LOSCHELDER

Newsletter Datenschutzrecht

April 2020

Sehr geehrte Damen und Herren,

„Covid-19“ ist auch weiterhin das beherrschende Thema in der Öffentlichkeit und für die Wirtschaft. Auch datenschutzrechtlich bringen die Corona-Pandemie und die staatlichen Maßnahmen zu ihrer Eindämmung vielfältige Fragestellungen auf den Tisch. Hierzu haben wir Ihnen bereits zu Beginn der Krise erste Handlungshilfen zukommen lassen. Sie finden dazu und zu vielen anderen Themen einen Überblick unter https://loschelder.de/de/corona-taskforce.html.

Zwischenzeitlich haben sich auch verschiedene Datenschutzaufsichtsbehörden positioniert. Unser erster Beitrag liefert Ihnen einen Überblick zu den sich daraus ergebenden Handlungsspielräumen für Unternehmen, etwa bei der Gestaltung von HomeOffice-Arbeitsplätzen oder im Bereich der Pandemieprävention und -bekämpfung. In unserem zweiten Beitrag geben wir Ihnen einen Überblick über das heiß diskutierte Handytracking zur Eindämmung der Corona-Pandemie. Nachdem ein entsprechender Vorstoß aus dem BMG wegen heftiger Kritik zurückgezogen wurde, hat das RKI am 7. April eine eigene Corona-App veröffentlicht und bittet um eine „Datenspende“. Ferner sind Bluetooth-basierte Apps zur Kontrolle von persönlichen Kontakten in der Entwicklung. Wie auch immer Sie zu diesem Thema stehen: Die stetige Diskussion hierüber ist von enormer Bedeutung, um Transparenz und eine Kontrolle von Datenschutz und Datensicherheit zu gewährleisten.

Unser dritter Beitrag widmet sich einem Thema abseits der Corona-Krise: Die Datenschutzaufsichtsbehörden haben einmal mehr Hinweise zur Social Media-Nutzung veröffentlicht.

Inmitten der Corona-Krise wollen wir gemeinsam mit Ihnen den Blick nach vorne werfen und stellen uns im vierten Beitrag die Frage, ob das Virus und seine tiefgreifenden Folgen nicht auch eine Chance für die zuletzt hier und da ins Stocken geratene Digitalisierung bietet. Und zu guter Letzt wollen wir Ihnen auch in diesem Monat die besonders interessanten Bußgeldfälle und einige Kuriositäten nicht vorenthalten.

Inhalt

Datenschutz in Corona-Zeiten

Die Corona-Pandemie hat das öffentliche Leben grundlegend umstrukturiert, auch das Arbeitsleben. Dieses findet zunehmend im HomeOffice statt, auch außerhalb namentlicher Meldepflichten sehen sich Arbeitgeber zur Eindämmung des Corona-Virus und zum Schutz ihrer Belegschaft der Verarbeitung auch von personenbezogenen Daten (potentiell) erkrankter Mitarbeiter verpflichtet. Welche Arten der Datenverarbeitung hier als zulässig angesehen werden, unterliegt einer stets aktuellen Bewertung mit Blick auf den Stand der Pandemie und die politische und öffentliche Diskussion. Die Datenschutzaufsichtsbehörden haben sich dazu zwischenzeitlich ebenfalls zu Wort gemeldet und sorgen so für mehr Rechtssicherheit und Handlungsspielräume von Unternehmen.

Die Stellungnahmen der Datenschutzaufsichtsbehörden werden von zwei Themenfeldern bestimmt: Welche Anforderungen sind im HomeOffice einzuhalten und in welchem Umfang dürfen Unternehmen Informationen über potentielle Erkrankungen bei ihren Mitarbeitern verarbeiten. Und sogar vom EU-Level gibt es eine Stellungnahme des EDSA zum Datenschutz in Corona-Zeiten.

Die gute Nachricht vorab: Die Behörden betreiben Datenschutz mit Augenmaß. Etwa aus Hamburg oder Rheinland-Pfalz wird explizit verlautbart, dass die Aufsichtsbehörden sich der außergewöhnlichen Situation bewusst sind und Interimslösungen zur Aufrechterhalten des Betriebs daher auch dann unbeanstandet lassen könnten, wenn diese nicht vollumfänglich DSGVO-konform seien, etwa bei schnellen HomeOffice-Lösungen. Zudem setzt sich eine zunehmend pragmatische Sicht hinsichtlich der Verarbeitung von Gesundheitsdaten über (potentielle) Infektionen durch: Der BfDI verweist explizit darauf, dass die Gesundheit der Bürgerinnen und Bürger derzeit im Mittelpunkt steht und verhältnismäßige Datenverarbeitungsvorgänge daher auch regelmäßig zulässig seien. Möglich ist dies dogmatisch, wie wir im vergangenen Monat berichteten, etwa aus Gründen der **öffentlichen Gesundheit** (§ 22 Abs. 1 Nr. 1 lit. c BDSG, Art. 9 Abs. 2 lit. i DSGVO).

1. Datenschutz im (provisorischen) HomeOffice

Der für die öffentlichen Stellen zuständige BayLfD hat sich mit den datenschutzrechtlichen Aspekten des HomeOffice beschäftigt und eine vorläufige Sonderinformation veröffentlicht: Da es in der Kürze der Zeit und in dem notwendigen Umfang nicht möglich sei,

flächendeckend Dienstgeräte für die heimische Arbeit zur Verfügung zu stellen, wurden Rahmenbedingungen erarbeitet, bei deren Einhaltung eine Nutzung privater Geräte sowie von Messenger- und Cloud-Diensten datenschutzrechtlich akzeptabel sei. Für Videokonferenzen oder die Kommunikation über Messenger-Dienste ist danach die Nutzung privater Geräte für Beschäftigte öffentlicher Stellen oder außerhalb öffentlicher Einrichtungen Tätiger möglich, wenn

- keine sensitiven Daten (z.B. Gesundheitsdaten) gespeichert werden, oder – soweit dies nicht zu verhindern ist – eine einfache Möglichkeit zur Löschung besteht,
- die Kommunikation so wenig Daten wie möglich umfasst (Datensparsamkeit) und
- mobile Geräte durch eine PIN oder ein Passwort geschützt werden.

Ab dem Moment, in dem die Nutzung dieser Geräte nicht mehr erforderlich ist, müssen die gespeicherten Daten mit Personenbezug gelöscht werden. Dies umfasst auch die Löschung dienstlich genutzten Telefonnummern von privaten Telefonen.

Zur Umsetzung der technisch-organisatorischen Anforderungen im HomeOffice hat das BSI eine Reihe von Hinweisen veröffentlicht.

Daneben haben sich etwa auch die Aufsichtsbehörden aus Hamburg, Baden-Württemberg und Rheinland-Pfalz zur Frage datenschutzkonformer Videokonferenzsysteme geäußert, teils indes nur bedingt hilfreich: Insgesamt stehen die Aufsichtsbehörden kommerziellen Kommunikationsdiensten von US-Anbietern kritisch gegenüber, da diese teilweise auf Metadaten zugreifen und diese an Dritte weitergeben. Zuletzt war deswegen der Anbieter *Zoom* heftig in die Kritik geraten, der ein aufgedecktes Datenleck in Richtung Facebook jedoch geschlossen und auch im Übrigen erheblich nachgebessert hat. Präferiert werden von den Aufsichtsbehörden offene Lösungen, die auf den eigenen Servern „On-Premises“ eingebunden werden. Diese aber sind weniger massentauglich und oft auch nur bedingt für Videokonferenzen mit vielen Teilnehmern geeignet.

2. Daten von (potentiell) Erkrankten, Kontaktpersonen uvm.

Mit Schwerpunkt auf der Datenverarbeitung rund um (potentielle) Erkrankungen veröffentlichte der BfDI einige Informationen und ein FAQ:

- **(Gesundheits-) Daten von Beschäftigten:** Um die Ausbreitung des Virus einzudämmen, sei es dem Arbeitgeber datenschutzrechtlich erlaubt, (Gesundheits-) Daten von Arbeitnehmern zu erheben und zu verarbeiten. Er dürfe neben Namen und eigenem Gesundheitszustand des Arbeitnehmers auch dessen Kontakte innerhalb des Betriebes dokumentieren. Dies soll für die Fälle zulässig sein, in denen es zu einer Infektion, nachweislich zum Kontakt zu einer infizierten Person gekommen ist oder wenn innerhalb des relevanten Zeitraums ein Aufenthalt in einem – als Risikogebiet eingestuften – Gebiet stattgefunden hat. Dabei darf es auch zu einer Mitteilung an die übrigen Arbeitnehmer kommen. Soweit es möglich ist, muss diese Mitteilung jedoch ohne Nennung des Namens erfolgen, um die überflüssige Erhebung und Verarbeitung von Gesundheitsdaten zu vermeiden. Ist dies allerdings nicht möglich oder hilfreich, darf die Weitergabe im Rahmen des Beschäftigungsverhältnisses erfolgen.

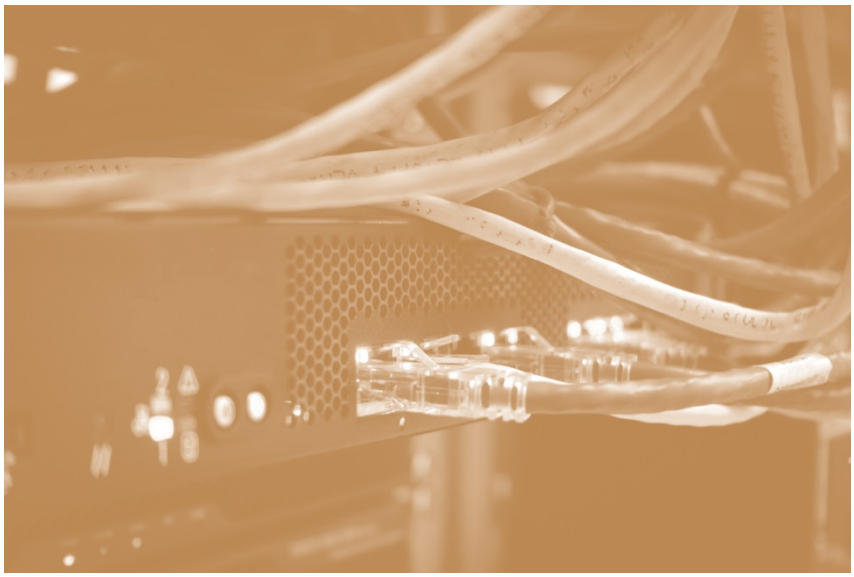
- **(Gesundheits-) Daten von Kunden und Gästen:** Gerade in Betrieben mit noch anhaltendem Kunden- oder Gästeverkehr ist die Erhebung der oben genannten Daten zur Feststellung erlaubt, ob diese selbst infiziert sind, in Kontakt mit einer nachweislich infizierten Person standen, oder ob diese sich zum relevanten Zeitraum in einem – als Risikogebiet eingestuften – Gebiet aufhielten. Da Angaben zu Kontakten oder zum Aufenthalt zunächst nicht unmittelbar auf den Gesundheitszustand des Betroffenen schließen lassen, sei die Erhebung gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO erlaubt. Für den Fall, dass von Beginn an Gesundheitsdaten erhoben werden (etwa Informationen über eine Infektion, die Körpertemperatur oder Husten), ist die Verarbeitung nur nach Art. 9 Abs. 2 lit. i DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. c BDSG erlaubnisfähig.

Die generelle Offenlegung der Infektionen oder des Infektionsverdachts zur Ermöglichung von Vorsorgemaßnahmen

für Kontaktpersonen ginge über die Fürsorgepflicht des Arbeitgebers hinaus. Dies sei nur in den Fällen zulässig, in denen es keine andere Möglichkeit zur Ermöglichung der Vorsorgemaßnahmen gäbe.

3. Kontaktmöglichkeiten

Aus einem FAQ des LfDI Baden-Württemberg ergibt sich, dass der Arbeitgeber für die Erstellung eines innerbetrieblichen Kommunikationsnetzwerks die Kontaktdaten seiner Arbeitnehmer temporär speichern darf. Dies soll dazu dienen, die Arbeitnehmer frühzeitig über die Schließung des Betriebs zu informieren und sie dazu aufzufordern, zuhause zu bleiben. So soll zusätzlich die Gefahr der Infektion verringert werden. Details rund um die Verwendung privater Kontaktinformationen der Mitarbeiter hat auch die Datenschutzaufsichtsbehörde aus Rheinland-Pfalz veröffentlicht.



Tracking von Handydaten zur Eindämmung des Coronavirus?

Am 07.04.2020 hat das RKI eine eigene App gelauncht, mit der zur Eindämmung der Corona-Pandemie um eine „Datenspende" gebeten wird: „Hände waschen, Abstand halten, Daten spenden - Ihr Beitrag gegen Corona". Die ursprünglich für die Novelle des Infektionsschutzgesetzes geplante Rechtsgrundlage zur Weitergabe von Handy- und Standortdaten an das RKI wurde aus dem Entwurf zur Änderung des Infektionsschutzgesetzes (IfSG) nach heftiger Kritik ersatzlos gestrichen. Anonymisierte Daten haben die Telekommunikationsanbieter zur Nachverfolgung von Bewegungen bereits an die Behörden übermittelt. Das personalisierte Tracking indes geht hierbei noch einen erheblichen Schritt weiter.

- Derzeit wird in Politik und Gesellschaft heftig diskutiert, ob eine personalisierte oder auch anonymisierte Auswertung von Kontakten, Standortdaten und Bewegungsmustern oder anderen Daten zur Eindämmung der Corona-Pandemie genutzt werden soll. Plakativ formuliert geht es der oftmals pulsierend geführten Debatte um die Abwägung zwischen öffentlicher Gesundheit und Freiheitsrechten der Bürger. Wir wollen das aktuelle Thema hier aufgreifen, weil es viele grundlegende datenschutzrechtliche Aspekte und Fragestellungen berührt, die - ggf. auch in ganz anderem Kontext - für Unternehmen relevant sind. Anonymisierung und Erarbeitung von Statistiken: Die Bundesregierung hat ihre Entscheidung rund um Ausgangssperren und Kontaktverboten auch auf die Auswertung von Bewegungsdaten gestützt, die ihnen anonymisiert von Telekommunikationsdienstleistern zur Verfügung gestellt wurden. So konnten sie nachvollziehen, ob sich etwa größere Menschenansammlungen in Parks aufhielten oder aber nicht. Das Grundprinzip ist bspw. von Google Maps bekannt und wird dort für aktuelle Verkehrsmeldungen verwendet. Herausfordernd ist zum einen, eine tatsächliche Anonymisierung abzusichern. Zum anderen kann auch die anonymisierte Verwendung zu erheblichen Einschnitten in die Freiheit eines jeden Einzelnen führen, wenn etwa über anonyme Bewegungsdaten Sperrzonen abgesichert werden, sei es etwa als Quarantänesicherung eines Kreises.

- Bewegungsprofile und Kontrolle von Kontakten: Das BMG wollte im Rahmen der jüngsten Novellierung des Infektionsschutzgesetzes eine Rechtsgrundlage für die Übermittlung auch personenbezogener Verkehrsdaten der Telekommunikationsanbieter an die öffentliche Hand zur Eindämmung der Corona-Pandemie schaffen. So hätte etwa auch über GPS-Daten eine Information an alle Kontaktpersonen laut Handy-Bewegungsprofilen übermittelt werden können, wenn ein Benutzer der App positiv auf das Coronavirus getestet wird (alle anderen Nutzer der App, die innerhalb der letzten zwei Wochen Kontakt zu der Person gehabt haben, hätten dann darüber informiert werden können). Das Hackathon Wirvs.Virus auf Bundesebene hatte etliche Vorschläge in dieser Richtung aufgebracht. Der Vorschlag aus dem BMG ist nach heftiger Kritik indes kurzfristig wieder zurückgezogen worden.

  Wie der aktuellen Berichterstattung zu entnehmen ist, sind derzeit Handy-Apps in der Entwicklung, die auf einen Datenaustausch via Bluetooth setzen, um Nutzer darauf hinzuweisen, dass sie in der Vergangenheit mit einer an Corona infizierten Person in Kontakt standen.

- Freiwillige Einwilligung und wissenschaftliche Auswertung: Nunmehr hat das RKI eine eigene App veröffentlicht, unter dem Titel „Corona-Datenspende-App“ mit dem Untertitel „Hände waschen, Abstand halten, Daten spenden - Ihr Beitrag gegen Corona“. Das RKI setzt auf eine freiwillige Teilnahme und damit auf die Einwilligung der Nutzer. Der BfDI twitterte auf Nachfrage am 07.04.2020, er habe eine „ad hoc“-Einschätzung abgegeben und „keine offensichtlichen Datenschutzverstöße“ festgestellt. In der Sache geht es dem RKI um den Erhalt pseudonymisierter Daten aus Fitness-Apps u.ä., konkret dem Geschlecht, Alter (in 5-Jahres-Schritten), Gewicht (in 5kg-Schritten), Körpergröße (in 5cm-Schritten), Gesundheits- und Aktivitätsdaten, Schlafverhalten, Herzfrequenz und Körpertemperatur. Diese werden wissenschaftlich ausgewertet, um mehr über das Corona-Virus zu erfahren. Schon zum Launch haben 50.000 Nutzer nach RKI-Angaben die App heruntergeladen.

Klappe die Xte: Datenschutzaufsichtsbehörden und Social Media Nutzung

Abgesehen von den dringenden Fragen, die die Corona-Krise mit sich bringt, gibt es im Datenschutzrecht auch von einem Dauerbrenner Neues zu berichten : Die Skepsis der Datenschutzaufsichtsbehörden gegen die Social Media-Plattformen hat mittlerweile klarere Strukturen angenommen, auch wenn nach wie vor hinreichende (überprüfbare) Entscheidungen fehlen. Einige Datenschutzaufsichtsbehörden haben Guidelines zum Umgang mit Social Media-Auftritten veröffentlicht.

Diese adressieren zunächst öffentliche Stellen, so etwa der vom Datenschutzbeauftragten des Landes Rheinland-Pfalz veröffentlichte Handlungsrahmen für die Nutzung von Social Media vom 06.03.2020 sowie verschiedenen Hinweisen aus Baden-Württemberg von Anfang Februar. Dies erscheint konsequent: Die Datenschutzaufsichtsbehörden hatten vielfach verkündet, zunächst die öffentlichen Stellen in die Verantwortung zu nehmen, bevor sie private Unternehmen wegen ihrer Ansicht nach datenschutzrechtswidrigen Unternehmenspräsenzen auf den Social Media-Plattformen in die Pflicht nähmen.

Im aktuellen Handlungsrahmen aus Rheinland-Pfalz macht die Aufsichtsbehörde wesentliche Eckpunkte deutlich, die entsprechend auch für private Unternehmen gelten:

- **Erlaubnisgrundlage:** Da die eigene Social Media-Präsenz in der Regel über den Kernbereich der öffentlichen Aufgaben hinausgeht, ist das Angebot nicht erforderlich und bedarf einer Einwilligung durch den Benutzer. Ist der Nutzer ohnehin auf den Plattformen aktiv und hat er dafür die Nutzungsbedingungen bereits akzeptiert, wird eine Einwilligung angenommen, soweit die Nutzungsbedingungen der Plattform der Informationspflicht gerecht wird (ohne hinreichende Information ist regelmäßig keine freiwillige Einwilligung möglich). Für diejenigen Nutzer, die ansonsten keine Social Media-Plattformen nutzen, ist eine zusätzliche Einwilligungsmöglichkeit erforderlich, die den Vorgaben der DSK entspricht. Sollte dies für den Betreiber der Plattform (technisch) nicht möglich sein – zu beachten ist hier, dass Facebook eine solche Möglichkeit **nicht** bereitstellt –, muss die öffentliche Stelle in Erwägung ziehen, das Social Media-Angebot auf angemeldete Nutzer zu beschränken. In diesem Fall muss i.d.R. jedoch ein alternativer Zugang zu den bereitgestellten Informationen ermöglicht werden.

- **Vereinbarung über die gemeinsame Verantwortlichkeit:** Öffentliche Stelle und Plattform-Betreiber sind nach der aktuellen EuGH-Rechtsprechung regelmäßig gemeinsam für bestimmte Bereiche der Datenverarbeitung verantwortlich. Dann aber müssen sie auch eine Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO schließen. Auch hier ergeben sich inhaltliche Mindestanforderungen aus einem Beschluss der DSK. Im Falle von Facebook reicht die in die Nutzungsbedingungen integrierte Seiten-Insight-Ergänzung nach Ansicht der Aufsichtsbehörden nicht aus, andere Plattformen, etwa Twitter, bieten eine solche Ergänzung nicht an. Dies war einer der wesentlichen Gründe für den zuletzt vollzogenen „Twexit“ des LfDI BW.

- **Informationspflicht / Impressumspflicht:** Die Behörde, die eine Social Media-Präsenz unterhält, trifft gegenüber dem Benutzer eine eigene Informationspflicht nach Art. 13, 14 DSGVO. Diese erfordert neben der Angabe zu Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten etwa auch den Hinweis über die Art und den Zweck der

Verarbeitung personenbezogener Daten. Diese Datenschutzerklärung muss aus dem Social Media-Angebot mit maximal einem (so etwas EDSA) bis zu zwei Klicks erreichbar sein.

- **Konzept:** Der verantwortliche Fanpage-Betreiber muss der Datenschutzaufsichtsbehörde in einem Konzept seine fundierten Erwägungen darlegen können, weshalb der Verzicht zu einer ernsthaften Beeinträchtigung der Aufgabenerfüllung führen würde. Dabei kann es nach Ansicht der Aufsichtsbehörde RLP ausreichen, wenn die Zahl der durch Social Media angesprochenen Nutzer deutlich höher ist, als es bei den bisherigen Informationskanälen (z.B. Website).

- **Alternativen:** Die öffentliche Stelle muss dafür sorgen, dass neben dem Social Media-Angebot auch andere Möglichkeiten bestehen, diese zu kontaktieren (z.B. per E-Mail) und Kenntnis von den dort angebotenen Informationen zu erlangen (z.B. Website).

- **Sonstige Pflichten des Verantwortlichen:** Die öffentliche Stelle muss zudem alle anderen Pflichten des Verantwortlichen aus der DSGVO erfüllen. Neben der Pflicht, den Betrieb des Social Media-Angebots in das Verzeichnis der Verarbeitungstätigkeiten einzutragen (Art. 30 DSGVO), müssen technisch-organisatorische Maßnahmen im Sinne der Art. 24, 25 und 32 DSGVO getroffen werden. Zudem ist für den Einzelfall zu bewerten, ob eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchzuführen ist.

- **Wichtige Ausnahmen:** Zu beachten ist besonders, dass in sensiblen Bereichen oder im Zusammenhang mit Daten, die unter den Art. 9 DSGVO fallen (z.B. Gesundheitsdaten) auf Social Media-Dienste verzichtet werden sollte.

Sollten diese Anforderungen durch die öffentlichen Stellen nicht eingehalten werden, kann dies dazu führen, dass das Angebot eingestellt werden muss (Art. 58 Abs. 2 f DSGVO).

Kommt es daneben bei dem Betrieb der Social Media-Dienste zu Verletzung personenbezogener Daten, kann der Betroffene gegen

die öffentliche Stelle als Verantwortlicher einen Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO geltend machen.

Die Hinweise helfen, um den eigenen Social Media-Auftritt des Unternehmens nochmals zu überprüfen. Sie ändern aber nichts an der nach wie vor misslichen Lage, dass mangels hinreichender überprüfbarer Entscheidungen der Aufsichtsbehörden eine Überprüfung ihrer Position nicht stattfinden kann, zumal die Unterhaltung von Social Media-Präsenzen für viele Unternehmen aktuell beinahe alternativlos ist, um ihre Kunden auf alternativen Kanälen zu erreichen. Dass dies selbst bei öffentlichen Stellen der Fall sein kann, erkennen die Rheinland-Pfälzer denn auch unter dem Stichpunkt „Konzept“ nunmehr ausdrücklich an. Die weitere Entwicklung bleibt hier abzuwarten; wir halten Sie auf dem Laufenden.

Corona – Chance für die Digitalisierung?

Viele Unternehmen in Deutschland haben in den vergangenen Wochen Möglichkeiten gesucht und gefunden, um ihren Geschäftsbetrieb trotz der massiven Einschränkungen (zumindest teils) aufrechtzuerhalten und damit Leistungserbringung, Arbeitsplätze und Umsätze zu sichern. Dazu gehören insbesondere die erhebliche Ausweitung von Home-Office-Arbeit, der Rückgriff auf automatisierte und IT-basierte Geschäftsprozesse sowie die Ausweitung und Stärkung des Onlinevertriebs. Bemerkenswert ist, dass diese Entwicklungen auch bei solchen Unternehmen angekommen sind, die daran bisher nicht gedacht bzw. diese Themen bisher nicht forciert haben. Folgende Themen dürfen wir heute für Sie beleuchten:

1. IT-Organisation/IT-Notallplan

Gerade in Krisenzeiten liegt es in der Verantwortung der Geschäftsleitung, die Arbeitsfähigkeit des Unternehmens so weit wie möglich aufrecht zu erhalten. Dazu gehört heute mehr denn je eine funktionierende IT-Infrastruktur. Dafür muss es einen Krisenplan geben (oder ein solcher muss zumindest sehr kurzfristig erarbeitet werden).

Dazu gehört insbesondere:

- Die generelle Aufrechterhaltung der IT,
- die Ausrüstung von Mitarbeitern mit Hard- und Software für einen Home-Office-Betrieb,
- Regelungen zum Support und zu Ansprechpartnern und Stellvertretungsregelungen,
- Stresstest der bestehenden Infrastruktur, bspw. bei weitgehender Home-Office-Arbeit,
- Aufrechterhaltung der Datensicherheitsmaßnahmen und Offenhaltung der Kommunikationswege,
- Richtlinien zum Umfang mit unternehmens- und personenbezogenen Daten im Home-Office,
- Kommunikationswege zu externen IT-Dienstleistern.

2. IT-bezogenes Vertragsmanagement

IT-Verträge folgen im Grundsatz dem allgemeinen Zivilrecht, also insbesondere dem Dienstvertrags- oder Werkvertragsrecht. In den allermeisten Fällen ist das vertragliche Verhältnis durch IT-Individualregelungen oder AGB konkretisiert. Solchen Regelwerken werden sich regelmäßig die Rechtsfolgen „*höherer Gewalt*" entnehmen lassen, also vor allem eine Möglichkeit der Leistungsverweigerung bzw. ein Ausschluss für eine Schadensersatzhaftung, wenn die Leistungserbringung durch „höhere Gewalt" unmöglich oder unzumutbar wird. Auftraggeber und Auftragnehmer sind indes gut beraten, die Voraussetzungen und Folgen eines vertraglich vereinbarten Gestaltungsrechts sorgsam abzuwägen. Für den Fall, dass keine AGB einbezogen sind und auch im Übrigen keine schriftliche Vertragsurkunde vorliegt oder in den vorhandenen Unterlagen keine Regelung zu den Folgen „*höherer Gewalt*" zu finden ist, müssen sowohl Auftragnehmer als auch Auftraggeber prüfen, ob nach den allgemeinen gesetzlichen Grundlagen ein Grund für die Nicht- oder zu späte Erbringung der Leistung besteht. Ein typisches Beispiel ist die tatsächliche Unmöglichkeit, beispielsweise, wenn einem externen IT-Dienstleister der Zugang zum Serverraum verwehrt bleibt, weil dieser gerade aus den Skiferien in Österreich zurückgekehrt ist. Inwieweit Folgen der Corona-Krise zu einer „höheren Gewalt" führen, kann nicht pauschal beantwortet werden (siehe dazu auch hier).

Zu beachten ist, dass der Gesetzgeber aktuell neue Regelung schafft: Ein aufgrund der Auswirkungen der Corona-Krise vom Gesetzgeber vorgesehenes zivilrechtliches Moratorium sieht ein besonderes Leistungsverweigerungsrecht für Kleinstunternehmen vor (bis 9 Mitarbeiter und 2 Mio. EUR Jahresumsatz; dazu auch hier). Das dürfte im Ansatzpunkt auf nahezu alle freiberuflichen IT-Dienstleister zutreffen (Freelancer), ebenso auf kleine Systemhäuser oder Softwareprogrammierer. Voraussetzung ist, dass infolge von Umständen, die auf die COVID-19-Pandemie zurückzuführen sind, das Unternehmen die Leistung nicht erbringen kann oder dem Unternehmen die Erbringung der Leistung ohne Gefährdung der wirtschaftlichen Grundlagen seines Erwerbsbetriebs nicht möglich wäre. Hier wird man sich in der Praxis zwangsläufig die Frage stellen, ob ein Unvermögen tatsächlich auf die Folgen der Ausbreitung des Virus zurückzuführen ist. Auch wird es

erheblichen Streit darüber geben, wann eine Gefährdung der wirtschaftlichen Grundlagen eines Erwerbsbetriebs vorliegt. Der Auftraggeber (Gläubiger) kann – sofern er selbst in wirtschaftliche Schieflage gerät – die Leistungsverweigerung zurückweisen, was wiederum zu einem Rücktrittrechts für den Schuldner führt.

3. HR-Themen, insbesondere Home-Office

Ohne entsprechende rechtliche Grundlage kann weder der Arbeitnehmer beanspruchen, im Home-Office zu arbeiten, noch der Arbeitgeber fordern, dass der Arbeitnehmer im Home-Office arbeitet. Daher bedarf es hier einvernehmlicher Absprachen; hierzu sollten viele Arbeitnehmer grundsätzlich bereit sein. Vor dem Ausspruch etwaiger Freistellungen sollten Sie daher versuchen, mit möglichst vielen Arbeitnehmern, die in eine Risikokategorie fallen, solche Home-Office-Vereinbarungen zu schließen. Der Abschluss einer entsprechenden Betriebsvereinbarung mit einem Betriebsrat dürfte nicht rechtswirksam sein. Wichtig ist im Übrigen, die arbeitsschutzrechtlichen Anforderungen an die Gestaltung des Arbeitsplatzes im Home-Office umzusetzen. Dazu dürfen wir auf die Hilfestellungen der Behörden in unserem ersten Beitrag verweisen.

Rein tatsächlich müssen die entsprechenden Kapazitäten für einen umfassenden Home-Office-Einsatz auch technisch gegeben sein. Das bedeutet: Mitarbeiter müssen über entsprechende Endgeräte sowie über einen gesicherten Zugang zum Firmennetzwerk verfügen. Dieser muss auch für den dann erheblich ausgeweiteten Zugriff ausgelegt sein. Das sollte rechtzeitig in Stresstests geprüft werden. Zu berücksichtigen ist insbesondere, dass die Anforderungen an den Daten- und Know-how-Schutz gewährleistet bleiben, dass also den Mitarbeitern verdeutlicht wird, welche Sicherheitsmaßnahmen sie von zu Hause erfüllen müssen und dass der Zugang zum Netzwerk angemessen abgesichert ist. Sollten sich hier Lücken auftun, gehen Unternehmen erhebliche Risiken im Bereich Datenschutz und Know-how-Schutz ein. Zu den aktuellen HR-Themen finden Sie auch hier weitere Informationen.

4. Automatisierte Geschäftsmodelle und Online-Vertrieb

Die interne Nutzung automatisierter Geschäftsprozesse hat selbstverständlich den Vorteil, dass diese unabhängig vom Gesundheitszustand der Belegschaft funktionieren. Hierbei sollte sichergestellt sein, dass Personen, die für den Support, die Wartung oder die Überwachung zuständig sind, im Betrieb oder von zu Hause arbeiten können und im Ernstfall auch einen oder mehrere Stellvertreter haben.

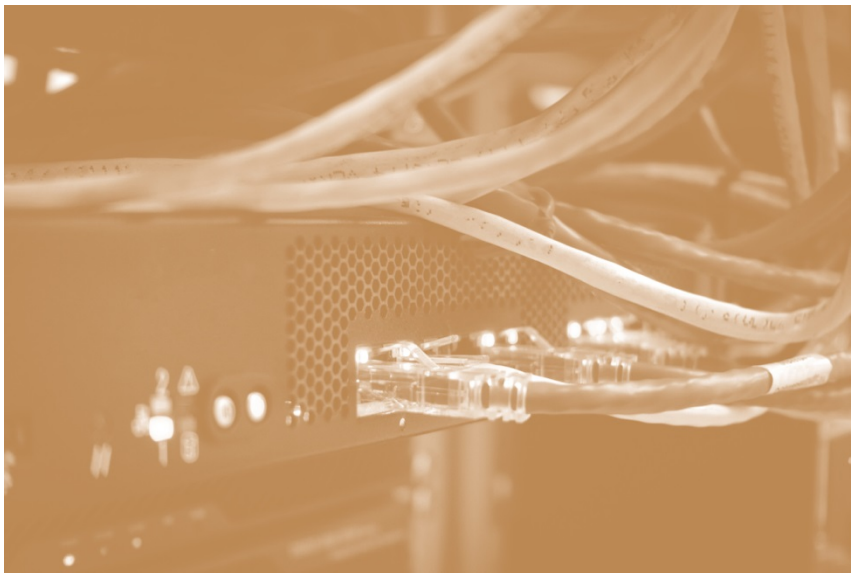
Der Onlinevertrieb funktioniert derzeit mehr oder weniger noch reibungslos, da die behördlichen Anordnungen zur Schließung von Ladenlokalen nur den stationären, also niedergelassenen Vertrieb mit einem direkten Kundenkontakt betreffen. Voraussetzung für einen funktionierenden Onlinevertrieb ist eine entsprechende Infrastruktur. Dazu gehört insbesondere ein funktionsfähiges Frontend (spezifisch für den B2B- oder B2C-Verkehr) sowie ein verlässliches Backend, dass im besten Fall mit der Lagerhaltung verknüpft ist, um echtzeitgenaue Lagerbestände im Shop anzuzeigen. Aus rechtlicher Sicht ist insbesondere darauf zu achten, dass Betreiber alle Informationspflichten erfüllen. Diese sind insbesondere im B2B-Bereich äußerst detailliert und vielgestaltig und betreffen sowohl die äußere Gestaltung des Webshops, als auch die zur Durchführung einer Bestellung erforderliche Kommunikation via E-Mail. Ungenauigkeiten und Fehler können in diesem Bereich schnell zu Abmahnungen durch Wettbewerber oder Verbraucherverbände führen. Ferner sind Betreiber von Webshops sehr gut beraten, entsprechende und auf ihre Interessen zugeschnittene AGB zu verwenden. Hersteller, die ihren Händlern Vorgaben zum Onlinevertrieb machen wollen, haben zudem die vertriebskartellrechtlichen Schranken zu beachten.

5. Datenschutz/Know-how-Schutz/Compliance

Das Datenschutzrecht und das Geschäftsgeheimnisgesetz kennen keine Amnestie für Krisenzeiten. Die Compliance-Maßnahmen dürfen also nicht ausgesetzt werden. Entscheidend ist insbesondere, dass auch in Krisenzeiten und bei allem Trubel die Kommunikationswege sichergestellt und nicht „verstopft“ sind, sondern freigehalten werden. Denn sollte sich zur Corona-Krise noch ein weitläufiges und unbemerkt gebliebenes Datenleck gesellen, dürften die Kapazitäten von Unternehmen in IT, Personal- und Rechtsabteilung bald an ihre Grenzen geraten. Denn dann

ergeben sich zahlreiche neue und vor allem haftungsträchtige Probleme aus den Bereichen Datenschutz und Know-how Schutz.

Werden Home-Office-Arbeitsplätze neu geschaffen, wird auch die Erarbeitung einer entsprechenden Richtlinie erforderlich werden, die den Umgang mit unternehmens- und personenbezogenen Daten regelt. Nur so können wertvolles Know-how wirksam geschützt und Datenschutzverstöße vermieden werden.



Zu guter Letzt: Geldbußen des Monats

Zu guter Letzt haben wir diesmal einige interessante Bußgelder aus dem Norden für Sie – teils gar aus EWR-Staaten, die die DSGVO inkorporiert haben – und zwei Kuriositäten.

- **Norwegen**

Die norwegische Datenschutzaufsichtsbehörde hat der Gemeinde Rælingen eine Geldbuße in Höhe von umgerechnet rund 80.000 Euro auferlegt. Die Gemeinde nutzte an Schulen eine App, die die Kommunikation zwischen Schulen und Eltern von Kindern mit Behinderungen vereinfachen sollte. Innerhalb dieser App konnten die Eltern in den entsprechenden Feldern Angaben zur Gesundheit und Medikation der Kinder machen. Die App war ohne Log-in zugänglich. Auch gab es keinerlei Richtlinien für Eltern und Lehrer, wie mit den personenbezogenen Daten der betroffenen Kinder umgegangen werden sollte.

Angesichts derartiger technisch-organisatorischer Mängel stellte die Datenschutzaufsichtsbehörde einen Verstoß gegen Art. 32 DSGVO fest. Überdies war angesichts dessen die Einwilligung der Eltern unwirksam.

- **Island**

In Island kam es – ebenfalls im Zusammenhang mit einer Schule – zur Verhängung eines Bußgeldes in Höhe von umgerechnet 9.000 Euro durch die dortige Datenschutzaufsichtsbehörde.

Versehentlich versendete ein Lehrer im Anhang einer E-Mail vertrauliche Informationen über ehemalige Schülerinnen und Schüler. Die Informationen stammten aus einer früheren Befragung des Lehrers und enthielten überwiegend Angaben zum Wohlbefinden, den Lernerfolgen aber auch zu sozialen Beziehungen, Eigenschaften, die den Befragten fehlten und teilweise sogar Angaben zur geistigen und körperlichen Gesundheit.

- **Dänemark**

In Dänemark kam es bei mehr als 20 Banken zu Verstößen gegen den Datenschutz, insbesondere gegen Art. 33 DSGVO. Zwischen Mai 2018 und August 2019 kam es zur ungewollten Offenlegung persönlicher Adressen von mehr als 20.000 Bankkunden im Zusammenhang mit Überweisungen zwischen unterschiedlichen Banken. Grund dafür war ein Fehler in der von den Banken verwendeten Software, die mangels Verschlüsselung die übermittelten Daten nicht schützte. Bei einem derart massiven Fehler erstaunlich: Da unmittelbar nachdem der Fehler aufgefallen war schnell und effektiv Maßnahmen zur Behebung eingeleitet wurden, sah die dänische Datenschutzaufsichtsbehörde von der Verhängung eines Bußgeldes ab.

- **Auftragsverarbeitung in allen Fällen**

Insbesondere im Finanzsektor tätige Unternehmen sind qua Gesetz verpflichtet, der BaFin eine Reihe von Informationen zu übermitteln. Vielfach haben diese Unternehmen dazu wohl einen Auftragsverarbeitungsvertrag von der BaFin verlangt – mit ihnen als Auftraggeber und der BaFin als kontrolliertem (!) Auftragnehmer. Sie merken vermutlich sofort: Dies passt vorne und hinten nicht. Das liegt auch auf der Hand – die BaFin erfüllt hier eigenverantwortlich die ihr obliegenden gesetzlichen Aufgaben.

Dennoch hat sich dieses Phänomen derart gehäuft, dass die BaFin in ihren FAQ zum MVP-Portal darauf hinweist.

- **Listenpflicht und Einwilligung: +/+ oder +/-?**

Gerade zu Beginn der Corona-Krise wurden zunehmend Anwesenheitslisten geführt, auf Veranstaltungen, in öffentlichen Verkehrsmitteln oder Flugzeugen. Der Zweck derartiger Listen lag in der Ermöglichung der Kontaktaufnahme und Nachverfolgung etwaiger Infektionsketten und damit vermutlich oftmals im öffentlichen Gesundheitsinteresse. Zur Erinnerung: Dann ist eine Datenverarbeitung schon auf gesetzlicher Grundlage erlaubt. Dennoch haben verschiedene Städte und Kommunen zeitglich mit dem Hinweis auf die Pflicht zur Angabe von Namen und Kontaktmöglichkeiten eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO eingeholt. Kurios und für uns im Dunkeln bleibt, wie eine solche Einwilligung dann freiwillig sein kann.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de