtlichen Anforderungen bei dem Einsatz solcher Lösungen bislang nur wenig Beachtung geschenkt worden ist. Spätestens jetzt,

nachdem die Umstellung auf Remote-Arbeit in vielen Unternehmen erfolgt ist und das Tagesgeschäft aufrechterhalten wird, sollten datenschutzrechtliche Versäumnisse und damit einhergehende Risiken ausgemacht und beseitigt werden. Bedingt durch die Vielzahl der Anbieter (Freeware/Open-Source/kommerzielle Anbieter) kann kein allgemeingültiges Handlungskonzept präsentiert werden. Entscheidend ist stets eine Einzelfallbetrachtung, die je nach Tool und Softwarelösung stark variieren kann. Folgende Checkliste dient als Leitfaden, welche Punkte geklärt und ggf. umgesetzt werden sollten:

Was habe ich bei der Auswahl von Videokonferenz- und Webinarsystemen zu beachten?

Bei der Auswahl des Dienstes ist besonders darauf zu achten, dass die angebotene Lösung eine datenschutzkonforme und -freundliche Nutzung ermöglicht. Insbesondere muss der Anbieter **hinreichende Datensicherheitsvorkehrungen** („technische und organisatorische Maßnahmen", kurz: TOM) gewährleisten. Grundsätzlich sollten deshalb spezielle Business-Lösungen für die geschäftliche Kommunikation eingesetzt werden, da diese in aller Regel deutlich höhere Standards hinsichtlich Sicherheit und Vertraulichkeit der ausgetauschten Informationen als für den Privatbereich entwickelte Tools erfüllen. Auch wird empfohlen, nach Möglichkeit Anbieter aus der EU auszuwählen, da diese der DS-GVO unterliegen und den **europäischen Datenschutzstandard** vorhalten müssen. Daraus darf selbstverständlich nicht geschlossen werden, dass außereuropäische Anbieter (z.B. aus den USA) per se kein angemessenes Datenschutzniveau gewährleisten. Durch zusätzliche Garantien können vielmehr auch solche Anbieter eine sichere Nutzung ihrer Dienste sicherstellen (siehe dazu unten).

In jedem Fall sollte eine **hinreichende Verschlüsselung** bei der Datenübertragung gewährleistet sein. Auch sollte z. B. durch automatisierte Löschroutinen sichergestellt werden, dass erfasste und ausgetauschte Informationen, Kommunikationsinhalte sowie geteilte Dokumente nur solange wie notwendig bereitgestellt und gespeichert werden. Mit Blick auf den Grundsatz der **datenschutzfreundlichen Voreinstellungen** („Privacy by Default") sollte das Tool zudem „ab Werk" so konfiguriert sein, dass standardmäßig Daten der Teilnehmer nur im erforderlichen Umfang erfasst und übermittelt werden, insbesondere etwaige Trackingmechanismen oder Datenanalysen des jeweiligen Anbieters deaktiviert sind. Ob dies tatsächlich der Fall ist, sollte jedoch zur Vermeidung von Haftungsrisiken stets vor Einsatz des Tools überprüft und ggf. durch eigene Konfiguration der Einstellungen sichergestellt werden.

Es empfiehlt sich zudem, nur solche Dienste zu verwenden, bei denen **keine Ton- und Videomitschnitte** – jedenfalls nicht ohne die erforderliche Einwilligung der Teilnehmer – möglich sind. Aus Sicht der baden-württembergischen Datenschutzaufsicht sollte für Teilnehmer darüber hinaus die Möglichkeit bestehen, auch ohne aktive Videokamera an einem Meeting teilzunehmen, gerade in der aktuellen Zeit, in der viele Konferenzen aus den Privatwohnungen heraus erfolgen (vgl. › **hier**).

Aber auch hier ist auf den jeweiligen Einzelfall abzustellen. Im Rahmen von Online-Fortbildungskonferenzen kann beispielsweise ein sog. „Aufmerksamkeitstracking" bei

entsprechender Information der Teilnehmer zulässig sein, damit ein Nachweis – etwa bei Pflichtfortbildungen – über die „aktive" Teilnahme geführt werden kann.

In jedem Fall gilt: Die Klärung dieser Details obliegt – wie die baden-württembergische Aufsichtsbehörde klargestellt hat – den Verwendern dieser Systeme. Diese sind für den datenschutzkonformen Einsatz solcher Systeme verantwortlich und sollten sich daher bereits bei Auswahl einen Überblick über Vertragsbedingungen, Funktionsweise und Datenflüsse verschaffen (vgl. › **hier**).

Bedarf es eines gesonderten Abschlusses von Auftragsverarbeitungsverträgen?

Grundsätzlich ja! Anbieter von Videokonferenz- und Webinar-Lösungen sind in aller Regel sog. Auftragsverarbeiter (Art. 28 DS-GVO). Das bedeutet, dass der Anbieter Daten der Teilnehmer nur im Auftrag und entsprechend der Weisungen des Auftraggebers verarbeitet. Die meisten Anbieter bieten derartige Auftragsverarbeitungsverträge (Data Processing Agreement) standardmäßig an, die gesondert abzuschließen sind. Teilweise sind Auftragsverarbeitungsverträge auch Bestandteil der Nutzungsbedingungen und werden mit ihrer Akzeptanz „automatisch" abgeschlossen. Dann sollte lediglich überprüft werden, ob diese Verträge den Vorgaben des Art. 28 Abs. 3 DS-GVO genügen. Zu Klärung dieser Frage sollte ein Blick in die Vertragsbestimmungen (und nicht auf die Datenschutzhinweise des Anbieters) geworfen werden.

Zu beachten ist: Sobald der Web-Tool-Anbieter auch Verarbeitungen zu eigenen Zwecken (z. B. eigene Nutzungsanalysen, Trackingmechanismen, Profiling) durchführt und hierbei auf die Daten der Teilnehmer zugreift (z.B. Name, Telefonnummer, IP), liegt regelmäßig keine Auftragsverarbeitung vor. Vielmehr kann dann eine sog. gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) vorliegen, die weitergehende Haftungsrisiken birgt. Von der Nutzung solcher Dienste wird daher abgeraten.

Bedarf es einer Datenschutzinformation durch den Einladenden?

Grundsätzlich ja! Als datenschutzrechtlich „Verantwortlicher" ist der Verwender eines Webkonferenz- oder Webinardienstes verpflichtet, die Konferenzteilnehmer (Mitarbeiter, Kunden, Geschäftspartner) über bestimmte Umstände der Datenverarbeitung bei Nutzung des Dienstes zu informieren. Dies gilt selbst dann, wenn der Anbieter des Tools entsprechende eigene Datenschutzinformationen bereitstellt. Es empfiehlt sich daher, entsprechende Hinweise in die eigene Datenschutzerklärung aufzunehmen und darin ggf. auf die Datenschutzhinweise des jeweiligen Anbieters ergänzend zu verweisen. In der Einladung oder auf der Anmeldeseite zur Konferenz sollten die Datenschutzhinweise dann z.B. über einen bereitgestellten Link für die Teilnehmer abrufbar sein.

Wie sollen diese Datenschutzhinweise ausgestaltet sein?

Ebenso wie die „bekannten" Datenschutzhinweise (z.B. Datenschutzerklärung auf einer Website)

müssen auch die Hinweise für die Nutzung von Webkonferenz- und Webinarsystemen den Mindestinhalt von Art. 12 bis 14 DS-GVO widerspiegeln. Zusätzlich empfiehlt die baden-württembergische Aufsichtsbehörde, dass den Teilnehmern Hinweise gegeben werden, wie die Web-Tools besonders datensparsam genutzt, also welche Einstellungen zur Datenminimierung vorgenommen werden können (vgl. › **hier**).

Was ist bei Anbietern und Diensten außerhalb der EU / des EWR zu beachten?

Ob bei Nutzung von Web-Diensten Daten in ein Land außerhalb der EU bzw. des EWR (sog. Drittland) – und damit außerhalb des Geltungsbereichs der DS-GVO – übertragen werden, ist einzelfallbezogen zu beurteilen. Es kommt insoweit auf den konkreten Anbieter sowie darauf an, wo der Dienst gehostet wird. Datenübermittlungen in ein Drittland – und damit die Nutzung entsprechender Dienste – sind nur unter besonderen Voraussetzungen zulässig (Art. 44 ff. DS-GVO). Durch zusätzliche Garantien muss gewährleistet sein, dass das Datenschutzniveau der EU eingehalten wird. Für einige Länder hat die Europäische Kommission ein angemessenes Datenschutzniveau ausdrücklich festgestellt. Andere Garantien sind bspw. Standardvertragsklauseln, Binding Corporate Rules oder eine Verpflichtung unter das EU-US-Privacy Shield.

Welche internen Funktionsträger müssen vor Einsatz von Web-Tools eingebunden werden?

Die Entscheidung zur Nutzung von Webkonferenz- und Webinarsystemen obliegt grundsätzlich der Geschäftsführung / dem Vorstand. Darüber hinaus wird – soweit vorhanden – der Betriebsrat einzubinden sein, da sich derartige Systeme zumindest objektiv regelmäßig zur Überwachung der eigenen Mitarbeiter eignen (§ 87 Abs. 1 Nr. 6 BetrVG). Ferner sollte der Datenschutzbeauftragte in die Auswahl mit einbezogen werden; zwingend notwendig ist dies allerdings nicht.

Welche Regeln müssen Mitarbeiter bei der Nutzung solcher Systeme beachten?

Ferner sind bei der Nutzung der Systeme durch die Mitarbeiter einige Grundregeln zu beachten: Eine Teilnahme an der Webkonferenz sollte nur mittels eines Logins oder durch Freigabe des Organisators möglich sein. Andernfalls besteht die Gefahr, dass „ungewünschte" Teilnehmer in Meetings beitreten. Besonders sensible oder vertrauliche Informationen sollten grundsätzlich nicht ausgetauscht werden. Auch bei dem Teilen von Dokumenten oder des eigenen Bildschirms ist streng darauf zu achten, dass solche Inhalte nur im erforderlichen Umfang gezeigt werden. Ebenso sollte vermieden werden, dass im Hintergrund des Teilnehmers keine vertraulichen Dokumente sichtbar sind (z.B. beschriftete Leitz-Ordner). Zu diesem Zweck verfügen viele Tools über die Möglichkeit, den Hintergrund vollständig unkenntlich zu machen oder auszublenden (sog. Blurring-Funktion) und so – gerade im Homeoffice – die Privatsphäre zu schützen. Durch entsprechende Handlungsanweisungen sollten die Mitarbeiter insoweit sensibilisiert werden.

3. Nochmals in Kürze: Was ist sonst bei der Umstellung auf Homeoffice zu beachten?

Bei der Verlagerung von Tätigkeiten in Telearbeit oder Mobiles Arbeiten sind einige grundsätzliche Anforderungen, insbesondere solche an die Datensicherheit zu beachten. Aufgrund eingeschränkter Kontroll- und Einflussmöglichkeiten des Arbeitgebers sowie notwendiger Datenübermittlungen bei Remote-Zugriffen ist das Risiko eines Datenmissbrauchs und unberechtigter Zugriffe von außen durch Unbefugte deutlich höher. Deshalb sind Unternehmen verpflichtet, speziell für die Homeoffice-Arbeit angemessene technische und organisatorische Maßnahmen zu implementieren, um einen hinreichenden Schutz der Daten zu gewährleisten. Die DS-GVO regelt das Erfordernis, personenbezogene Daten durch hinreichende und dem Risiko jeweils angemessene Datensicherheitsvorkehrungen zu schützen, explizit in Art. 25, 32 DS-GVO. Für andere Daten, insbesondere Geschäfts- und Betriebsgeheimnisse sowie andere vertrauliche geschäftliche Informationen gilt selbstverständlich mit Blick auf regelmäßig mit Geschäftspartnern vertraglich vereinbarte Vertraulichkeitspflichten nichts anderes. Solche Datensicherheitsvorkehrungen für den Homeoffice-Bereich sind zum Beispiel:

- Zugriff auf die firmeninterne Infrastruktur über ein VPN, das die Verbindung zum firmeninternen Netz durch eine ausreichend starke Verschlüsselung schützt, und/oder Nutzung sicherer Cloud-Lösungen mit automatischen Backup-Funktionen
- Verschlüsselung und sicherer Passwortschutz von Endgeräten und Datenträgern, ggf. Sperrung von USB-Zugängen und anderen Anschlüssen
- Nutzung sicherer Kommunikationssysteme/ Messenger-Dienste
- Einsatz sicherer und datenschutzkonformer Video- oder Telefonkonferenzsysteme (insb. Anbieter außerhalb der EU/des EWR nur bei Bestehen erforderlicher Datenschutzgarantien und unter Deaktivierung etwaiger Datenanalysen, Profiling- oder Trackingmechanismen seitens des Anbieters)
- IT- und Datenschutzrichtlinie einschließlich Verhaltensrichtlinien für Mitarbeiter für sicheres Arbeiten im Homeoffice und im öffentlichen Raum, u.a.
    - Verwendung sicherer privater Internet-Anschlüsse
    - Untersagung der privaten Nutzung beruflich zur Verfügung gestellter Arbeitsgeräte
    - Untersagung der Nutzung privater Hard- und Software für berufliche Zwecke oder im Falle von BYOD ausschließlich Verwendung privater Endgeräte mit entsprechenden Sicherheitsvorkehrungen und Sicherheitssoftware (neueste Updates installiert, Virenschutz, Firewall etc.)
    - Verwendung verschlüsselter firmeneigner Datenträger
    - Sichere Aufbewahrung und Schutz betrieblicher Unterlagen, Datenträger und Endgeräte vor Einsichtnahme und Zugriff seitens unbefugter Personen, insb. Sichtschutz, Aktivieren

der automatischen Bildschirmsperre beim Verlassen des Arbeitsplatzes und kein unbeaufsichtigtes Liegenlassen von Unterlagen und Datenträgern
    - Keine Weiterleitung beruflicher E-Mails an private Postfächer
    - Datenschutzkonforme Vernichtung von Papierdokumenten
    - Sofortige Meldung von Störungen oder datensicherheitsrelevanten Auffälligkeiten bei der EDV-Arbeit
- Sensibilisierung und dokumentierte Verpflichtung der Mitarbeiter auf den vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung der datenschutzrelevanten Maßnahmen
- Erforderliche Datenschutzverträge (insb. Auftragsverarbeitungsverträge) mit etwaig eingebundenen IT-Dienstleistern

4. Verarbeitung von Gesundheitsdaten

Trotz der Bestrebungen, die Mitarbeiter möglichst im Homeoffice arbeiten zu lassen (zu den arbeitsrechtlichen Fragestellungen siehe › **hier**), ist dies in manchen Branchen schlicht nicht möglich. Ein Bauvorhaben kann bspw. nicht von zu Hause aus errichtet werden. Die Mitarbeiter müssen zur Arbeit auf die Baustelle. Die einzelnen Bundesländer haben mittlerweile Merkblätter mit der Auflistung einzelner einzuhaltender Maßnahmen zum Infektionsschutz herausgegeben (für NRW vgl. › **hier**). Einige Unternehmen sind zudem bereits dazu übergegangen, zum Schutz der eigenen Mitarbeiter am Eingang zur Betriebsstätte Fiebermesskontrollen einzurichten. Die Verarbeitung von Gesundheitsdaten ist datenschutzrechtlich jedoch nicht unbedenklich. Bei Informationen über die Gesundheit eines Mitarbeiters handelt es sich um besonders sensible Daten, deren Erhebung und Verarbeitung gemäß Art. 9 DS-GVO, §§ 22, 26 Abs. 3 BDSG nur unter sehr strengen Voraussetzungen zulässig ist.

Es verwundert daher nicht, dass sich sowohl die Datenschutzkonferenz, ein Zusammenschluss der deutschen Datenschutzaufsichtsbehörden (vgl. › **hier**), als auch der Europäische Datenschutzausschuss (vgl. › **hier**) sehr frühzeitig zu der Frage geäußert haben, inwieweit Arbeitgeber Gesundheitsdaten ihrer Mitarbeiter im Zusammenhang mit der Corona-Pandemie verarbeiten dürfen. Die wichtigsten Fragen haben wir für Sie nochmals zusammengefasst:

Welche Informationen darf der Arbeitgeber bei seinen Mitarbeitern in Bezug auf eine mögliche Corona-Infizierung erfragen?

Im Grundsatz gilt: Fragen nach dem Gesundheitszustand eines Mitarbeiters sind erlaubt, soweit sie auf mögliche Einschränkungen der Arbeitstätigkeit bzw. -fähigkeit oder Gesundheitsrisiken für andere Mitarbeiter zielen. Der Arbeitgeber ist aufgrund seiner Fürsorgepflicht verpflichtet, angemessene Schutzmaßnahmen für die Belegschaft und ggf. betroffene Dritte wie Kunden und Geschäftspartner zu ergreifen. Dazu gehören nach Auffassung der Datenschutzaufsichtsbehörden auch angemessene Maßnahmen zur Verhinderung einer

pandemischen Verbreitung meldepflichtiger Krankheiten und damit zur frühzeitigen Erkennung von Corona-Erkrankungen am Arbeitsplatz. Folgende Fragen sind daher zulässig:

- Frage zu einer positiven Corona-Testung
- Frage nach coronatypischen Symptomen wie Husten und Fieber nur in begründeten Verdachtsfällen (nicht: pauschale Befragung zum Gesundheitszustand oder Grippesymptomen)
- Befragung von Urlaubsrückkehrern nach Aufenthalten in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet (nicht: Fragen allgemein nach Reisezielen)
- Frage nach direktem Kontakt mit nachweislich infizierten Personen innerhalb der letzten 14 Tage
- Befragung eines positiv getesteten Mitarbeiters, zu welchen Personen er im Arbeitsumfeld direkten Kontakt hatte

Anstelle einer Befragung kann der Arbeitgeber seine Mitarbeiter auch verpflichten, sich selbst aktiv zu melden, wenn eine der vorstehenden Fragen auf sie zutrifft. Eine Meldung von Kollegen, die vermeintlich Symptome aufweisen, ist hingegen zu untersagen.

In welchem Umfang dürfen diese Informationen verarbeitet werden?

Maßgeblich ist der Grundsatz der Datenminimierung. Die vorgenannten Informationen dürfen nur im absolut notwendigen Umfang erhoben und gespeichert sowie ausschließlich zweckgebunden, das heißt ausschließlich zu Zwecken des Gesundheitsschutzes und der Aufrechterhaltung des Betriebs, verwendet werden. Sie müssen zudem absolut vertraulich behandelt werden. Nach Wegfall des jeweiligen Zwecks, also allerspätestens dem Ende der Pandemie, müssen die erhobenen Daten unverzüglich gelöscht werden.

Sind Fiebermessungen erlaubt?

Die Frage ist umstritten. Vertretbar erscheint die Messung der Körpertemperatur unseres Erachtens jedoch, sofern die betreffenden Mitarbeiter in einem Arbeitsumfeld tätig sind, die zwangsweise mit einem besonders engen Kontakt zu anderen Personen verbunden sind, und/oder es bereits Fälle nachweislich Infizierter im Unternehmen gibt. Vorzuziehen sind Fiebermessungen auf freiwilliger Basis. In jedem Fall sind die Mitarbeiter zuvor umfassend über die Maßnahme und den Umgang mit Verdachtsfällen zu informieren. Die Ergebnisse einer solchen Messung dürfen zudem nicht gespeichert werden. Im Falle eines begründeten Verdachtes einer Infektion mit Covid-19 sollte der betroffenen Person vielmehr untersagt sein, die Arbeitsstätte für einen festgelegten Zeitraum von regelmäßig mindestens 14 Tagen aufzusuchen. Soweit vorhanden bedarf es der Einbindung des Betriebsrats.

Müssen die Mitarbeiter darüber informiert werden?

Der Arbeitgeber ist verpflichtet, die betroffenen Personen über die Umstände der Verarbeitung ihrer Daten nach Maßgabe von Art. 12 bis 14 DS-GVO zu informieren. Die Mitarbeiter sind insbesondere darüber zu informieren, zu welchen Zwecken Informationen zu ihrer Person (z.B. Gesundheitsdaten) verarbeitet werden, auf welcher Rechtsgrundlage dies basiert, an wen diese Informationen weitergegeben werden und wie lange sie aufbewahrt werden. Auch sind die Mitarbeiter über ihre diesbezüglichen Rechte aufzuklären. Dies gilt auch, soweit beispielsweise Temperaturmessungen am Eingang der Arbeitsstätte vorgenommen werden. In diesem Fall können die Datenschutzhinweise beispielsweise vorab per Rundmail oder durch Aushang bzw. Aushändigung von Hinweisen vor Ort erteilt werden.

Dürfen oder müssen Arbeitgeber die Identitäten von infizierten Kolleginnen und Kollegen offenlegen?

Arbeitgeber sollten ihre Mitarbeiter über COVID-19-Fälle informieren und entsprechende Schutzmaßnahmen ergreifen, aber nicht mehr Informationen als nötig preisgeben. Regelmäßig kann eine solche Information abteilungs- bzw. teambezogen ohne konkrete Namensnennung erfolgen. Auch kann eine Kontaktaufnahme mit den Gesundheitsbehörden genügen, die dann weitere erforderliche Maßnahmen ergreift. Nur soweit diese Maßnahmen nicht genügen, um dem Risiko einer Ausweitung von Infektionen zu begegnen, ist eine Offenlegung der Identität eines positiv getesteten oder unter Infektionsverdacht stehenden Mitarbeiters gegenüber unmittelbaren Kontaktpersonen (z.B. direkte Kollegen) ausnahmsweise erlaubt, damit diese Personen Vorsorgemaßnahmen treffen können. Die Personen müssen sich allerdings zur Vertraulichkeit und Verschwiegenheit verpflichten. Der betroffene Mitarbeiter sollte hierüber allerdings vorab informiert werden. Eine Offenlegung der Identität gegenüber der gesamten Belegschaft ist hingegen mit Blick auf eine mögliche Stigmatisierung des Betroffenen nicht erlaubt. Auch eine Einwilligung des Betroffenen empfiehlt sich als datenschutzrechtliche Grundlage zur Offenlegung seiner Identität nicht, da die Freiwilligkeit einer solchen Einwilligung regelmäßig zweifelhaft sein dürfte.

Eine Weitergabe von Daten über erkrankte Mitarbeiter oder solche mit Aufenthalt in Risikogebieten oder direktem Kontakt zu einer positiv getesteten Person an Gesundheitsbehörden ist auf Anfrage erlaubt.

Sofern Sie eine individuelle rechtliche Beratung wünschen, sprechen Sie unsere Mitglieder der **Praxisgruppe Datenschutz** jederzeit gerne an.