netvocat.

Externer Datenschutz & Seminare

Datenschutz in der Coronakrise

Vorwort

Zunächst einmal möchten wir unsere Betroffenheit allen Bürgern und Unternehmen gegenüber ausdrücken, die – wie wir auch – von der Krise und ihren massiven Auswirkungen ziemlich überrascht wurden.

Wir hoffen und tragen selbstverständlich unseren Beitrag dazu bei, dass wir in Deutschland und Europa mit vereinten Kräften, mit Solidarität, Vernunft und Rücksichtnahme auf die gefährdeten Gruppen dieses Problem schnellstmöglich in den Griff bekommen können.

Nichtsdestotrotz haben auch in Krisenzeiten rechtliche Regelungen, insbesondere derart bußgeldbewehrte Regelungen wie im Datenschutz, weiterhin Geltung, weshalb die nunmehr teilweise überstürzten Maßnahmen in Unternehmen dennoch rechtlich abgesichert werden müssen.

Wir sorgen für größtmögliche Rechtssicherheit mit geringstmöglichem Aufwand für Ihr Unternehmen – insbesondere in der Coronakrise.

Wir von netvocat möchten Ihnen dabei helfen, indem wir mit möglichst geringem Aufwand für Ihr Unternehmen Ihre Maßnahme absichern möchten, indem wir Ihnen für die verschiedenen nachfolgenden Situationen Dokumente unterschriftsreif zur Verfügung stellen können. Kostentransparenz ist durch moderate Pauschalen ebenfalls gegeben.

Sämtliche Dokumente können auch kurzfristig in Englisch zur Verfügung gestellt werden. Eine Prüfung, ob die Dokumente auch ausländischen Regelungen entsprechen, ist nicht umfasst. Allerdings können wir bei Bedarf Korrespondenzkollegen mit einer solchen Prüfung kurzfristig beauftragen.

Für Rückfragen stehen wir gerne zur Verfügung. Bleiben Sie gesund!

Herzlichst,
Daniela Wagner-Schneider & Team
Geschäftsführerin | Rechtsanwältin | Datenschutzbeauftragte DSB TÜV
netvocat® GmbH – Externer Datenschutz & Seminare

Datenschutz in der Coronakrise

Fakt ist, dass es zurzeit zahlreiche datenschutzrechtlich relevante Datenverarbeitungsvorgänge gibt, die alle den Grundsätzen und Regelungen des Datenschutzrechts entsprechen müssen. In der Coronakrise geht es um die Verarbeitung von Gesundheitsdaten und somit um die besonderen Kategorien personenbezogener Daten gem. Art. 9 (sensible Daten) Datenschutz-Grundverordnung (DS-GVO).

Erhebung und Übermittlung von Gesundheitsdaten

Grundsätzlich ist ein Mitarbeiter als Betroffener nicht verpflichtet, dem Arbeitgeber über die Arbeitsunfähigkeitsbescheinigung hinaus Angaben zu seiner Erkrankung zu machen. In der Coronakrise jedoch berechtigen arbeitsrechtliche Fürsorgepflichten sowie Pflichten aus dem Infektionsschutzgesetz den Arbeitgeber zu intensiveren Eingriffen in den Datenschutz der Mitarbeiter.

Dennoch müssen sämtliche Datenverarbeitungsvorgänge auch in diesen besonderen Zeiten den Datenschutzgrundsätzen wie Datensparsamkeit, Zweckbindung, Rechtmäßigkeit und Transparenz entsprechen.

Datenschutz ist unabdingbar – auch in der Coronakrise. Wir klären Sie auf.

Der Grundsatz der Datensparsamkeit beinhaltet z. B. dass der Arbeitgeber zwar einen erkrankten Mitarbeiter nach seinem Aufenthaltsort in Risikogebieten oder nach Kontaktpersonen, nicht jedoch nach einzelnen Details zum Gesundheitszustand fragen darf. Eine derartige Auskunftspflicht oder auch die Pflicht, sich einer ärztlichen Untersuchung zu unterziehen, besteht für den Mitarbeiter lediglich gegenüber den Gesundheitsbehörden. Im Zweifel, sofern der Mitarbeiter nicht kooperiert, muss sich der Arbeitgeber an das Gesundheitsamt wenden, das den Mitarbeiter gegebenenfalls zur Durchführung einer ärztlichen Untersuchung veranlassen kann.

Datenschutz und Coronakrise - FAQ

Nachfolgend stellen wir die derzeit dringendsten Fragen im Datenschutzrecht dar.

Darf der Arbeitgeber zurzeit private Handynummern oder andere private Kontaktdaten von Mitarbeitern erheben, um diese im Notfall informieren zu können?

- Ja, wenn der Mitarbeiter einverstanden ist. Dann ist es erlaubt, private Kontaktdaten zu erheben und temporär zu speichern. Eine Verpflichtung dahingehend besteht jedoch nicht. Des Weiteren muss ein eindeutiger, konkreter und legitimer Zweck für die Datenerhebung gegeben sein, z. B. um weitere Erkrankungen zu verhindern. Dieser Zweck besteht jedoch nur für den Zeitraum der Coronakrise. Danach sind die Daten wieder zu löschen, da der Zweck entfallen ist.

Darf der Arbeitgeber Mitarbeiter ohne Verdachtsmomente nach ihren letzten Aufenthaltsorten fragen?

- Nein. Der Arbeitgeber darf weder schriftlich, noch mündlich danach fragen, ohne dass ein konkreter Verdacht einer Infektion besteht. Er kann nur auf die Risikogebiete hinweisen und anordnen, dass sich jeder Mitarbeiter, der sich dort aufgehalten hat, dies mitteilt.

Darf der Arbeitgeber Mitarbeiter nach Aufenthalten in Risikogebieten oder Kontakten zu Infizierten fragen?

- Ja, der Arbeitgeber darf danach fragen, ob sich der (noch nicht erkrankte) Mitarbeiter in einem Risikogebiet aufgehalten hat oder Kontakt zu Infizierten hatte. Der Arbeitgeber darf dies insbesondere dann fragen, wenn feststeht, dass der Mitarbeiter mit dem Corona-Virus infiziert ist. Auch weitere Nachfragen sind zulässig, wenn dies erforderlich ist. Der Arbeitgeber darf diese Daten zur betrieblichen Gesundheitsorganisation auch verarbeiten, da er seiner Fürsorgepflicht gegenüber den anderen Mitarbeitern aufgrund des Arbeitsrechts und des Arbeitsschutzgesetzes nachkommen muss. Die Rechtsgrundlage für die Verarbeitung der Daten ergibt sich aus Art. 6 Abs. 1 S. 1 lit. c, Art. 9 Abs. 2 lit. b, Abs. 4 DS-GVO in

Verbindung mit §§ 26 Abs. 3 S. 1, 22 Abs. 2 Nr. 1 lit. b Bundesdatenschutzgesetz (BDSG).

Darf der Arbeitgeber bei allen Mitarbeitern vor Betreten der Räumlichkeiten die Temperatur messen?

- Nein. Die Temperaturmessung stellt die Erhebung von Gesundheitsdaten dar. Dieser Datenverarbeitungsvorgang muss für den Zweck der Erfüllung der Fürsorgepflicht betreffend die Eindämmung des Infektionsrisikos verhältnismäßig, d. h. geeignet, erforderlich und das mildeste Mittel sein. Da die Temperaturmessung jedoch keine verlässliche Aussage über eine Infektion mit dem Corona-Virus zulässt, ist sie weder geeignet, noch erforderlich und somit nicht verhältnismäßig.

Darf der Arbeitgeber von den Mitarbeitern verlangen, dass sie sich nach Rückkehr aus dem Urlaub einem Corona-Test unterziehen müssen?

- Nein. Der Arbeitgeber darf lediglich anordnen, dass sich der Mitarbeiter einer amtsärztlichen oder betriebsärztlichen Untersuchung unterziehen muss. Diese Anordnung ist jedoch nur zulässig, wenn ein konkreter Verdacht auf eine Infektion besteht, weil sich der Mitarbeiter z. B. in einem Risikogebiet aufgehalten hat.

Darf der Arbeitgeber die Mitarbeiter auf einen Heimarbeitsplatz (Home Office) versetzen oder diese Arbeitsform anordnen?

- Nein. Der Arbeitgeber darf nicht einseitig bestimmen, dass der Mitarbeiter seine private Wohnung als Arbeitsplatz zur Verfügung stellen muss. Der Arbeitgeber kann dem Mitarbeiter lediglich die Möglichkeit anbieten, zuhause zu arbeiten. Nur wenn der Mitarbeiter einwilligt, ist die Beschäftigung im Home Office möglich. Besser ist jedoch, eine Vereinbarung mit dem Mitarbeiter zu schließen, die u. a. Regelungen betreffend die Arbeitsmittel und die Datensicherheit, sowie eine Richtlinie zum Datenschutz im Home Office enthalten sollte.

Darf der Arbeitgeber im Unternehmen unter Angabe des Namens über einen infizierten Mitarbeiter informieren, um weitere Mitarbeiter zu ermitteln, die mit ihm Kontakt hatten?

- Nein. Der Arbeitgeber darf nur gemeinsam mit dem Infizierten die anderen Kontaktpersonen ermitteln und diese sodann informieren und frei stellen. Ist dies nicht möglich, muss sich der Arbeitgeber an das Gesundheitsamt zwecks weiterer Maßnahmen wenden. Nur, wenn dies auch nicht möglich oder zielführend ist, darf der Arbeitgeber als ultima ratio die Mitarbeiter unter Namensnennung über die Infektion informieren, um weitere Gefahren abzuwenden.

Müssen Arbeitgeber Gesundheitsdaten oder Informationen über den Aufenthalt in Risikogebieten oder Kontaktpersonen von infizierten Mitarbeitern nach Aufforderung an Gesundheitsbehörden übermitteln?

- Ja. Die Behörden sind gem. §§ 16 Abs. 1, 2 S. 3, 30, 31 Infektionsschutzgesetz (IfSG) berechtigt, diese Daten zu erheben, um weitere Maßnahmen zu treffen und Verbote zu erlassen. Die Arbeitgeber sind daher verpflichtet, auf Anfrage diese Daten zu übermitteln.

Müssen Unternehmen nach behördlicher Aufforderung vorsorglich Daten von Kunden erheben oder übermitteln, für den Fall, dass sich dort eine infizierte Person aufgehalten hat? Dürfen Unternehmen dies ohne behördliche Anordnung tun?

- Gem. § 16 Abs. 1 IfSG kann eine behördliche Anordnung dahingehend erfolgen, Daten von Kunden oder Besuchern präventiv zu speichern oder zu übermitteln. Dem muss das Unternehmen Folge leisten. Die Legitimation ergibt sich aus Art. 6 Abs. 1 S. 1 c), Abs. 2, 3 DS-GVO. Es ist jedoch darauf zu achten, diese Datenverarbeitungsvorgänge sowohl in das Verzeichnis der Verarbeitungstätigkeiten (VVT), als auch in die Datenschutzhinweise für die Kunden/Besucher gem. Art. 13, 14 DS-GVO aufzunehmen.
  Ohne behördliche Anordnung darf ein Unternehmen präventiv Daten von Kunden/Besuchern nur mit deren Einwilligung gem. Art. 6 Abs. 1 S. 1 a), Art. 7 DS-GVO und nur zu dem Zweck einer möglichen Übermittlung

an Behörden verarbeiten und nur für die Dauer einer möglichen Inkubationszeit speichern. Danach sind die Daten zu löschen.

Welche Daten müssen Gesundheitsdienstleister (Krankenhäuser, Ärzte, Hospize etc.) für den Fall einer möglichen Infektion in ihrer Einrichtung von ihren Patienten erheben und an die Gesundheitsbehörden melden?

- Gemäß §§ 6, 7, 8, 9 IfSG in Verbindung mit der „Verordnung über die Ausdehnung der Meldepflicht nach § 6 Absatz 1 Satz 1 Nummer 1 und § 7 Absatz 1 Satz 1 des Infektionsschutzgesetzes auf Infektionen mit dem erstmals im Dezember 2019 in Wuhan/Volksrepublik China aufgetretenen neuartigen Coronavirus ("2019-nCoV") vom 30. Januar 2020 (BAnz AT 31.01.2020 V1)“ (CoronaVMeldeV) besteht die Pflicht für Gesundheitsdienstleister, nicht nur alle Angaben zu einer Infektion zu melden, sondern auch im Verdachtsfall eine Meldung abzugeben. Die Meldung muss u. a. sämtliche Daten zu dem Patienten, zu Diagnosen, Zeitangaben betreffend die Erkrankung, sowie Infektionsquellen mit genauen Angaben über Stadt und Land der Infektion enthalten. Darüber hinausgehende Informationen können, müssen jedoch nicht, von Gesundheitsdienstleistern erhoben werden, sofern dies aus medizinischen Gründen erforderlich scheint und eine datenschutzrechtliche Rechtsgrundlage vorliegt. Auch hier ist darauf zu achten, dass solche Datenverarbeitungsvorgänge, wie eine Meldung an die Behörden oder eine weitere Datenerhebung, in das Verzeichnis der Verarbeitungstätigkeiten (VVT) und in die Datenschutzhinweise für die Patienten gemäß Art. 13, 14 DS-GVO aufgenommen werden.

Dürfen Beschäftigte aktuell mobil mit Privatgeräten arbeiten?

- Ja. Laut BayLfD dürften Beschäftigte öffentlicher Stellen aktuell für ihre berufliche Tätigkeit private Geräte wie Handys, Tablets, Laptops etc. verwenden. Ebenso gestattet sei die Nutzung von Messenger- und Clouddiensten. Hiernach dürften Beschäftigte öffentlicher Stellen sowohl untereinander, als auch mit Patienten/Kunden per Messengerdienst oder Videokonferenz über Clouddienste (z. B. Skype) kommunizieren. Allerdings gälten folgende Beschränkungen, dass keine sensiblen Daten auf den Privatgeräten gespeichert werden sollten bzw. diese jedenfalls ein-

fach gelöscht werden können müssten. Es sollten möglichst wenige personenbezogene Daten über diese Medien kommuniziert werden. Die Geräte müssten mindestens mit PIN oder Passwort geschützt sein. Wenn die Nutzung dieser Dienste nicht mehr erforderlich sei, müssten alle Daten, insbesondere Telefonnummern sofort von den Privatgeräten gelöscht werden.
Speziell im Gesundheitsbereich müsse bei der Nutzung dieser Dienste und Übertragung sensibler Daten auf eine Ende-zu-Ende-Verschlüsselung geachtet und die Anforderungen der DSK-Konferenz im Whitepaper vom 7.11.2019 „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“[1] eingehalten werden. Zudem dürfe es aus IT-Sicherheitsgründen keine Anbindung an die internen IT-Systeme geben.

Quellen:

- https://www.datenschutz.rlp.de/de/themenfelder-themen/beschaeftigtendatenschutz-corona/
- https://www.baden-wuerttemberg.datenschutz.de/faq-corona/
- https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154
- https://www.datenschutz-bayern.de/corona/sonderinfo.html
- https://www.cmshs-bloggt.de/rechtsthemen/coronavirus-handlungsempfehlungen-fuer-unternehmen/coronavirus-datenschutz-aufsichtsbehoerden-dsk/
- https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

[1] https://www.datenschutz-bayern.de/dsbk-ent/DSK_98-KKH-Messenger.pdf

Kontakt

netvocat® GmbH – Externer Datenschutz & Seminare
Großherzog-Friedrich-Str. 40
66111 Saarbrücken
Tel.: 0681/590 97 98 – 50
Fax: 0681/590 97 98 – 30
E-Mail: info@netvocat.de
Internet: www.netvocat.de

Sie erreichen uns von Montag bis Freitag von 08:00 Uhr bis 17.00 Uhr.

Aktuell erreichen Sie uns am besten per **E-Mail oder Telefon** unter den o. g. Adressen und Nummern.
Gerne bieten wir auf Nachfrage auch **Web-Meetings** an.

Ihre Ansprechpartner für neue Anfragen sind:

- Daniela Wagner-Schneider, Geschäftsführerin, Rechtsanwältin, Datenschutzbeauftragte DSB TÜV: dwagner-schneider@netvocat.de

- Elina König, Diplom-Juristin: ekoenig@netvocat.de

Wir sind gerne für Sie da – sprechen Sie uns an!

Impressum:

1. Auflage

Herausgeber:
netvocat GmbH – Externer Datenschutz & Seminare
Großherzog-Friedrich-Str. 40
66111 Saarbrücken
Tel.: 0681/590 97 98 – 50
Fax: 0681/590 97 98 – 30
E-Mail: info@netvocat.de
Internet: www.netvocat.de

Grafik: © kras99/stock.adobe.com