27. März 2020

Datenschutz in Zeiten von Covid-19

„Unter der derzeitigen Situation der Corona-Krise und den dadurch bewirkten Kontakteinschränkungen kommt der Kommunikation über soziale Medien eine ganz neue besondere Bedeutung. Gleichzeitig stellen sich für viele Menschen und Unternehmen Fragen bei der Umgestaltung ihrer Arbeitsplätze auf ein Home-Office. Dieses alles berührt auch den Datenschutz und den Schutz der Privatsphäre. Das gilt nicht zuletzt für den Umgang mit Gesundheitsdaten von Personen, die mit dem Virus in Kontakt gekommen sind. Vieles in der Normalität des täglichen Lebens hat sich durch die Corona Pandemie verändert und wirft neue Fragen gerade für den Schutz der Privatsphäre auf. Auf dieser Seite wollen wir zeitnah aktuelle Informationen zu Fragestellungen bereitstellen, die uns derzeit gehäuft durch Anfragen von Bürgerinnen und Bürgern erreichen. Gerade in Zeiten von hoher Unsicherheit gegenüber bevorstehenden sozialen, ökonomischen und kulturellen Umbrüchen gilt: Der Schutz der Daten muss eine verlässliche Konstante im Leben von uns allen bleiben. Individuelle Rechte und Freiheiten mögen sich in einer neuen Weise im Lichte der gegenwärtigen Krise darstellen, sie sind jedoch nach wie vor wirksam und können nach wie vor durch die Betroffenen geltend gemacht werden."

Prof. Dr . Johannes Caspar,
der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

www.datenschutz-hamburg.de
E-Mail: mailbox@datenschutz.hamburg.de
Ludwig-Erhard-Str. 22 - 20459 Hamburg - Tel.: 040 - 4 28 54 - 40 40 - Fax: 040 - 4 28 54 – 40 00
Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Der öffentliche PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707).

Inhalt

1. Auswirkungen der Pandemie auf die Datenschutzaufsicht

1.1. *Erreichbarkeit unserer Behörde*

Um die Auswirkungen der Coronavirus-Epidemie für das Personal zu begrenzen und einen geregelten Dienstbetrieb aufrechtzuerhalten, hat der Hamburgische Beauftragte seit dem 13. März Home Office eingeführt. Zwischenzeitlich wurden von der Hamburgischen Gesundheitsbehörde Allgemeinverfügungen erlassen, die darauf abzielen, vermeidbare physische Begegnungen und Kontakt von Menschen auf engem Raum zu unterbinden. Wann eine Rückkehr zur regulären Büroarbeit wieder erfolgen kann, ist derzeit nicht vorhersagbar. Beratungen erfolgen daher bis auf Weiteres nur nach vorheriger Terminvereinbarung. Bitte prüfen Sie aber, ob eine persönliche Beratung unbedingt nötig ist und nehmen Sie bitte von spontanen persönlichen Besuchen Abstand. Unsere Behörde ist weiterhin – wie gewohnt – über E-Mail (mailbox@datenschutz.hamburg.de) und Telefon (040/42854-4040) erreichbar.

1.2. *Umgang mit Fristen*

Die Handlungsfähigkeit des HmbBfDI wird dadurch aufrechterhalten, dass die Mitarbeiterinnen und Mitarbeiter des HmbBfDI fast ausschließlich im Homeoffice arbeiten. Dadurch, dass wenig Vorbereitungszeit für diese Ausnahmesituation vorhanden war, können jedoch nicht alle Funktionen mit der vorherigen Effizienz bedient werden. Entsprechendes Verständnis haben wir grundsätzlich, wenn dies auch bei den durch uns kontrollierten Stellen der Fall ist. Von uns gesetzte Fristen für Antworten an uns werden während der Zeit der Pandemie großzügiger bemessen. Darüber hinaus geht der HmbBfDI derzeit mit begründeten Anträgen auf Fristverlängerung wohlwollend um.

Gesetzliche Fristen der DSGVO gelten unverändert weiter. So haben Betroffene zum Beispiel auch in Krisenzeiten das Recht, von jedem Verantwortlichen binnen eines Monats Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten. Eine Verlängerung nach Art. 12 Abs. 3 S. 2 DSGVO ist weiterhin nur ausnahmsweise möglich, wenn dies aufgrund der Komplexität und der Anzahl von Anträgen erforderlich ist.

Im Zuge des Einschreitensermessens kann es im Einzelfall jedoch geboten sein, dass der HmbBfDI Verstöße nicht verfolgt, in denen die gesetzliche Frist überschritten wird, weil die Arbeitsfähigkeit des Verantwortlichen pandemiebedingt stark eingeschränkt ist. Bei der Beurteilung wird es entscheidend auf die Länge der Überschreitung sowie die

Unternehmensgröße und die damit verbundene berechtigte Erwartung an die Professionalität des Verantwortlichen ankommen.

Die Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 Abs. 1 DSGVO hat „unverzüglich und möglichst binnen 72 Stunden" zu erfolgen. Die gesetzliche Formulierung ist hier weiter als bei Art. 12 Abs. 3 DSGVO, sodass pandemiebedingte Einschränkungen der Arbeitsfähigkeit hier gegebenenfalls Berücksichtigung finden können. Wichtig ist jedoch, dass Sicherheitslücken sofort geschlossen werden, damit z.B. Kriminelle die aktuelle Ausnahmesituation nicht für ihre Zwecke missbrauchen können, und dass die Meldung an die Aufsichtsbehörde nicht unnötig verzögert wird.

1.3. *Bußgeldverfahren*

In laufenden Bußgeldverfahren werden derzeit bis auf weiteres keine Bußgeldbescheide erlassen, um die Unternehmen und Gewerbetreibende im gegenwärtigen Anpassungsprozess an die zahlreichen Veränderungen der Corona-Krise zu entlasten.

2. Kontaktlose Kommunikation

2.1. *Datenschutz und Datensicherheit, Tools und Software*

Folgende technische Fragen sollte man sich oder dem Betreiber einer Software stellen, um zu entscheiden, ob dieser Dienst unter datenschutzrechtlichen Gesichtspunkten zur Kommunikation genutzt werden kann. Hierbei spielt vor allem eine Rolle, ob die Nutzerinnen und Nutzer der Software über bestimmte Kriterien informiert werden oder für den Einsatz zustimmen muss (Liste nicht abschließend).

2.1.1. Wird ein Konto benötigt oder stehen Gastzugänge zur Verfügung?

- Setzt die Videokonferenzsoftware eine Registrierung eines jeden Teilnehmenden voraus?
- Lässt sich die Registrierung durch eine Anbindung an die bereits bestehende Infrastruktur, wie LDAP oder ActiveDirectory, automatisieren?
- Können Nutzer*innen als Gast ohne eine Registrierung teilnehmen? Ein Konto kann erforderlich werden, wenn beispielsweise Zugriffsrechte auf geteilte Daten oder administrative Funktionen für bestimmte Nutzerinnen und Nutzer gewährt werden sollen. Beim Einsatz von Ende-zu-Ende-Verschlüsselung mit Authentifizierung kann ein

Nutzerinnen- und Nutzerkonto notwendig sein, um Nutzerinnen- und Nutzeridentitäten verifizieren zu können.

Auch sollte das Löschen oder Sperren eines Nutzerinnen- und Nutzerkonto bedacht werden, um Konten den weiteren Zugang zu verwehren.

2.1.2. Wird Analytics eingesetzt, wertet der Betreiber des Dienstes die Daten der Nutzerinnen und Nutzer aus und verwendet sie kommerziell?

Dies betrifft die gesammelten Daten über die Nutzerinnen und Nutzer selbst, wie beispielsweise durch Hochladen der Adressbücher und die Auswertung der bei der Kommunikation ausgetauschten Daten. Betroffen sind Inhaltdaten wie Video- und Audioströme sowie Metadaten wie Nutzungszeiten, Kontakte und Aufenthaltsorte der Nutzerinnen und Nutzer.

2.1.3. Welche Kosten entstehen bei der Verwendung?

Ein Kommunikationstool kann frei von direkten betrieblichen Kosten durch einen Anbieter zur Verfügung gestellt werden. Ein mögliches Geschäftsmodell ist die kommerzielle Nutzung von Metadaten, die auch über Nutzer*innen-Tracking erhoben werden können.

Andere Betreiber bieten ihren Dienst gegen Bezahlung an. Der Preis bestimmt in der Regel, in welchem Umfang die Software genutzt werden kann. So lassen sich bestimmte Funktionen der Software oder die zulässige maximale Nutzerinnen- und Nutzeranzahl durch den Betrag skalieren.

Als dritte Alternative steht der eigene Betrieb eines Dienstes. Neben möglichen Lizenzkosten für die Software entstehen in der Regel auch Aufwände beim Betrieb der Infrastruktur, die zum Einsatz der Software benötigt wird.

2.1.4. Ist die eingesetzte Software quelloffen und/oder frei?

Beim Einsatz von proprietären Konferenzdiensten ist der Anwender auf die Angaben von Betreiber und Hersteller des Dienstes angewiesen. Eine Kontrolle der Aussagen ist in der Regel nicht möglich. Quelloffene Software lässt sich einfacher überprüfen. Zur Transparenz gehört auch die Offenlegung der Konfiguration des Dienstes durch den Betreiber.

Ein Hinweis muss der partiellen Öffnung von Diensten gelten; bei einigen Herstellern ist die Client-Software zur Teilnahme quelloffen, das Backend bleibt aber eine Blackbox und erlaubt keine Verifikation der Herstelleraussagen.

2.1.5. Wird verschlüsselt kommuniziert?

- Welche Grundeinstellungen gelten für jede Konferenzsitzung?
- Muss eine Verschlüsselung manuell aktiviert werden?
- Wird eine Transportverschlüsselung verwendet oder ist eine Auswertung durch Dritte möglich?
- Kommt eine Ende-zu-Ende-Verschlüsselung zum Einsatz oder ist der Betreiber in der Lage, die Inhalte der Kommunikation einsehen zu können?
- Wird Text-Chat-Kommunikation anders behandelt als Video- und Audiodaten?

Oftmals sind die Herstellerangaben unspezifisch. Daher sollten diese Fragen mit den Betreibenden des Dienstes geklärt werden.

2.1.6. Wird der Dienst auf Servern in der EU betrieben?

Bei der Wahl des Dienstes bestimmt in der Regel der Dienst-Anbieter, auf welcher Infrastruktur und an welchen Standorten der Dienst betrieben wird. Zu hinterfragen ist, ob Standorte in Staaten genutzt werden, die nicht dem Datenschutzniveau des europäischen Standards entsprechen. Hier kann auch von Relevanz sein, wenn einzelne Komponenten des Dienstes über Ländergrenzen hinweg verteilt sind. Es ist ratsam den Betreiber nach dem entstehenden Datenfluss zu fragen. Legt der Betreiber den entstehenden Datenfluss offen?

2.1.7. Bietet der Dienst alle Funktionen für meine Nutzerinnen- und Nutzergruppengröße?

Manche Dienste schränken die Anzahl der gleichzeitig genutzten Funktionen ein, zum Beispiel eine maximale Anzahl von gleichzeitig sendenden Videostreams oder die maximale Nutzeranzahl einer Ende-zu-Ende verschlüsselten Konferenz.

2.1.8. Gibt es einen Web- oder dedizierten Client?

Unter der Voraussetzung der Verwendung von aktuellen Browsern ist die Installation einer dedizierten Client-Software nicht zwingend. In der Regel erkauft man bei Web-Clienten sich relative Unabhängigkeit von Geräten und Betriebssystemen sowie der Notwendigkeit der stetigen Aktualisierung.

2.1.9. Soll das Tool nur zur Zeit der Corona-Pandemie genutzt werden oder ist ein Dauerbetrieb geplant?

Für den Fall eines Dauerbetriebs sollten nur Verfahren in den Auswahlprozess einbezogen werden, die die erforderlichen technischen Maßnahmen zur Gewährleistung der Sicherheit- und Vertraulichkeit der verarbeiteten personenbezogenen Daten erfüllen. Der Stand der Technik ist hierbei einzuhalten.

Unter der Situation der Covid-19-Pandemie herrschen besonderen Umstände der Verarbeitung, die bei der Abwägung der Nutzung zu berücksichtigen sind. Insbesondere besteht ein besonderes Interesse am Schutz der Beschäftigten und der Aufrechterhaltung des Dienstbetriebs. Die Auswirkungen, etwa eine Befristung der Vertragsdauer mit einem Dienstleister, sind daher zu berücksichtigen.

In der kommenden Woche werden wir hierzu weiterführende Informationen liefern. Zum einen wird demonstriert, wie anhand der vorliegend dargestellten (teilweise abstrakten) Kriterien Kommunikationstools selbst bewertet werden können. Zum anderen wird anhand spezifischer Kommunikationssoftware dieses Vorgehen demonstrieren und mögliche offene Fragestellungen diskutiert.

2.2. *Umsetzung im Bildungswesen (Schulen, Hochschulen, Ausbildungseinrichtungen)*

Tools, die im Schulzusammenhang genutzt werden sollen, müssen zum Schutz der personenbezogenen Daten der Schülerinnen und Schüler die Anforderungen aus Art. 32 DSGVO an die Datensicherheit erfüllen. Insbesondere sind in diesem Kontext die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Diese Gewährleistungsziele können auf vielfältig Art und Weise sichergestellt werden. Eine Möglichkeit stellt der eigenverantwortliche Betrieb von Lernplattformen dar. Vor diesem Hintergrund rentieren sich die Anstrengungen, die Hamburg während der letzten Jahre unternommen hat, um mit der flächendeckenden schulischen Anbindung an das Portal EduPort eine Basis für die datenschutzkonforme Kommunikation und Zusammenarbeit zwischen Lehrkräften und perspektivisch auch mit Schülerinnen und Schülern zu ermöglichen. Über EduPort, das vom städtischen IT-Dienstleister Dataport gehostet und administriert wird, können Lehrkräfte auch aus dem Homeoffice Dokumente in der schulischen Cloud ablegen, Materialien mit Kolleginnen und Kollegen teilen und gemeinsam bearbeiten, Schultermine planen und veröffentlichen und auf weitere schulische IT-Systeme zugreifen. Sämtliche Daten liegen so an einer zentralen Stelle im Verantwortungsbereich der FHH. Hamburg steht mit EduPort eine

datenschutzkonforme Realisierungsmöglichkeit zur Verfügung, sodass der HmbBfDI davon ausgeht, dass dieses in den Schulen verwendet wird.

Bei anderen Services kann nicht mit Sicherheit gesagt werden, welche Informationen für die verschiedenen Anbieter einsehbar sind. So könnten prinzipiell Metadaten der einzelnen Nutzerinnen und Nutzer eingesehen und mit weitergehenden Telemetrie-Funktionen Aussagen darüber getroffen werden, welche Nutzerin und welcher Nutzer zu welcher Zeit bestimmte Dokumente bearbeitet und ggf. geteilt hat. Auch Aspekte wie verschlüsselte Dateihaltung und Kommunikation sowie Speicherort und Zugriffsrechte auf die (personenbezogenen) Daten müssen immer individuell betrachtet werden.

Sollte eine Nutzung von weiteren Tools zur Bereitstellung eines (digitalen) Unterrichtsangebots für zuhause erwogen wird, darf die alternative Möglichkeit des Postversands von Unterrichtsmaterialien nicht außer Acht gelassen werden. Denn auf diesem Wege kann gewährleistet werden, dass jeder Schüler und jede Schülerin gleichermaßen die Möglichkeit hat, am Unterricht teilzunehmen (Teilhabegerechtigkeit). Dies gilt auch in Hinblick auf die Erforderlichkeit der Verarbeitung und den Grundsatz der Datenminimierung von personenbezogenen Daten.

Es ist datenschutzrechtlich grundsätzlich möglich, angesichts der gegebenen Umstände nicht die gleichen Anforderungen an technische und organisatorische Maßnahmen zu stellen, wie unter normalen Bedingungen. Dennoch sollte die aktuelle Situation keine Beschaffung von langfristig einzusetzender IT rechtfertigen, deren Nutzung im Nachgang der Corona-Krise als nicht datenschutzkonform zu bewerten wäre. Gerade der Einsatz in Schulen, über den sich zunächst die Schulbehörde mit den Schulen zu verständigen hat und nicht der Hamburgische Beauftragten für Datenschutz und Informationsfreiheit eine Grundsatz- und Auswahlentscheidung treffen kann, muss sich daran orientieren. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit steht hier beratend zur Verfügung und muss im Übrigen im Beschwerdefall tätig werden. Die Entscheidung für oder gegen ein bestimmtes digitales Kommunikationstool, ist in erheblicher Weise insbesondere von der Zahl der Teilnehmer, dem Inhalt der Kommunikation und der Zeit der Nutzungsdauer abhängig und sollte daher für jeden Einsatzbereich individuell entschieden werden.

3. Verarbeitung von personenbezogene Covid-19-Daten durch infizierte Personen, Gesundheitseinrichtungen und Gesundheitsbehörden

3.1. *Wann handelt es sich bei personenbezogenen Angaben im Zusammenhang mit Covid-19 um besonders geschützte Gesundheitsdaten?*

Nach Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO) stellen personenbezogene Daten dann Gesundheitsdaten dar, wenn sie sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus ihnen Informationen über den Gesundheitszustand der betroffenen Person hervorgehen.

Angaben, die über Patienten, Bewohner, Klienten etc. erhoben werden, um das Risiko einer bestehenden COVID-19-Infektion zu ermitteln, sind daher dann Gesundheitsdaten, wenn sie Informationen zu bestehenden Symptomen enthalten oder aber die Einstufung des Betroffenen als Kontaktperson und daher einen begründeten Infektionsverdacht nach sich ziehen. Negativauskünfte, wie die Verneinung von Symptomen, relevanten Kontakten oder Reisen stellen demgegenüber keine Gesundheitsdaten dar. Da allerdings bei der Abfrage entsprechender Informationen unklar ist, ob sämtliche relevanten Fragen verneint oder aber bejaht werden, muss die Erhebung und Verarbeitung durch einen Erlaubnistatbestand des Art. 9 Abs. 2 DSGVO gedeckt sein und in technischer und von Gesundheitsdaten genügen.

3.2. *Meldepflichten und korrespondieren Verarbeitungsbefugnisse von erkrankten Personen, Ärzten, Therapeuten und Gemeinschaftseinrichtungen*

Wer als erkrankte Person, Arzt, Therapeut oder Institution des Gesundheitswesens aufgrund gesetzlicher Meldepflichten im Zusammenhang mit Covid-19-Erkrankungen zur Mitteilung personenbezogener Daten Dritter verpflichtet ist, kann die entsprechende Datenübermittlung im Umfang der Meldepflicht auf Art. 6 Abs. 1 lit. c, 9 Abs. 2 lit. i DSGVO in Verbindung mit den einschlägigen nationalen Regelung als Rechtsgrundlage stützen.

3.2.1. Welche personenbezogenen Angaben zu Dritten dürfen erkrankte Personen dem Gesundheitsamt mitteilen?

Erkrankte Personen sind nach § 25 Abs. 3 Infektionsschutzgesetz (IfSG) in Verbindung mit § 16 Abs. 2 Satz 3 IfSG verpflichtet, auf Verlangen die für die Ermittlungen des Gesundheitsamtes zur

Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit notwendigen Auskünfte zu erteilen. In diesem Rahmen ist auch die namentliche Benennung relevanter Kontaktpersonen, die unter Umständen eine von der DSGVO und dem BDSG erfasste Datenverarbeitung darstellen kann, gemäß Art. 6 Abs. 1 lit. c, 9 Abs. 2 lit. i DSGVO in Verbindung mit den genannten Vorschriften des IfSG zulässig.

3.2.2. Welche Personengruppen aus dem Gesundheits-und Sozialbereich müssen personenbezogene Daten über Erkrankte und Nichterkrankte an das Gesundheitsamt melden?

Zur namentlichen Meldung bei einer COVID-19-Infektion, einem begründeten Infektionsverdacht oder dem Tod im Zusammenhang mit der Infektion an das zuständige Gesundheitsamt sind

- der feststellende Arzt sowie in Einrichtungen nach § 23 Abs. 5 Satz 1 IfSG zusätzlich der leitende Arzt, in Krankenhäusern mit mehreren selbständigen Abteilungen der leitende Abteilungsarzt, in Einrichtungen ohne leitenden Arzt der behandelnde Arzt
- Angehörige eines anderen Heil- oder Pflegeberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung oder Anerkennung erfordert,
- Leiter von Einrichtungen nach § 36 Abs. 1 Nr. 1 bis 6 IfSG und
- Heilpraktiker

verpflichtet.

3.2.3. Wann muss eine Meldung durch die unter 3.3.2 genannten Meldepflichtigen erfolgen?

Gemäß der Verordnung über die Ausdehnung der Meldepflicht nach § 6 Abs. 1 Satz 1 Nr. 1 und § 7 Abs. 1 Satz 1 des Infektionsschutzgesetzes auf Infektionen mit dem erstmals im Dezember 2019 in Wuhan/Volksrepublik China aufgetretenen neuartigen Coronavirus ("2019-nCoV") sind nicht nur bestätigte Infektionen, sondern auch der begründete Verdacht einer Erkrankung sowie der Tod in Bezug auf eine Infektion zu melden.

3.2.4. Welche personenbezogenen Daten sind von den unter 3.3.2 aufgeführten Meldepflichtigen anzugeben?

Die namentliche Meldung muss in Bezug auf die erkrankten, infektionsverdächtigen oder verstorbenen Personen – soweit vorliegend – folgende Angaben enthalten:

- Name und Vorname,
- Geschlecht,
- Geburtsdatum,
- Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend: Anschrift des derzeitigen Aufenthaltsortes,
- weitere Kontaktdaten,
- Tätigkeit in Einrichtungen und Unternehmen nach § 23 Abs. 3 Satz 1 oder nach § 36 Abs. 1 und 2 mit Namen, Anschrift und weiteren Kontaktdaten der Einrichtung oder des Unternehmens,
- Betreuung oder Unterbringung in Einrichtungen nach § 23 Abs. 5 Satz 1 oder § 36 Abs. 1 Nr 1 bis 6 mit Namen, Anschrift und weiteren Kontaktdaten der Einrichtung,
- Diagnose oder Verdachtsdiagnose,
- Tag der Erkrankung, Tag der Diagnose, gegebenenfalls Tag des Todes und wahrscheinlicher Zeitpunkt oder Zeitraum der Infektion,
- wahrscheinliche Infektionsquelle, einschließlich der zugrunde liegenden Tatsachen,
- in Deutschland: Landkreis oder kreisfreie Stadt, in dem oder in der die Infektion wahrscheinlich erworben worden ist, ansonsten Staat, in dem die Infektion wahrscheinlich erworben worden ist,
- Überweisung, Aufnahme und Entlassung aus einer Einrichtung nach § 23 Abs. 5 Satz 1 IfSG, gegebenenfalls intensivmedizinische Behandlung und deren Dauer,
- Spender für eine Blut-, Organ-, Gewebe- oder Zellspende in den letzten sechs Monaten,
- Zugehörigkeit zu den in § 70 Abs. 1 Nr. 1 bis 3 IfSG genannten Personengruppen.

Liegen den meldepflichtigen Personen nicht alle der vorgenannten Angaben vor und sind diese für die Behandlung, Pflege oder Betreuung nicht erforderlich, so muss und darf nicht allein zu dem Zweck der Meldung eine Erhebung erfolgen.

3.3. *Erhebungs- und Verarbeitungsbefugnisse von Ärzten, Therapeuten und sonstigen ambulanten Leistungserbringern*

3.3.1. Dürfen Arztpraxen, Therapeuten und sonstige ambulante Leistungserbringer von Ihren Patienten im Vorwege eines Termins Informationen zur Einschätzung des Risikos einer bestehenden COVID-19-Infektion abfragen?

Die Abfrage von Symptomen und Risikofaktoren einer COVID-19-Infektion im Vorwege eines Praxisbesuchs dient dem Zweck, die Patienten und Beschäftigten der Praxis bzw. Gesundheitseinrichtung dadurch bestmöglich zu schützen, dass Patienten in begründeten Verdachtsfällen nicht ungeschützt mit anderen Patienten oder medizinischem Personal in Kontakt kommen. Die entsprechende Datenverarbeitung kann somit hinsichtlich der anfallenden Gesundheitsdaten auf Art. 9 Abs. 2 lit. i DSGVO i. V. m. den einschlägigen infektionshygienischen Vorschriften und angesichts einschlägiger Nebenpflichten des Behandlungsvertrags auf Art. 9 Abs. 2 lit. h DSGVO als Rechtsgrundlage gestützt werden.

3.3.2. Wie kann ein Fragebogen zur Ermittlung des Infektionsrisikos datensparsam gestaltet werden?

Um dem Grundsatz der Datenminimierung zu genügen und lediglich die für die Risikoeinschätzung erforderlichen Daten zu erheben,

- ist statt konkreter Reiseziele nur abzufragen, ob innerhalb der letzten 14 Tage ein Aufenthalt in einem der vom Robert Koch-Institut (RKI) benannten Risikogebieten stattgefunden hat;
- muss kein konkreter Reisezeitraum abgefragt werden, sondern nur, ob die Reiserückkehr aus einem vom RKI benannten Risikogebiet mindestens 14 Tage zurückliegt;
- sind die auf eine COVID-19-Infektion hinweisenden Symptome nicht einzeln, sondern gebündelt abzufragen.

3.3.3. Über welche Kommunikationskanäle können die maßgeblichen Angaben von den Patienten datenschutzkonform abgefragt werden?

Grundsätzlich sollte die Abfrage telefonisch oder elektronisch über einen verschlüsselten Kanal erfolgen. Zum Übersenden eines ausgefüllten Fragebogens mittels unverschlüsselte E-Mail oder

Fax darf aus Gründen der Datensicherheit hingegen nur dann aufgefordert werden, wenn eine telefonische Abfrage der relevanten Angaben aufgrund des Patientenandrangs mit den verfügbaren Kapazitäten nicht mehr zu leisten ist und solange ein verschlüsselten Kanal noch nicht realisiert werden konnte.

Zwar erfolgt die Übermittlung der personenbezogenen Daten bei der Erhebung der Fragebogenantworten mittels E-Mail oder Fax durch die Betroffenen selbst. Allerdings muss der Verantwortliche, also die Praxis oder Einrichtung, bei der Auswahl der für die Verarbeitung eingesetzten Mittel bzw. bereitgestellten Erhebungskanäle Art. 25 Abs. 1 DSGVO berücksichtigen. Da es sich bei den Angaben der Patienten um Gesundheitsdaten und damit personenbezogene Daten mit hohem Schutzbedarf handeln kann, würde eine gezielte unverschlüsselte elektronische Erhebung unter „normalen" Bedingungen nicht dem in technischer Hinsicht zu gewährleistenden hohen Schutzniveau genügen.

Auch im Rahmen von Art. 25 Abs. 1 DSGVO sind allerdings die Umstände der Verarbeitung zu berücksichtigen. Zu den Umständen der Verarbeitung gehört auch die besondere Situation einer Pandemie, die ausnahmsweise eine gezielte unverschlüsselte elektronische Erhebung rechtfertigen kann, solange keine sichereren Erhebungskanäle zur Verfügung stehen, die eine kontaktlose und schnelle Übermittlung ermöglichen.

Ein verschlüsselter Kanal lässt sich beispielsweise durch ein Web-Formular mit Transportverschlüsselung (https, TLS) umsetzen und so eine angemessene Vertraulichkeit der Kommunikation sicherstellen.

3.3.4. Unter welchen datenschutzrechtlichen Bedingungen dürfen Ärzte, Therapeuten, und Heilpraktiker Videosprechstunden anbieten oder ihre Behandlung ausschließlich über elektronische Kommunikationsmedien durchführen?

Sofern eine Fernbehandlung berufsrechtlich zulässig ist, muss bei der Auswahl des Kommunikationsmediums stets auf eine ausreichende Verschlüsselung und einen Serverstandort in der EU oder einem sicheren Drittland geachtet werden. Die Gewährleistung eines ausreichenden Datenschutzniveaus ist regelmäßig bei gemäß § 5 Abs. 2 der Anlage 31b zum BMV-Ä zertifizierten Videodienstanbietern gegeben.

Generell ist von einer Speicherung berufsbezogener und ggf. einer berufsrechtlichen Verschwiegenheitspflicht unterliegenden personenbezogenen Daten auf dem Privatgerät abzusehen.

Der Zugang zu personenbezogenen Daten auf den Endgräten muss z.B. durch ein Pin oder ein Passwort vor Dritten geschützt und die Daten müssen auf dem Datenträger verschlüsselt gespeichert werden.

3.4. *Datenerhebung und -verarbeitung durch die Gesundheitsämter und das Robert Koch-Institut (RKI)*

3.4.1. Darf das RKI die Handy- bzw. Bewegungsdaten von Erkrankten oder Kontaktpersonen auswerten?

Der Schutz der Allgemeinheit vor übertragbaren Krankheiten ist ein überragend wichtiges Gemeinschaftsgut. Hierzu kann es geboten sein, auch digitale Technologien unter Nutzung personenbezogener Daten einzusetzen. Die grundlegenden Prinzipien des Datenschutzes sind dabei zu beachten: Die Verarbeitung personenbezogener Daten muss geeignet, erforderlich und verhältnismäßig sein. Das gilt in besonderer Weise für eine umfassende Überwachung von Personen zum Schutz der Allgemeinheit vor gefährlichen Infektionskrankheiten, denn diese greift tief in deren Privatsphäre ein. In Deutschland gibt es derzeit weder eine hinreichende Rechtsgrundlage für ein Tracking der Standortdaten von Personen zur Ermittlung von möglichen Kontaktpersonen noch für ein Handy-Tracking in Echtzeit zur Feststellung von Verstößen gegen Quarantäne- oder Kontaktbeschränkungsbestimmungen. Eine solche Rechtsgrundlage kann der Bundesgesetzgeber schaffen. Er muss dabei die verfassungsrechtlichen Prinzipien, insbesondere die Verhältnismäßigkeit, wahren.

Anders liegt die Sache bei der Weitergabe von anonymisierten Handydaten zur statistischen Auswertung von Gruppenverhalten durch Mobilfunknetzbetreiber. Soweit es sich um wirksam anonymisierte Daten handelt, stehen die Regelungen des Datenschutz- bzw. Telekommunikationsgesetzes nicht dagegen. Das ist der Fall, wenn die Daten so aggregiert sind, dass sie nicht ohne Weiteres auf bestimmte Personen zurückgeführt werden können. Sie sind in dieser Form geeignet, um Informationen über die Wirksamkeit von Maßnahmen gegen die Ausbreitung des Virus zu liefern. Für die Überwachung, ob es sich hierbei um anonymisierte Daten handelt, ist der BfDI zuständig. Hinsichtlich der Anonymisierung der eigenen Mobilfunkdaten durch den Mobilfunkanbieter steht Betroffenen ein Widerspruchsrecht gemäß Art. 21 Abs. 1 DSGVO zu. Teilweise bieten die Netzbetreiber auch einfache und datensparsame Abmeldemöglichkeiten, um die eigenen Daten von der anonymen Nutzung auszuschließen (vgl. https://www.telefonica.de/dap/selbst-entscheiden.html und https://www.optout-service.telekom-dienste.de/public/anmeldung.jsp).

Die Bundesregierung hat, auch nach Kritik von Seiten des Datenschutzes, bislang auf die geplante gesetzliche Möglichkeit verzichtet, Kontaktpersonen von Infizierten per Handyortung zu ermitteln.

3.4.2. Welche allgemeine Erhebungs- und Verarbeitungsbefugnisse haben die Gesundheitsämter und das RKI im Rahmen ihrer Ermittlungen?

Die Hamburger Gesundheitsämter unterliegen als bezirkliche Einrichtungen den Bestimmungen der DSGVO und des Hamburgischen Landesdatenschutzgesetzes (HmbDSG) sowie den bereichsspezifischen Datenschutzregelungen des IfSG.

Danach dürfen Gesundheitsämter neben den ihnen zu meldenden Angabe (s. dazu oben unter 3.2.4) weitere im Zusammenhang mit der Bekämpfung des Coronavirus erforderliche Informationen, insbesondere über die Erkrankung, die Ursachen, Behandlung Ansteckungsquellen und Kontaktpersonen, ggf. die Tätigkeit des Erkrankten, seine Betreuung, Unterbringung oder Behandlung in einer Gesundheits- oder Gemeinschaftseinrichtung, eigene Untersuchungsdaten erheben und verarbeiten.

Wird das RKI auf Ersuchen einer oder mehrerer Landesgesundheitsbehörde im Wege der Amtshilfe zur Bekämpfung von schwerwiegenden übertragbaren Krankheiten tätig, darf es die für die Amtshilfe erforderlichen personenbezogenen Daten verarbeiten.

4. Verarbeitung personenbezogener Covid-19-Daten durch den stationären Handel und Unternehmen mit Publikumsverkehr

4.1. *Ist ein Eingangsscreening in Geschäften und anderen Einrichtungen erlaubt?*

Die Befragung von Kunden oder Besuchern von Ladenlokalen nach Krankheitssymptomen ist unzulässig. Da derzeit ohnehin nur für die Daseinsvorsorge dringend erforderliche Geschäfte geöffnet haben, sind diese auch für jedermann, der keiner Quarantänepflicht unterliegt, zugänglich zu halten. Sie dürfen beispielsweise Personen mit Erkältungssymptomen nicht verwehrt werden. Allenfalls die Frage, ob eine tatsächliche Covid-19-Infektion besteht oder ob in den vergangenen zwei Wochen ein Aufenthalt in einem Risikogebiet erfolgt ist, ist möglich, da diese Personen ohnehin keine öffentlichen Orte betreten dürfen.

Eingangsscreening auf Risikoexposition und/oder Symptome, um das Risiko einer Übertragung und großer bzw. schwerer Folgeausbrüche zu verringern, sind zur Zeit nicht erfolgversprechend,

da es nach den bisherigen Erkenntnissen keine spezifischen Krankheitszeichen gibt, mit denen Träger des Covid-19-Virus frühzeitig erkannt werden können. Wer spezifische Anzeichen oder Symptome einer Atemwegsinfektion zeigt, ist damit nicht automatisch Träger des Covid-19-Virus. Fragen, nach Krankheitssymptomen wie Fieber, Husten, Schnupfen oder Halsschmerzen lassen also nicht erkennen, ob eine Infektion vorliegt. Trotz respiratorischer Symptome ließen sich bei bisher untersuchten Personen ebenso auch keine Infektionen nachweisen.

Eingangsscreening mit symptom- und/oder kontaktbasierten Fragen an die Besucher/Kunden können Infizierte nicht wirklich identifizieren. Im Übrigen handelt es sich um Gesundheitsdaten, deren Verarbeitung gem. Art. 9 DSGVO nur in streng geregelten Fällen erlaubt ist. Von daher sollten statt dieser Maßnahmen Besucher/Kunden im Eingangsbereich durch Aufstellen oder Aushändigung von Hinweisschildern/-blättern darauf hingewiesen werden, dass sie bei Vorliegen von respiratorischen Symptomen oder vorangegangenen Aufenthalten in Risikogebieten oder besonders betroffenen Gebieten in Deutschland gebeten werden, das Unternehmen aus Gründen der Sicherheit für die Mitarbeiter nicht zu betreten.

4.2. *Müssen Kundinnen und Kunden namentlich registriert werden?*

Die namentliche Erfassung aller Kundinnen und Kunden sowie Besucherinnen und Besucher von Geschäften und ähnlichen Einrichtungen ist in der Regel nur mit deren freiwilliger Einwilligung zulässig. Teilweise werden die Betroffenen nach ihren Namen und Kontaktdaten befragt, um später eventuelle Infektionsketten nachvollziehen zu können. Erhält ein Verantwortlicher eine individuelle Anordnung der Gesundheitsbehörde auf Grundlage des Infektionsschutzgesetzes, ist dieser Folge zu leisten. Von diesen Einzelfällen abgesehen gibt es in Hamburg – anders als in einigen Landkreisen des Umlands – keine Rechtsgrundlage zur Erfassung der Identität der Besucher. Deshalb können solche Maßnahmen in der Regel nur aufgrund einer freiwilligen Einwilligung erfolgen. Für die Wirksamkeit der Einwilligung ist es erforderlich, dass diese diskriminierungsfrei abgelehnt werden kann. Die Besucherin oder der Besucher muss also dennoch das Angebot des Geschäfts nutzen können.

Ausnahmsweise ist die Erhebung von Namen und Kontaktdaten auch ohne Einwilligung zulässig in Konstellationen, die ein hohes Infektionsrisiko bergen. Nach Einschätzung des Robert Koch Institut wird eine namentliche Registrierung empfohlen für Kontaktpersonen, die z.B. ohne Sicherheitsabstand ein mindestens 15-minütiges Gespräch „face-to-face" führen oder die mit Körperflüssigkeiten in direkte Berührung kommen[1]. In der Regel sind derartige Dienstleistungen derzeit ohnehin durch Allgemeinverfügung untersagt. Tätigkeiten, die noch ausgeübt werden

[1] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Kontaktperson/Management.html

dürfen, etwa ärztliche Behandlungen oder Beratungstermine in Kreditinstituten sind in der Regel ohnehin nicht anonym und werden umfassend dokumentiert. Wo dies nicht der Fall ist, kann eine Registrierung nach den Empfehlungen des Robert-Koch-Instituts aufgrund der hohen individuellen Ansteckungsgefahr auch ohne wirksame Einwilligung zulässig sein nach Art. 6 Abs. 1 lit. f DSGVO.

In jedem Fall müssen entsprechende Datenschutzhinweise, insbesondere gemäß Art. 13 DSGVO, vor Erhebung der Daten an den Kunden/Besucher erfolgen. Die Daten müssen vor dem Zugriff Unberechtigter sowie sicher aufbewahrt werden und die Speicherung darf nur kurzfristig erfolgen. Deshalb dürfen Listen, in denen solche Daten geführt werden, nicht offen herumliegen und für jedermann zugänglich sein. Oftmals ist es besser, die Daten zu jedem erfassten Besucher/Kunden auf einem gesonderten Blatt zu führen und danach sicher wegzuschließen, wenn sie nicht elektronisch geführt werden. Die Speicherfristen richten sich nach der Inkubationszeit. Nach spätestens 6-8 Wochen sollten die Daten gelöscht werden, wenn bis dahin keine Erkrankung aufgetreten ist.

Wir verzeichnen eine besondere Häufung von Anfragen bezüglich zweier in Hamburg sehr verbreiteter Bäckereiketten, die beide ihren Hauptgeschäftssitz in Schleswig-Holstein haben. Solche Unternehmen unterliegen auch hinsichtlich ihrer Filialen in Hamburg der Aufsicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, das sich ebenfalls zu der Thematik geäußert hat (Link). Bitte wenden Sie sich mit Fragen und Hinweisen zu Unternehmen mit Hauptsitz in Schleswig-Holstein an die dortigen Kolleginnen und Kollegen unter folgendem Link.

5. Covid-19 im Beschäftigtenverhältnis

5.1. *Mitarbeiterbefragungen nach Krankheitssymptomen und Urlaubsorten*

Beschäftigte unterliegen grundsätzlich keiner Pflicht, Ihrem Arbeitgeber Diagnosen oder Krankheitssymptome zu offenbaren. Im Fall einer allgegenwärtigen Pandemie sind davon Ausnahmen denkbar. Die Fürsorgepflicht des Arbeitgebers gebietet es, Maßnahmen zu treffen, um Mitarbeiterinnen und Mitarbeiter vor Infektionen zu schützen. Um Kontakte mit potentiell infektiösen Kolleginnen und Kollegen zu vermeiden, ist es in der aktuellen Pandemiesituation nicht zu beanstanden, wenn vor Betreten des Arbeitsplatzes erfragt wird, ob die betroffene Person

- selbst mit dem Covid-19-Virus infiziert ist sind oder im Kontakt mit einer nachweislich infizierten Person stand oder

- sie sich im relevanten Zeitraum in einem vom Robert Koch Institut als Risikogebiet eingestuften Gebiet aufgehalten hat.

Nicht erlaubt ist beispielsweise die offen gestellte Frage, in welchem Land eine Urlaubsabwesenheit verbracht wurde oder mit welchen Personen der Betroffene in Kontakt stand. Eine Negativauskunft des Betroffenen, dass die oben genannten Punkte auf ihn nicht zutreffen, ist ausreichend. Alternativ zur individuellen Abfrage kann auch verlangt werden, dass Beschäftigte sich aktiv melden, wenn sie einen der oben genannten Punkte erfüllen.

Es handelt sich um eine Abfrage von Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO. Diese ist, wenn aufgrund der Ausgestaltung des Arbeitsplatzes mit Ansteckungen zu rechnen ist, gerechtfertigt nach § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DSGVO.

In Arbeitsumfeldern mit besonders engem Kontakt ist in der derzeitigen Lage auch ausnahmsweise die Messung der Körpertemperatur oder das Erfragen von Covid-19-sypzifischen Symptomen denkbar. Dasselbe gilt für Mitarbeiterinnen und Mitarbeitern in Einrichtungen, die für die akute Versorgung der Bevölkerung unverzichtbar sind, etwa Krankenhäuser oder Medizinproduktehersteller. In diesen Fällen sind nicht die konkret erfragten Informationen wie Krankheitssymptome oder die Körpertemperatur zu speichern, sondern lediglich die Information, dass aufgrund des Eingangs-Checks der Betroffene aufgefordert wurde, sich für einen definierten Zeitpunkt nicht an die Arbeitsstätte zu begeben.

5.2. *Offenlegung der Identität von Infizierten an Kolleginnen und Kollegen*

Die Identitäten positiv auf Covid-19 getesteter Kolleginnen und Kollegen sind vertraulich zu behandeln, soweit dies ohne Gesundheitsgefahren für andere möglich ist. Die Tatsache, dass ein Betroffener Träger des Virus ist, kann sehr stigmatisierende Wirkung haben. Daher ist die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist demgegenüber nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen erforderlich ist.

Dabei ist je nach Empfängerkreis der Information differenziert vorzugehen. Je nach Unternehmensgröße wird es in der Regel für die meisten Kolleginnen und Kollegen sowie gegebenenfalls für Externe ausreichend sein, zu wissen, dass eine unbenannte Person aus einer konkreten Abteilung positiv getestet wurde. Gegebenenfalls sind Zusatzinformationen sinnvoll, etwa an welchen Tagen die Person anwesend war, an welchen Meetings sie teilgenommen hat und welche Gemeinschaftseinrichtungen (z.B. Kantine, Bibliothek) sie genutzt hat. Innerhalb der Abteilung wird je nach Abteilungsgröße eine weitere Differenzierung nach untergeordneten

Organisationseinheiten möglich sein. Bei Personen, die direkten Kontakt hatten, kann die zielgerichtete Offenlegung der Identität erforderlich sein. Dies betrifft beispielsweise Personen, die sich ein Bürozimmer teilen oder solche, bei denen es wahrscheinlich ist, dass ein Händedruck stattgefunden hat. Die Zulässigkeit folgt dann aus § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b DSGVO.

5.3. *Erhebung der privaten Telefonnummer durch Arbeitgeberinnen und Arbeitgeber*

Beschäftigte sind auch in der aktuellen Situation in der Regel nicht verpflichtet, dem Arbeitgeber ihre private Telefonnummer oder E-Mail-Adresse mitzuteilen. Aufgrund der derzeitigen betrieblichen Planungsunsicherheiten kann es jedoch vielfach im Interesse der Beschäftigten sein, kurzfristig auf diesen Kanälen über Beschränkungen am Folgetag informiert zu werden. Daher ist es zulässig, wenn Arbeitgeber von denjenigen Kolleginnen und Kollegen, die dies wünschen, auf Einwilligungsbasis Telefonnummern und E-Mail-Adressen einholen und diese nur für die Dauer der Pandemiesituation abspeichern. Wichtig ist, dass die Teilnahme freiwillig geschieht und diskriminierungsfrei erfolgt. Eine Weigerung muss also möglich sein, ohne dass berufliche Nachteile drohen. Wer seine privaten Kontaktdaten nicht offenbaren möchte, darf nicht vom Informationsfluss abgeschnitten sein. Es ist dann aber nachvollziehbar, dass dann die Information erst später an den Betroffenen gelangt. Dies kann geschehen, indem der Betroffene sich aktiv telefonisch oder im Internet erkundigt oder zum Beispiel am folgenden Arbeitstag durch einen Aushang am Firmeneingang über Einschränkungen, eine temporäre Betriebsschließung oder andere Maßnahmen informiert wird. Die Freiwilligkeit der Einwilligung folgt abhängig von den konkreten Umständen aus § 26 Abs. 2 S. 2 BDSG, wenn die Arbeitnehmerin oder der Arbeitnehmer durch die Abgabe der Einwilligung einen zeitlichen Vorteil erzielen möchte. Wichtig ist, dass der Zweck der Erhebung klar kommuniziert wird und die Kontaktdaten dann auch nur zu dem Zweck verwendet werden. Zudem muss die Einwilligung jederzeit ohne Angabe von Gründen und ohne diskriminierende Folgen widerruflich sein. Dann sind die auf diese Weise erhobenen Kontaktdaten durch den Arbeitgeber zu löschen.

6. Weitere Hilfestellungen

6.1. *DSK*

Die Datenschutzkonferenz des Bundes und der Länder (DSK) hat am 13. März 2020 Informationen für Arbeitgeber und Dienstherren zum Umgang mit dem Datenschutz im Zusammenhang mit der Corona-Pandemie veröffentlicht. Die Datenschutzaufsichtsbehörden

stellen darin klar, dass der Schutz personenbezogener Daten und Maßnahmen zur Bekämpfung der Infektion sich nicht entgegenstehen.

Die DSK-Hinweise können auf der Website des Bundesbeauftragten für Datenschutz und Informationsfreiheit heruntergeladen werden.

6.2. *EDSA*

Der Europäische Datenschutzausschuss (EDSA bzw. EDPB) hat außerdem Informationen und ein offizielles Statement zum Datenschutz und Covid-19 auf ihrer Website veröffentlicht. Eine deutsche Übersetzung ist in Arbeit.

6.3. *Mobiles Arbeiten*

- Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), „Telearbeit und Mobiles Arbeiten“:
- Information des Bundesamts für Sicherheit in der Informationstechnik (BSI), „Home-Office? – Aber sicher!“
- Artikel der European Union Agency for Cybersecurity (ENISA), „Top Tips for Cybersecurity when Working Remotely“
- Information des unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, „Datenschutz: Plötzlich im Homeoffice – Und nun?“

6.4. *Informationen anderer Landesbehörden*

FAQ zum Thema Corona aus Baden-Württemberg

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/FAQ-Corona.pdf

Hinweise aus Schleswig-Holstein

- https://www.datenschutzzentrum.de/corona/

Hinweise aus Bayern

- https://www.datenschutz-bayern.de/corona/
- Hier werden zudem auch Sonderinformationen zum Thema „Mobiles Arbeiten“ und Datenschutz im Gesundheitswesen aufgezeigt.

Informationen der Kolleginnen und Kollegen aus Rheinland-Pfalz

- Eine Podcast-Sonderfolge zum Thema Covid-19
- Informationen zum Schulunterricht in Zeiten der Corona-Krise