Ahlers & Vogel

JusLetter

April 2020

Datenschutz und Covid-19

von Rechtsanwalt Dr. Stefan Hoeft * und Rechtsanwalt Dirk Schuster**

Die anhaltende Ausbreitung des Corona-Virus zwingt Privatpersonen wie Unternehmen gleichermaßen dazu, geeignete Maßnahmen zur Eingrenzung der Pandemie zu ergreifen. Auch wenn datenschutzrechtliche Fragestellungen nicht im Fokus der Präventionsmaßnahmen stehen, sollte das Datenschutzrecht bei der Umsetzung solcher Maßnahmen nicht unberücksichtigt bleiben.

Insbesondere der Schutz der sensiblen Gesundheitsdaten, deren Verarbeitung durch Art. 9 DSGVO enge Grenzen gesetzt sind, wirft bei der Umsetzung der Präventionsmaßnahmen Fragen auf. Aber auch die Verarbeitung anderer personenbezogener Daten, die aufgrund der Corona-Pandemie benötigt werden, bedarf einer gesonderten Bewertung.

Viele Unternehmen haben zur weiteren Eindämmung der Pandemie und zur Aufrechterhaltung der betrieblichen Tätigkeit entschieden, Mitarbeiter im Home-Office arbeiten zu lassen. Dabei müssen Unternehmen nicht nur datenschutzrechtliche Fragestellungen, sondern auch die Sicherheit der Informationssysteme beachten und durch geeignete technische und organisatorische Maßnahmen die Integrität der IT-Systeme gewährleisten.

(Gesundheits)daten von Mitarbeitern und Kunden

Die Abwägung zwischen der Fürsorgepflicht und dem Umgang mit den besonders sensiblen Gesundheitsdaten führt zu einem offenkundigen Spannungsverhältnis, zu dem sich die Aufsichtsbehörden zwischenzeitlich geäußert haben. So hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) FAQs erarbeitet, die sich nicht nur dem Umgang mit Gesundheitsdaten widmen. Auch der Bundesbeauftrage für Datenschutz und Informationsfreiheit hat sich zu einer datenschutzkonformen Erhebung und Verarbeitung von Gesundheitsdaten geäußert.

Auch wenn die Aufsichtsbehörden eine Rechtfertigung für die Verarbeitung von Gesundheitsdaten in Art. 9 Abs. 2 DSGVO sowie § 26 Abs. 3 BDSG erkennen, wird dabei stets betont, dass sich die Erhebung und die Verarbeitung von Gesundheitsdaten stets am Einzelfall unter Abwägung der Gesamtumstände zu orientieren hat. Die anlasslose und pauschale Erhebung von Gesundheitsdaten, wie zum Beispiel ein obligatorisches Messen der Temperatur, wird regelmäßig nicht den Anforderungen der gesetzlichen Rechtfertigungstatbeständen genügen.

Nach Auffassung des LfDI BW sind vor allem die Frage nach einem Aufenthalt in einem Risikogebiet sowie die Erhebung und Verarbeitung der Information, mit welchen Personen ein Erkrankter Kontakt hatte zulässig. Im Rahmen der weiteren Verarbeitung darf der Name einer erkrankten Person im Regelfall nicht offengelegt werden, da die Offenlegung zur Umsetzung weiterer Maßnahmen in der Regel nicht erforderlich und eine stigmatisierende Wirkung zu vermeiden ist.

Auch die Erhebung anderer personenbezogener Daten kann im Rahmen der Umsetzung von Präventionsmaßnahmen erforderlich werden. So hält der LfDI BW die Erhebung privater Kontaktdaten zur Information von Mitarbeitern in Notfällen für unproblematisch, wenn die Mitarbeiter hiermit einverstanden sind. Eine Pflicht der Mitarbeiter zur Offenlegung privater Kontaktdaten besteht jedoch nicht.

Weitergehende Maßnahmen sind rechtlich nur zulässig, sofern der Betroffene in die Verarbeitung einwilligt. Die Wirksamkeit der Einwilligung ist dabei am Maßstab des Art. 7 DSGVO sowie § 26 BDSG zu messen. Danach hat die Einwilligung freiwillig zu erfolgen, ist schriftlich zu fixieren und kann jederzeit vom Betroffenen frei widerrufen werden.

Auch die Daten von Kunden und Besuchern können nach Auffassung des LfDI BW unter bestimmten Voraussetzungen erhoben und an die zuständigen Behörden übermittelt werden. Liegt zum Beispiel eine behördliche Anordnung vor, kann die Verarbeitung auf Art. 6 Abs. 1 lit c DSGVO gestützt werden. Zu beachten ist jedoch, dass im Rahmen der nach Art. 13, 14 DSGVO zu erteilenden Informationen bereits auf eine derartige Datenverarbeitung hingewiesen werden muss. Fehlt ein derartiger

Hinweis, sollte dieser nachgeholt werden und die Datenschutzerklärungen für die Zukunft angepasst werden.

Bei der datenschutzrechtlichen Bewertung der Präventionsmaßnahmen müssen daher stets die datenschutzrechtlichen Prinzipien der Verhältnismäßigkeit, der Datenminimierung sowie der Zweckbindung berücksichtigt werden. Aufgrund der Sensibilität der Gesundheitsdaten ist zudem der Integrität und der Vertraulichkeit der erhobenen und verarbeitenden Daten gesteigerte Aufmerksamkeit zu widmen. Insbesondere dürfen erhobene Gesundheitsdaten nicht unbefugt an Dritte herausgegeben werden und sind unverzüglich zu löschen, nachdem der Zweck der Verarbeitung wegfällt. Die jeweiligen Maßnahmen und die getroffene datenschutzrechtliche Bewertung sind zudem sorgfältig zu dokumentieren.

Datenschutz im Home-Office

Als Teil der präventiven Maßnahmen zur Verhinderung der weiteren Ausbreitung der Pandemie haben eine Vielzahl von Unternehmen die Tätigkeit Ihrer Mitarbeiter in das Home-Office verlagert.

Mit der Auslagerung der Arbeit in die heimischen vier Wände gehen rechtliche Risiken einher, denen der Arbeitgeber durch geeignete technische und organisatorische Maßnahmen vorbeugen kann und muss. Dabei sollten nicht nur datenschutzrechtliche Belange, sondern auch die Sicherheit der IT-Infrastruktur des Unternehmens im Fokus stehen.

Gänzlich vermieden werden sollte die Nutzung privater IT-Systeme im Rahmen der Home-Office Tätigkeit. Durch die Bereitstellung von Hard- und Software des Unternehmens, können die jeweiligen Nutzerberechtigungen umfangreich angepasst und die Art der Nutzung vorgegeben werden, um eine zweckfremde Verwendung zu unterbinden. Zudem sollte mittels einer VPN-Verbindung der Zugriff auf die IT-Systeme des Unternehmens ermöglicht werden, um eine dezentrale Speicherung personenbezogener Daten zu verhindern. Die mobilen Arbeitsgeräte sowie die genutzten Kommunikationswege müssen zudem mit Passwörtern geschützt bzw. verschlüsselt werden, um unbefugte Zugriffe Dritter weitestgehend ausschließen zu können.

Das Ausdrucken von Dokumenten mit personenbezogenen Daten sollte ebenfalls unterbunden werden. Ist ein Ausdruck zwingend erforderlich, sollte Vorgaben zur Aufbewahrung und Vernichtung der gedruckten Dokumente aufgestellt werden.

Cyberkriminalität und Covid-19

Selbst auf die Cyberkriminalität hat Covid-19 Auswirkungen. So warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) aktuell vor einer Zunahme von Cyber-Angriffen mit Bezug zum Corona-Virus auf Unternehmen und Bürger.

Unternehmen und Betriebe werden per E-Mail durch die Täter aufgefordert, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben. Die Cyber-Kriminellen geben sich als vermeintliche Institutionen zur Beantragung von Soforthilfegeldern aus. Die so erlangten Daten werden anschließend für kriminelle Aktivitäten genutzt.

Auch das in der Covid-19 Krise bestehende Informationsbedürfnis des einzelnen, wird kriminell ausgenutzt. Derzeit gibt es eine exponentielle Zunahme an Registrierungen von Domainnamen mit den Schlagwörtern wie "corona" oder "covid". Neben der natürlich bestehenden Nutzung für legitime Informationsangebote werden jedoch viele dieser Webseiten für kriminelle Zwecke genutzt. Der Nutzer wird auf den kriminellen Seiten zum Download und anschließen der Installation vermeintlicher Softwareupdates aufgefordert. Hierbei werden die Systeme der Nutzer mit Schadprogramm infiziert. Eine weitere Masche der Täter ist, dass Spam Mails mit vermeintlichen wichtigen Informationen in Bezug auf Corona im Dateianhang zur Verbreitung von Schadsoftware versendet wird. Wenn diese Schadprogramme erst einmal den Rechner infiziert haben, können die Täter unter anderem auf z.B. das Online Banking zugreifen oder eben gerade bei Heimarbeitsplätzen auch Zugriff auf Unternehmensnetzwerke erlangen, um sensible Daten auszuspähen oder Information zu verschlüsseln und damit dann die Opfer anschließend zu erpressen.

Mit betrügerischen Online-Shops machen sich Täter zudem die derzeit erhöhte Nachfrage nach Schutzbekleidung oder Atemmasken zunutze. Diese Waren werden nach Bestellung und Bezahlung nicht geliefert oder sind von minderwertiger Qualität.

Cyberkriminalität ist das größte Unternehmensrisiko

Die Cyberkriminalität hat in den letzten Jahren deutlich zugenommen. In dem neuesten Risikobarometer der Allianz-Versicherung hat Cyberkriminalität sich sogar zum größten Risiko für Unternehmen entwickelt und führt damit erstmals die Rangliste der potenziellen Gefahrenquellen für Unternehmen an.

Bei der Befragung von weltweit rund 2.700 Experten in mehr als 100 Ländern antworteten rund 39 Prozent der Befragten auf die Frage nach der größten Bedrohung mit IT-Risiken. Damit verdrängte diese Gefahr erstmals die Bedrohungen durch Betriebsunterbrechungen vom ersten Platz der Gefahrenliste, die noch von 37 Prozent genannt wurden.

Cyberkriminalität ist dabei kein Problem, was lediglich in Deutschland zum größten Risiko geworden ist, sondern steht auch in vielen anderen der untersuchten Länder unter den ersten drei Gefahren. Ganz an der Spitze stehen Cybervorfälle sogar in Belgien, Frankreich, Indien, Südafrika, Südkorea, Österreich, Schweden, der Schweiz, Spanien, Großbritannien und in den USA.

Unternehmen tragen dabei nicht nur das Risiko immer größerer und teurerer Datenskandalen oder von Cybererpressung- und Spoofing-Vorfällen, sondern auch die seit Einführung der Datenschutzgrundverordnung (DSGVO) deutlich erhöhten Bußgelder aufgrund strengerer Datenschutzbestimmungen und auch daraus resultierender Schadenersatzklagen.

Um diesem steigenden Risiko Herr zu werden bzw. zumindest begrenzen zu können, bedarf es im Vorwege natürlich der richtigen Aufstellung auf technischer Seite, aber eben auch, gerade im Hinblick auf die DGSVO, der richtigen rechtlichen Aufstellung des Unternehmens. Ferner im Blick auf eine im jeweiligen Einzelfall vorzunehmende Risikoanalyse der Frage der Absicherung solcher Risiken durch Eindeckung einer entsprechenden Versicherung. Angesichts dessen, dass hier zumindest über eines der größten Unternehmensrisiken der heutigen Zeit gesprochen wird, besteht ebenso die Gefahr, dass eine Ignoranz dieses Themas auch die Frage der Haftung der Vertretungsberechtigten des Unternehmens gegenüber dem Unternehmen selbst aufkommen lässt.

Hinweis

Unser Jusletter beruht auf einer sorgfältigen Recherche der Rechtslage. Deren allgemeine Darstellung kann die Besonderheiten des jeweiligen Einzelfalles jedoch nicht berücksichtigen. Der Jusletter dient nur der Information und ist keine vertragliche Beratungsleistung. Er kann deshalb eine individuelle Rechtsberatung nicht ersetzen.

Diesen und weitere Jusletter finden Sie auf unserer Website www.ahlers-vogel.de.

Kontakt

Ahlers & Vogel _ Bremen
Contrescarpe 21 _ 28203 Bremen
Telefon +49 (421) 33 34-0
Telefax +49 (421) 33 34-111
E-Mail: bremen@ahlers-vogel.de

Ahlers & Vogel _ Hamburg
Schaarsteinwegsbrücke 2 _ 20459 Hamburg
Telefon +49 (40) 37 85 88-0
Telefax +49 (40) 37 85 88-88
E-Mail hamburg@ahlers-vogel.de

Ahlers & Vogel _ Leer
Hafenstraße 6 _ 26789 Leer (Ostfriesland)
Telefon +49 (0491) 45 45 229-0
Telefax +49 (0491) 45 45 229-99
E-Mail leer@ahlers-vogel.de

*__Dr. Stefan Hoeft__ studierte Rechtswissenschaften in Hamburg, wo er anschließend auch promovierte. Zu seinen Tätigkeitsgebieten zählen das Transport- und Speditionsrecht sowie das IT- und Versicherungsrecht. Er ist Mitglied des Fachanwaltsausschusses Versicherungsrecht (Zulassung von Fachanwälten) der Hanseatischen Rechtsanwaltskammer Bremen sowie Fachanwalt für Versicherungsrecht, ferner Mitglied des gemeinsamen Fachausschusses für Transport- und Speditionsrecht der norddeutschen Rechtsanwaltskammern sowie Fachanwalt für Transport- und Speditionsrecht und Autor im Bereich Seehandels- und Transportversicherungsrecht. Herr Dr. Hoeft ist seit 1999 für unsere Sozietät tätig und seit 2008 Partner.

**__Dirk Schuster__ studierte Rechtswissenschaften in Göttingen und absolvierte sein Referendariat in Oldenburg und Bremen. Seit Dezember 2016 betreut Herr Schuster unsere Mandanten im Schwerpunkt im Bereich des Kauf- und Werkvertragsrecht. Seine Tätigkeit in unserer Sozietät konzentriert sich insbesondere auf das Gebiet des Kauf- und Leasingrechts im Zusammenhang mit Kraftfahrzeugen. Herr Schuster berät Autohändler unterschiedlicher Marken in Bezug auf die Abgasthematik und verfügt diesbezüglich über eine breite Erfahrung. Darüber hinaus ist Herr Schuster im Bereich des IT-Rechts, hier insbesondere im Softwarevertragsrecht und Datenschutz sowie auf dem Gebiet der IT-Sicherheit tätig.