Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 01/2020

Der IT-Ticker 01/2020 informiert Sie über folgende Themen:

Auswirkung von COVID-19 auf laufende IT-Verträge

Im Zusammenhang mit dem Coronavirus und der Erfüllung von laufenden IT-Verträgen bestehen aktuell viele Unsicherheiten und Fragen. Sind die Vertragspartner von ihrer Leistungspflicht befreit? Muss der Softwareentwickler auch bei Erkrankung leisten und hat er noch Anspruch auf seine vertraglich vereinbarte Vergütung? Wann kann der Entwicklungsauftrag beendet werden? Besteht in IT-Serviceverträgen die Möglichkeit einer Entlastung eines Vertragspartners unter Berufung auf höhere Gewalt (force majeure)?

Die für IT-Verträge relevanten Regelungen in deutschen Gesetzen kennen den Begriff der höheren Gewalt nicht. Vielfach enthalten allerdings Verträge und Allgemeine Geschäftsbedingungen Regelungen zu diesem Themenkomplex. Diese Regelungen müssen im Einzelfall auf ihre Vereinbarkeit mit dem strengen deutschen AGB-Recht überprüft werden. Hinzu kommt, dass ein Ereignis der höheren Gewalt an enge Voraussetzungen gebunden ist, wie der Unvorhersehbarkeit des Ereignisses, das den Verwender an seiner Leistungsfähigkeit hindert. Wenn dieses Ereignis in Maßnahmen zur Eindämmung von COVID-19 besteht (z.B. Qurantänemaßnahmen), dürften diese zumindest bei Verträgen, die noch Ende Februar/ Anfang März 2020 abgeschlossen wurden, kaum mehr unvorhersehbar gewesen sein.

Wurden keine ausdrückliche Regelung getroffen, kommt es für die Frage, ob sich der Vertragspartner bei COVID-19 bedingten Leistungsschwierigkeiten entlasten kann, nach deutschem Recht auf die Frage an, ob Unmöglichkeit vorliegt.

Die reine Sorge vor einer Ansteckung begründet grundsätzlich keinen Fall der Unmöglichkeit, der die Vertragsparteien von ihren Leistungsverpflichtungen befreit. Etwas anderes kann nur in absoluten Ausnahmefällen gelten, wenn dem Vertragspartner aufgrund subjektiver Umstände die Leistungserbringung nicht zumutbar ist.

Liegt ein behördliches Verbot vor, welches die Durchführung des Vertrages hindert, (etwa eine Reisebeschränkung oder Ausgangssperren), kann ein Fall der (zumindest vorübergehenden) Unmöglichkeit vorliegen. In diesem Fall ist es der Vertragspartei zunächst vorübergehend unmöglich, ihren vertraglichen Leistungspflichten nachzukommen. Scheitert eine einvernehmliche Verschiebung

des Vertragszeitraums, kann die Leistungserbringung unter Umständen endgültig unmöglich werden. In diesem Fall besteht weder das Recht noch die Pflicht, die Vertragsleistung zu erbringen, auch erlöschen Anspruch und Pflicht auf Zahlung der Vergütung.

Soweit IT-Dienstleister und Softwareentwickler z.B, im Rahmen von Individualsoftwareentwicklung als Werkunternehmer tätig sind, sind sie hingegen vorleistungspflichtig. Ihre Vergütung können sie im Grundsatz erst dann verlangen, wenn das vollständige Werk (bspw. die Programmierleistung oder Implementierung/Datenmigration) durch den Besteller abgenommen worden ist. Es bestehen jedoch zwei Ausnahmen:

(1) Bei stufenweise abzunehmenden und zu vergütenden Werken, wie den Leistungsabschnitten eines Softwareprojekts, entfällt der Vergütungsanspruch für die bereits abgenommenen Teilleistungen des Werkunternehmers selbst im Fall eines späteren Projektabbruchs nicht.

(2) Wird die weitere Werkerstellung durch einen in der Person oder dem Verhalten des Bestellers liegenden Grund (Sphäre) unausführbar, hat der Werkunternehmer einen Anspruch auf den Teil der Vergütung und Ersatz etwaiger Auslagen, der der bisher geleisteten Arbeit entspricht. Ein Projektabbruch auf Grund öffentlicher Anordnung oder überwiegender Gesundheitsrisiken stellt nach unserer Auffassung jedoch keinen in der Sphäre des Softwareentwicklers liegenden Grund dar.

Der Auftraggeber kann einen Werkvertrag bis zur Vollendung des Werkes jederzeit und ohne besonderen Grund kündigen. In einem solchen Fall behält der Werkunternehmer seinen Anspruch auf Werklohn, muss sich jedoch ersparte Aufwendungen und anderweitig erzielte Verdienste darauf anrechnen lassen. Erfolgt eine Kündigung aus wichtigem Grund besteht ein Anspruch auf Vergütung nur für die bis zur Kündigung erbrachten Werkleistungen. Auf Seiten des Auftraggebers dürfte COVID-19 keinen wichtigen Kündigungsgrund darstellen. Auftragnehmer mit Kundenkontakt wie IT Servicetechniker oder Trainer und Workshopleiter können jedoch in der Regel in unverschuldeten Fällen von COVID-19-Infektionen den IT-Vertrag aus wichtigem Grund kündigen. Die Vorschriften über die sogenannte „Störung der Geschäftsgrundlage“ können zu einem Anspruch auf Anpassung des Vertrages (ggf. Verschiebung der Leistungszeiträume) führen. Wird die Vollendung des Werkes dauerhaft unmöglich (z.B. weil die Migration von Daten zum einzig möglichen und vereinbarten Stichtag nicht erfolgt ist), kann auch ein Rücktritt vom Vertrag erfolgen. In einem solchen Fall sind bereits erbrachte Leistungen zurückzuerstatten bzw. entsprechender Wertersatz zu leisten.

Praxishinweis:

Für Auftragnehmer ist es wichtig, mögliche Vertragsklauseln zu höherer Gewalt zu prüfen, die unter Umständen jeweils bereits die Konsequenzen regeln. Sie sollten Anzeigepflichten beachten, die sich aus diesen Klauseln ergeben. Wichtig ist auch die Einhaltung etwaiger vertraglicher Formerfordernisse für solche Anzeigen (z.B. Schriftform).

Auftraggeber dürfen von ihren Dienstleistern regelmäßig zumutbare Maßnahmen verlangen, die eigene Leistungsfähigkeit trotz der Auswirkungen des Coronavirus sowie der damit zusammenhängenden behördlichen Maßnahmen aufrechtzuerhalten.

In jedem Fall sollten mögliche Leistungsschwierigkeiten frühzeitig kommuniziert werden, um dem Vertragspartner die Möglichkeit zu geben, sich auf das Leistungshindernis einzustellen, Vorkehrungen zu treffen und schadensmindernde Maßnahmen zu ergreifen.

In Zweifelsfragen über die Auslegung vertraglicher Regeln und bei der Anwendung der gesetzlichen Regeln unterstützen wir Sie gerne.

Franka Becker, Düsseldorf
f.becker@skwschwarz.de
Dr. Matthias Orthwein, München
m.orthwein@skwschwarz.de

Absage oder Verschiebung von Veranstaltungen in Zeiten des Coronavirus – Welche Ansprüche bestehen?

Vor dem Hintergrund der aktuellen Entwicklungen im Zusammenhang mit dem Coronavirus werden derzeit zahlreiche Veranstaltungen (Messen, Kongresse, Konzerte usw.) abgesagt oder verschoben. Die Gründe für eine solche Absage oder Verschiebung sind vielschichtig: gerade bei größeren Veranstaltung liegt der Grund für die Absage/Verschiebung zumeist an einem behördlichen Verbot, andere Veranstaltungen werden abgesagt/verschoben, um die Gesundheit der Teilnehmer zu schützen oder weil Mitarbeiter des Veranstalters selbst erkrankt sind oder sich in Quarantäne befinden. Im Fall einer Absage/Verschiebung stellen sich Veranstalter und Teilnehmer die Frage, ob bereits vereinnahmte Entgelte (beispielsweise für Eintrittskarten) behalten werden dürfen oder Zahlungsansprüche fortbestehen bzw. – auf der anderen Seite – ob ein Anspruch auf Erstattung bereits gezahlter Entgelte und weiterer Schäden besteht.

1. Vorrang vertraglicher Vereinbarungen
Auszugehen ist hierbei zunächst von dem Grundsatz, dass Verträge einzuhalten sind. Findet eine Veranstaltung trotz „Corona-Krise“ statt und entscheidet sich der Teilnehmer dennoch, auf einen Besuch der Veranstaltung zu verzichten, besteht daher grundsätzlich kein Erstattungsanspruch gegen den Veranstalter. Insbesondere liegt in einer – möglicherweise sogar begründeten – Angst vor einer Infizierung mit dem Coronavirus kein Fall einer sog. Unmöglichkeit (siehe unten), die den Teilnehmer von seiner Pflicht zur Zahlung des vertraglich vereinbarten Entgelts befreit. Für den Fall, dass eine Veranstaltung jedoch abgesagt oder verschoben wird, kommt es für die Frage, ob Zahlungs- bzw. Erstattungsansprüche bestehen, in erster Linie auf den Vertrag zwischen Veranstalter und Teilnehmer sowie auf gegebenenfalls zusätzlich geltende Allgemeine Geschäftsbedingungen an. Erst wenn der Vertrag keine Rücktritts-, Kündigungs- oder vergleichbare Regelungen (beispielsweise sogenannte Force-Majeure-Klauseln, siehe unten) enthält, kommen die gesetzlichen Vorschriften zur Anwendung. Aus diesem Grund bedarf es zur Prüfung etwaiger Zahlungs- oder Erstattungsansprüche stets einer individuellen Prüfung der geschlossenen Verträge einschließlich einbezogener AGB.

2. Absage/Verschiebung der Veranstaltung aufgrund behördlicher Anordnung?
Wird eine Veranstaltung abgesagt oder verschoben, kommt der Frage, ob die Absage/Verschiebung aufgrund einer behördlichen Anordnung oder freiwillig durch den Veranstalter erfolgte, entscheidende Bedeutung zu:
Beruht die Absage/Verschiebung der Veranstaltung auf einer behördlichen Anordnung, ist es dem Veranstalter unmöglich, seinen vertraglichen Pflichten nachzukommen, so dass er nach dem deutschen Zivilrecht von der Leistungspflicht – Durchführung der Veranstaltung – befreit wird. Auf die Frage, ob auch eine gegebenenfalls vereinbarte Force-Majeure-Klausel eingreift (siehe unten), kommt es dann nicht mehr an. Im Gegenzug wird auch der Teilnehmer von seiner Pflicht befreit, das Entgelt für die Veranstaltung zu zahlen. Hat der Teilnehmer das Entgelt bereits vorab gezahlt, ist dieses zu erstatten. Fraglich ist dann nur noch, ob der Teilnehmer zusätzlich Anspruch auf Erstattung weiterer Schäden hat. Dies ist nicht der Fall, wenn der Veranstalter darlegen und beweisen kann, dass er die Unmöglichkeit nicht verschuldet oder aus anderen Rechtsgründen zu vertreten hat. Gelingt dies dem Veranstalter nicht, hat er dem Teilnehmer Schadenersatz zu leisten oder auf Seiten des Teilnehmers entstandene vergebliche Aufwendungen (beispielsweise für bereits gebuchte Fahrkarten oder Hotelbuchungen) zu erstatten.
Erfolgt die Absage/Verschiebung der Veranstaltung dagegen aufgrund eines freiwilligen Entschlusses des Veranstalters – etwa weil er vorbeugend handeln und die Gesundheit der Teilnehmer vor dem Coronavirus schützen will –, ist die Frage, ob der Veranstalter die Absage/Verschiebung verschuldet oder aus anderen Rechtsgründen zu vertreten hat, deutlich schwieriger zu beantworten: Während für Fälle, in denen eindeutig der Schutz der Gesundheit der Teilnehmer im Vordergrund steht, ein Verschulden wohl zu verneinen sein dürfte, ist dies bei einer Absage/Verschiebung mit dem bloßen allgemeinen Verweis auf die „Corona-Krise“ fraglich.

3. Keine Erstattungspflicht aufgrund „höherer Gewalt“?
Allerdings ist ein Verschulden immer dann ausgeschlossen, wenn ein Fall sog. „höherer Gewalt“ (französisch „force majeure“) vorliegt. Der Begriff selbst ist im deutschen Zivilrecht nicht definiert. Die Rechtsprechung versteht darunter ein *„betriebsfremdes, von außen durch elementare Naturkräfte oder durch Handlungen dritter Personen herbeigeführtes Ereignis, dass nach menschlicher Einsicht und Erfahrung unvorhersehbar ist, mit wirtschaftlich erträglichen Mitteln auch durch die äußerste, nach der Sachlage vernünftigerweise zu erwartende Sorgfalt nicht verhütet oder unschädlich gemacht werden kann und auch nicht wegen seiner Häufigkeit vom Betriebsunternehmer in Kauf zu nehmen*

ist". Beispiele für typischen Fälle „höherer Gewalt" sind danach Naturkatastrophen, Streiks oder terroristische Angriffe. Nach der Rechtsprechung können darunter aber auch Epidemien oder Seuchen fallen. So haben einzelne Gerichte in der Vergangenheit beispielsweise den SARS-Virus und den Ausbruch von Cholera als Fälle „höherer Gewalt" qualifiziert. Ob tatsächlich auch die „Corona-Krise" einen solchen Fall darstellt (mit der Folge, dass auch bei einer freiwilligen Absage/Verschiebung keine Erstattungsansprüche des Teilnehmers bestehen), ist aber alles andere als eindeutig. Vielmehr sind im Rahmen einer individuellen Betrachtung stets die Umstände des Einzelfalls zu prüfen, ob den Veranstalter ein Verschulden an der Absage/Verschiebung der Veranstaltung (ohne behördliche Anordnung) trifft. Dies gilt insbesondere für Sonderfälle, in denen die Absage/Verschiebung aus Sicht des Veranstalters notwendig wird, weil Mitarbeiter – im schlimmsten Fall das ganze Team oder zumindest ein Großteil der Mitarbeiter – am Coronavirus erkrankt oder unter Quarantäne gestellt wird oder die Veranstaltung durch eine Vielzahl von Teilnehmerabsagen wirtschaftlich nicht mehr vertretbar erscheint. Während im erstgenannten Fall vieles gegen ein Verschulden spricht, dürfte der letztgenannte Fall eher anders zu beurteilen sein.

4. Ergebnis

Zusammenfassend bleibt festzuhalten, dass die Frage, ob und welche Zahlungs- oder Erstattungsansprüche sich aus der Absage oder Verschiebung von Veranstaltungen wegen des Coronavirus ergeben, vor allem von den vertraglichen Regelungen zwischen Veranstalter und Teilnehmer abhängen. Existieren keine vertraglichen Regelungen oder sind diese nicht anwendbar, besteht keine Erstattungspflicht des Veranstalters, wenn die Veranstaltung aufgrund behördlicher Anordnung abgesagt oder verschoben wurde. Im Fall einer freiwilligen Absage/Verschiebung könnte dagegen ein Fall „höherer Gewalt" vorliegen, was zur Folge hätte, dass ebenfalls keine Erstattungsansprüche bestehen. Hierfür ist aber stets eine individuelle Prüfung erforderlich. Im Rahmen der Prüfung sowie des weiteren Vorgehens sind vor allem folgende Punkte relevant:

- **Veranstalter/Teilnehmer**: Prüfung der vertraglichen Vereinbarungen (einschließlich AGB)
- **Veranstalter**: Zusätzliche Prüfung von Versicherungsschutz / Ermittlung von (rechtlichen) Risiken / Abwägung zwischen Gründen für Absage/Verschiebung und den Risiken einschließlich Dokumentation der Entscheidungsgründe
- **Veranstalter**: Information der Teilnehmer und sonstiger Dritter / Vornahme schadensmindernder Maßnahmen; **Teilnehmer**: Gegebenenfalls Geltendmachung von Ansprüchen gegen den Veranstalter
- **Veranstalter/Teilnehmer** Vor Einleitung rechtlicher Schritte Gespräche, ob eine einvernehmliche Lösung möglich ist

Jens Borchardt, Hamburg
j.borchardt@skwschwarz.de

Steht der Datenschutz dem Infektionsschutz im Weg?

Das Corona-Virus (Covid-19) stellt die Menschen vor große Herausforderungen. Die WHO hat Covid-19 mittlerweile als Pandemie eingestuft. Die Zahl der Infizierten steigt täglich. Die Folgen sind noch nicht abschätzbar und die Verunsicherung nimmt zu.

Datenschutz ist in diesem Zusammenhang sicherlich nicht das wichtigste Thema. Dennoch stellt sich vermehrt auch die Frage: Welche Maßnahmen erlaubt der Datenschutz dem Arbeitgeber und dem Unternehmen? Dürfen zum Schutz der Mitarbeiter, des Unternehmens und der Kunden oder Besucher sensible (Gesundheits-)Daten von Mitarbeitern und Besuchern erhoben werden? Die europäischen Datenschutzaufsichtsbehörden haben dazu unterschiedliche Auffassungen. Deutsche Datenschutzaufsichtsbehörden halten die Erhebung solcher Daten unter bestimmten Voraussetzungen grundsätzlich für zulässig. Die Maßnahmen müssen dabei vor allem notwendig und verhältnismäßig sein. Wann dies der Fall ist, wird im Einzelfall entschieden werden müssen.

Bei der Erhebung von personenbezogenen Daten im Zusammenhang mit der Corona-Pandemie werden typischerweise Bezüge zwischen Personen und deren Gesundheitszustand hergestellt. In diesem Fall handelt es sich um Gesundheitsdaten, die nach Artikel 9 Datenschutz-Grundverordnung (DSGVO) besonders geschützt sind. Die Verarbeitung von Gesundheitsdaten ist grundsätzlich nur eingeschränkt möglich. Diese Daten dürfen aber gegebenenfalls zur Eindämmung der Corona-Pandemie oder zum Schutz von Mitarbeitern datenschutzkonform verarbeitet werden. Mittlerweile

haben sich einige deutsche Datenschutzaufsichtsbehörden dazu geäußert und stellen Übersichten zum Umgang mit der Corona-Pandemie für Arbeitgeber zur Verfügung:

- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesbeauftragte für den Datenschutz Niedersachsen
- Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Die deutschen Aufsichtsbehörden kommen zu dem Ergebnis, dass Arbeitgeber alle Informationen erheben dürfen, die sie benötigen, um ihrer Sicherungspflicht nachzukommen. Die Fürsorgepflicht verpflichtet Arbeitgeber dazu, den Gesundheitsschutz der Gesamtheit ihrer Beschäftigten sicherzustellen. Davon sind Maßnahmen umfasst, die andere Beschäftigte vor einer Infektion durch eine erkrankte Person schützen. Diese Maßnahmen müssen dabei immer notwendig und verhältnismäßig sein. Die Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks, also typischerweise spätestens am Ende der Pandemie, müssen die erhobenen Daten unverzüglich gelöscht werden.

Was bedeutet dies jedoch jetzt genau für die Vielzahl von Maßnahmen, welche Arbeitgeber zum Schutz ihrer Beschäftigten aktuell ergreifen wollen oder müssen. Nachfolgend werden exemplarisch einige Maßnahmen dargestellt und auf Basis der oben erwähnten aktuellen Stellungnahmen kurz datenschutzrechtlich bewertet:

1. Zur Eindämmung und Bekämpfung der Corona-Pandemie kann es datenschutzrechtlich zulässig sein, wenn ein Arbeitgeber Informationen darüber erhebt, zu welchen Personen der erkrankte Mitarbeiter Kontakt hatte.
2. Die Nennung des Namens des betroffenen Mitarbeiters gegenüber Kollegen ist grundsätzlich zu vermeiden. Eine Namensnennung kann allerdings im Einzelfall notwendig sein, wenn Mitarbeiter, die in direktem Kontakt mit einem Infizierten waren, gewarnt und selbst zur Eindämmung der Ansteckungsgefahr von der Arbeit freigestellt werden müssen und diese ohne Namensnennung nicht ausfindig gemacht werden können.
3. Zudem darf der Arbeitgeber Urlaubsrückkehrer befragen, ob sie sich in einem durch das Robert Koch-Institut festgelegten Risikogebiet aufgehalten haben. Eine Negativauskunft des Beschäftigten genügt aber regelmäßig. Weitere Nachfragen dürfen allerdings erfolgen, wenn es dafür Gründe bzw. weitere Anhaltspunkte gibt, die diese rechtfertigen.
4. Darüber hinaus dürfen Arbeitgeber von ihren Beschäftigten grundsätzlich auch die aktuelle private Handynummer abfragen und temporär speichern, damit die Beschäftigten kurzfristig gewarnt werden können und z.B. nicht bei der Arbeit erscheinen. Dies ist allerdings nur mit Einverständnis des Beschäftigten zulässig und muss der Verringerung der Infektionsgefährdung dienen. Zu anderen Zwecken darf die Handynummer in keinem Fall verwendet werden, z.B. Kontaktaufnahme aus beruflichen Gründen nach Feierabend.
5. Die deutschen Datenschutzaufsichtsbehörden haben sich zu der Frage, ob Fiebermessen bei Arbeitnehmern und Besuchern zulässig ist, noch nicht positioniert. Bei Besuchern kann diese Maßnahme grundsätzlich vom Hausrecht des Arbeitgebers gedeckt sein. Anders ist das Temperaturmessen aber bei Beschäftigten zu bewerten. Bei Beschäftigten ist das verfassungsrechtlich geschützte Persönlichkeitsrecht zu berücksichtigen und es muss daher eine Verhältnismäßigkeitsprüfung stattfinden. Bei der Prüfung der Angemessenheit der Maßnahme kann die Branche des Unternehmens eine Rolle spielen (bspw. Lebensmittelbranche). Zudem kann ggfls. berücksichtigt werden, ob es bereits Verdachtsfälle in dem Betrieb gibt, ob ein Arbeitnehmer in einem Risikogebiet war oder ob das Unternehmen in einer Region gelegen ist, in der es eine Vielzahl von Infizierten gibt. Dies können gute Argumente sein, die für die Zulässigkeit des Temperaturmessens sprechen.

Die notwendigen Maßnahmen lassen sich rechtlich auf Grundlage der DSGVO und des BDSG (ggf. in Verbindung mit Landesdatenschutz- und weiteren Fachgesetzen) legitimieren. Die Berechtigung zur Verarbeitung personenbezogener Mitarbeiterdaten ergibt sich für Arbeitgeber im nicht-öffentlichen Bereich aus § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. f) DSGVO jeweils in Verbindung mit den einschlägigen beamtenrechtlichen sowie tarif-, arbeits- und sozialrechtlichen Regelungen des nationalen Rechts. Soweit Gesundheitsdaten verarbeitet werden, sind zudem § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b) DSGVO einschlägig.

Ähnlich wie die deutschen Datenschutzbehörden halten die irische Datenschutzaufsichtsbehörde DPC, die ungarische Datenschutzaufsichtsbehörde NAIH und die englische

Datenschutzaufsichtsbehörde ICO die Verarbeitung personenbezogener Daten, einschließlich Gesundheitsdaten, für zulässig, wenn dies notwendig und verhältnismäßig ist. Zu den Maßnahmen gehört nach der irischen DPC ausdrücklich auch die Verpflichtung aller Mitarbeiter zum Ausfüllen eines Fragebogens.

Ganz anders sieht das die französische Datenschutzaufsichtsbehörde CNIL. Danach dürfen Arbeitgeber keine Maßnahmen ergreifen, welche die Privatsphäre der Betroffenen verletzen können, insbesondere durch die Erhebung von Gesundheitsdaten. Diese Daten unterliegen laut CNIL dem besonderen Schutz der DSGVO und nationalen Bestimmungen. Das systematische Sammeln medizinischer Aufzeichnungen oder Fragebögen von allen Mitarbeitern sei daher unzulässig. In ähnlicher Weise äußert sich die luxemburgische Datenschutzaufsichtsbehörde CNPD.

Die CNIL weist zudem ausdrücklich darauf hin, dass obligatorische Körpertemperaturmessungen jedes Mitarbeiters oder Besuchers, die täglich an seine Vorgesetzten gesendet werden, unzulässig sind. Diese Ansicht teilen die italienische Datenschutzaufsichtsbehörde Garante sowie die niederländische Datenschutzaufsichtsbehörde AP.

Praxistipp:

Die Entwicklungen in Zeiten von Covid-19 sind dynamisch und die beschriebenen Positionen können sich deshalb auch jederzeit ändern. Zudem zeigen die unterschiedlichen Argumente und Bewertungen durch die europäischen Datenschutzaufsichtsbehörden, dass eine allgemeingültige Antwort auf die Frage der datenschutzrechtlichen Zulässigkeit einer Maßnahme kaum möglich ist. Ob eine Maßnahme zum Schutz der Mitarbeiter und des Unternehmens durch den Arbeitgeber zulässig ist oder nicht, kann daher auch immer nur am Status Quo und anhand des konkreten Einzelfalls bewertet werden.

Wir empfehlen daher, immer aktuell den konkreten Einzelfall zu beurteilen und unter Einbindung des Betriebsrates und des betrieblichen oder externen Datenschutzbeauftragten zu entscheiden, welche konkrete Maßnahme erforderlich und angemessen ist. Gerne unterstützen wir Sie bei der Beurteilung der datenschutzkonformen Verarbeitung von Daten im Zusammenhang mit der Umsetzung von Maßnahmen zur Eindämmung der Corona-Pandemie und zum Schutz der Beschäftigten und des Unternehmens.

Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de
Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de
Esther Noske Frankfurt/Main
e.noske@skwschwarz.de

Covid-19 und die IT-Notfallplanung im Unternehmen

Covid-19 und das Coronavirus haben das öffentliche Leben im Griff und Unternehmen prüfen, ob sie alle notwendigen Schritte unternommen haben, um die Folgen der Pandemie ausreichend abzufedern. Auch die Aufrechterhaltung einer funktionsfähigen IT-Infrastruktur ist für die meisten Unternehmen in einer digitalisierten Wirtschaft überlebensnotwendig. Dies gilt umso mehr, wenn gegenüber dem Regelbetrieb zusätzliche Remote Arbeitsmöglichkeiten eingerichtet und mit ausreichender Bandbreite und Hard- und Software versorgt werden müssen.

Neben der kaufmännischen Vernunft gebietet auch das Gesetz, dass die Unternehmen sich angemessen mit drohenden Risiken für den Unternehmensbetrieb befassen. Das gilt selbstverständlich an erster Stelle für Betriebe, die eine hohe Bedeutung für das Gemeinwesen haben und deren Ausfall die öffentliche Versorgung und Sicherheit gefährden würde. Diese Betreiber kritischer Infrastrukturen (KRITIS) werden u.a. durch das IT-Sicherheitsgesetz zur Risikovorsorge und zur Errichtung effektiver Notfallpläne verpflichtet. Auch bei der Verarbeitung personenbezogener Daten formuliert die Datenschutzgrundverordnung (Art. 32 Abs. 1 c) DSGVO) die Pflicht des Verantwortlichen und seiner Auftragsverarbeiter durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Daten auch in einer Krise rasch wiederhergestellt werden kann. Banken und Finanzdienstleister müssen gem. § 25a KWG und der

darauf basierenden Grundsätze der Bankenaufsicht „MaRisk“ zusammen mit ihrem IT-Dienstleister ein Notfallkonzept aufstellen und dessen Wirksamkeit regelmäßig durch dokumentierte Notfallübungen überprüfen. Das umfasst auch die Entwicklung von Geschäftsfortführungs- und Wiederanlaufplänen. Schließlich ergibt sich aus der allgemeinen gesetzlichen Pflicht zur kaufmännischen Sorgfalt gem. § 43 Abs. 1 GmbHG und § 91 Abs. 2 AktG eine ganz persönliche Unternehmerpflicht, die Aufstellung und Überwachung eines Notfallkonzeptes für unternehmenskritische Systeme und einen angemessenen Versicherungsschutz für den IT Ausfall sicherzustellen. Die Ausführung und Erstellung der Pläne kann z.B. auf den IT-Leiter delegiert werden, die Verantwortung für das Vorhandensein selber bleibt aber immer bei der Unternehmensleitung.

Praktisch stellt sich nun die Frage, welche Risiken in einem solchen Notfallplan zu adressieren sind und wie man dabei mit dem Pandemiefall umgeht. In der Praxis bilden viele IT-Notfallpläne bisher lediglich Naturkatastrophen, technische Ausfälle und Einbruch oder Vandalismus ab. Der Fokus liegt auf einem Ausfall der technischen Infrastruktur. Den Fall, dass die betreuenden Menschen und Servicetechniker ausfallen könnten, die zur Sicherstellung des Betriebes notwendig sind, wird in der Praxis bisher zu oft vernachlässigt. Dabei brauchen die Mitarbeiter noch nicht einmal selber von einem Virus befallen zu sein. Die aktuelle Entwicklung zeigt, welche Personallücken entstehen können, wenn bereits Verdachtsfälle für 14 Tage in häusliche Isolation beordert werden oder wenn die Kinderbetreuung ohne Alternativbetreuung ausfällt. Die Schließung von Betriebsstätten und Büros zur Vermeidung von Infektionen ist eine weitere Herausforderung für den fortlaufenden Betrieb von Servern und IT-Infrastruktur an diesen Standorten.

Praxistipp:

Egal, ob die vorhandenen Notfallpläne den Pandemiefall in zivilisierten Gesellschaften nicht als realistisches Szenario vorhergesehen haben oder ob die Erstellung und Erprobung von Notfallplänen für die IT bisher ganz einfach dem Unternehmensalltag zum Opfer gefallen sind: Spätestens jetzt ist der Zeitpunkt gekommen, die Aufrechterhaltung der oft überlebenswichtigen IT-Infrastruktur zu planen, vorhandene Pläne an die aktuellen Entwicklungen und Erfahrungen anzupassen und mit Blick auf die spezifischen Besonderheiten und Bedürfnisse des Unternehmens weiterzuentwickeln.

Gerne unterstützen wir Sie bei der Entwicklung entsprechender Regelungskonzepte und deren Implementierung, z.B. bei der (Nach-)Verhandlung der entsprechenden Supportverträge mit externen Dienstleistern oder bei der arbeitsrechtlich wirksamen Umsetzung der notwendigen Vorgaben im Unternehmen.

Praktische Hilfestellungen zur Erstellung und dem Inhalt von IT-Notfallplänen finden sich nicht zuletzt beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und insbesondere in den BSI-Standards (vgl. BSI-Standard 100-4: Notfallmanagement). Selten hat sich so deutlich gezeigt, dass die gerne als „bürokratisch“ oder „hinderlich“ geschmähten IT-Compliance-Anforderungen ganz reale Bedeutung für den Fortbestand des Unternehmens bekommen können. Sprechen Sie uns an, wie wir Sie bei Ihren dahingehenden Anstrengungen unterstützen können.

Dr. Matthias Orthwein, München
m.orthwein@skwschwarz.de

Coronavirus und Justiz – wie geht es weiter?

Die Auswirkungen der aktuellen Corona-Krise machen auch vor der deutschen Justiz nicht Halt. Einen Stillstand der Rechtspflege muss das aber nicht zwingend bedeuten. Nachstehend ein Kurzüberblick, welche Maßnahmen der deutsche Gesetzgeber den Prozessbeteiligten bereits jetzt einräumt.

Die Auswirkungen der aktuellen Corona-Krise machen auch vor der deutschen Justiz nicht Halt. Kürzlich wurde etwa bekannt, dass ein Hagener Amtsrichter für seine Verfahren eine Atemschutzpflicht angeordnet hat.[1] Rechtsgrundlage dafür ist die in § 176 GVG niedergelegte sog. „Sitzungspolizei“, wonach dem Vorsitzenden die Pflicht „zur Aufrechterhaltung der Ordnung“ obliegt. Angesichts der bereits in vielen Ländern angeordneten Schulschließungen ist zu erwarten, dass demnächst auch die Gerichte ihren Betrieb zurückfahren müssen. Einen Stillstand der Rechtspflege muss das aber nicht zwingend bedeuten. Nachstehend ein Kurzüberblick, welche Maßnahmen der deutsche Gesetzgeber den Prozessbeteiligten bereits jetzt einräumt.

Bereits seit 2013 existiert die Möglichkeit der sog. Video-Konferenzverhandlung nach § 128a ZPO. Diese ermöglicht den Parteien, aber auch Zeugen und Sachverständigen, sich während der Verhandlung „an einem anderen Ort aufzuhalten“ – etwa zuhause, statt in einem ggf. voll besetzten und risikobehafteten Gerichtssaal. Die Verhandlung kann sowohl auf Antrag der Beteiligten als auch durch das Gericht von Amts wegen (und gegen den Willen der Beteiligten) angeordnet werden. Auch vor Finanz- (§ 91a FGO), Verwaltungs- (§ 102a VwGO), Sozial- (§ 110a SSG) und Strafgerichten[2] gewährt der Gesetzgeber den Einsatz von Videotechnik.

Doch wie erfolgversprechend wäre ein entsprechender, vor dem Hintergrund von Covid-19 gestellter Antrag? Es lässt sich nur schwer ermitteln, inwieweit die Gerichte davon tatsächlich Gebrauch machen. Allerdings wird im Justizportal des Bundes und der Länder eine Liste der teilnehmenden Gerichte und Staatsanwaltschaften zur Verfügung gestellt und ständig aktualisiert.[3] Eine weitere, sogar nach Städten sortierte Übersicht findet sich etwas versteckt auf der Website der Europäischen Kommission.[4] Dort sind ferner ein Handbuch zum grenzüberschreitenden Einsatz[5] sowie eine Übersicht zu den teilnehmenden Gerichten in den jeweiligen Mitgliedstaaten veröffentlicht.[6] Auch die Websites einzelner Oberlandesgerichte informieren zu den bestehenden Möglichkeiten.[7]

Entgegen weit verbreiteter Vorurteile existieren an deutschen Gerichten die entsprechenden Möglichkeiten also durchaus. Auf den Einsatz von Atemschutzmasken kann daher wohl weitestgehend verzichtet werden. Zwar ging es dem Gesetzgeber bei der Einführung der Videokonferenzen eigentlich um weite Anreisen der Prozessbeteiligten.[8] Wäre sie vorauszusehen gewesen, wären aber sicherlich auch Krisen wie internationale Pandemien in die Gesetzesbegründung eingeflossen.

All dies zeigt: Auch im Bereich der Rechtspflege können die Prozessbeteiligten zu einer verzögernden Verbreitung des Corona-Virus beitragen. Ein gänzlicher Stillstand ist indes (noch) nicht erforderlich. Ein Blick in die aufgeführten Listen – aber auch ein Anruf bei Gericht – zeigt schnell, ob auf eine Verhandlung vor Ort nicht zugunsten einer Videoübertragung verzichtet werden kann.

Sandra Sophia Redeker, Berlin
s.redeker@skwschwarz.de
Tobias Voßberg, Berlin
t.vossberg@skwschwarz.de

Oberlandesgericht Köln geht von einem (sehr) weiten Auskunftsanspruch einer betroffenen Person aus

Kurz vor dem 2. Geburtstag der Datenschutz-Grundverordnung („DSGVO“), werden die ersten Urteile von Oberlandesgerichten veröffentlicht.

Dabei war absehbar, dass sich diese ersten Urteile insbesondere mit Artikel 15 DSGVO (Auskunftsrecht der betroffenen Person/Informationsrecht) befassen werden. Praxisrelevant ist die Frage nach der Reichweite eines Auskunftsanspruchs gemäß Artikel 15 DSGVO. Wie umfangreich muss eine erteilte Auskunft sein, um ausreichend und vollständig zu sein? Dabei geht es auch um die Quantität (wie viele personenbezogene Daten?) und die Qualität (welche personenbezogenen Daten?) einer Beauskunftung.

Die Formulierungen von Artikel 15 Abs. 1 und Abs. 3 S. 1 DSGVO deuten eher auf eine große Reichweite hin. Der Wortlaut von Artikel 15 Abs. 4 DSGVO hingegen erlaubt einen differenzierteren Ansatz. Während verschiedene Gerichte zur Reichweite unterschiedliche Ansichten vertreten, ist ein Urteil des Oberlandesgerichts Köln („OLG Köln“) besonders erwähnenswert. Diesem Urteil liegt ein Lebensversicherungsvertrag zugrunde.

1. Das OLG Köln geht von einem sehr weiten Anwendungsbereich von Artikel 15 DSGVO aus

Am 26. Juli 2019 hat das OLG Köln, Az. 20 U 75/18, in einem kürzlich veröffentlichten Urteil entschieden, dass Artikel 15 DSGVO eine große Reichweite hat und der Anwendungsbereich somit sehr weit sei. Eine Auskunft nach Artikel 15 DSGVO könne nicht (einseitig) auf eine Teilmenge der vorhandenen personenbezogenen Daten begrenzt werden.

Die Parteien hatten am 1. November 2000 einen Lebensversicherungsvertrag abgeschlossen. Der Kläger wollte Auskunft gegenüber der Beklagten über alle jemals verarbeiteten und noch immer in den Akten befindlichen personenbezogenen Daten im Zusammenhang mit seinem Lebensversicherungsvertrag.

Die Beklagte argumentierte, dass der Begriff „personenbezogene Daten“ nur Stammdaten umfassen würde (die Beklagte hatte diese dem Kläger bereits zur Verfügung gestellt). Weitere Informationen, insbesondere elektronisch gespeicherte Notizen über Telefongespräche und andere Gespräche mit dem Kläger, wollte die Beklagte nicht beauskunften, da diese Informationen nicht vom Anwendungsbereich eines Auskunftsanspruchs gemäß Artikel 15 DSGVO umfasst seien.

Das OLG Köln gab dem Kläger Recht. Das Gericht wies das Argument der Beklagten zurück, der Begriff „personenbezogene Daten“ sei eng auszulegen. Das OLG Köln begründet sein Urteil damit, dass dieser Begriff nach dem Wortlaut der DSGVO weit auszulegen sei (siehe u.a. Artikel 4 Abs. 1 DSGVO). Durch die Entwicklung der Informationstechnologien mit ihren umfassenden Verarbeitungs- und Verknüpfungsmöglichkeiten gebe es keine belanglosen Daten mehr (das OLG Köln verweist dabei auf das Volkszählungsurteil, der Grundsatzentscheidung des Bundesverfassungsgericht vom 15. Dezember 1983, Az. 1 BvR 209/83). Alle Informationen/Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, müssen als persönliche Daten betrachtet werden.

Das OLG Köln bestätigte, dass auch Gesprächs- oder Telefonnotizen über den Kläger, aufgezeichnete Aussagen des Klägers oder aufgezeichnete Aussagen über den Kläger personenbezogene Daten seien. Die Beklagte müsse dem Kläger auch eine Kopie dieser Daten im Rahmen des Auskunftsanspruchs zur Verfügung stellen.

Zudem dürfe sich die Beklagte nicht auf den Schutz ihrer Geschäftsgeheimnisse berufen. Personenbezogene Daten – die vom Kläger zur Verfügung gestellt oder zumindest vom Kläger angegeben und von der Beklagten zur Kenntnis genommen wurden – können kein Geschäftsgeheimnis der Beklagten darstellen.

2. Warum könnte dies für Sie relevant sein?

Datenschutzrechtlich Verantwortliche sollten inzwischen Prozesse implementiert haben, um Auskunftsansprüche von betroffenen Personen ausreichend beantworten zu können. Etliche betroffene Personen stellen inzwischen solche Auskunftsansprüche, insbesondere im Rahmen einer Auseinandersetzung (in der Praxis ist dies z.B. im Hinblick auf Kündigungsschutzklagen keine Seltenheit).

Es wäre vorteilhaft, die eigenen Prozesse daraufhin zu untersuchen, wie umfangreich eine Beauskunftung erfolgen kann. Ein Verantwortlicher sollte sogar Telefonnotizen und/oder Gesprächsnotizen über die betroffenen Personen berücksichtigen.

Wenn mehrere Gerichte, insbesondere aus höheren Instanzen, der zugrunde liegenden Argumentation des OLG Köln folgen, könnte dieses Urteil in der Zukunft eine enorme Bedeutung erlangen. Dies wird insbesondere dann der Fall sein, wenn eines Tages auch der EuGH diese Meinung teilt.

Dr. Stefan Peintinger, Frankfurt/Main
s.peintinger@skwschwarz.de

Reform EU-Preisverordnung: Neue Informationspflichten im Payment - EU setzt bei Transparenz auf Vergleichsplattformen

Die EU-Preisverordnung über grenzüberschreitende Zahlungen (Verordnung EG/924/2009) wurde überarbeitet. Ab dem 19.4.2020 gelten u.a. durch die neue EU-Preisverordnung (EU 2019/518) erhöhte Transparenzpflichten für Entgelte für die Währungsumrechnung bei elektronischen Überweisungen (Web- bzw. Online- und Mobile Banking) und im Zusammenhang mit kartengebundenen Zahlungsvorgängen (Einsatz einer Zahlkarte am POS und an Geldautomaten).

Die neuen Bestimmungen gelten für Zahlungsvorgänge innerhalb des Europäischen Wirtschaftsraums (EWR), wenn diese in einer EWR-Fremdwährung erfolgen und eine Währungsumrechnung enthalten. Konkret betrifft dies aktuell die Länder Großbritannien (GBP) - das britische Pfund ist trotz des Brexit zum 31.1.2020 während der nun laufenden Übergangszeit nach wie vor erfasst -, Bulgarien (BGN), Dänemark (DKK), Island (ISK), Kroatien (HRK), Norwegen (NOK), Polen (PLN), Rumänien (RON), Schweden (SEK), Liechtenstein (CHF), Tschechien (CZK) und Ungarn (HUF).

Neue Informationspflichten für Währungsumrechnungen

Im Online-Bereich hat der Zahlungsdienstleister vor Auslösung des Zahlungsvorgangs über die geschätzten Währungsumrechnungsentgelte die für die Überweisung gelten sowie den geschätzten Gesamtbetrag der Überweisung zu informieren.

Bei kartengebundenen Zahlungsvorgängen sind Informationspflichten im Hinblick auf Währungsumrechnungsentgelte und den anwendbaren Wechselkurs vor Auslösung des Zahlungsvorgangs zu erfüllen. Die Währungsumrechnungsentgelte müssen als prozentualer Aufschlag auf den letzten verfügbaren Euro-Referenzwechselkurs der EZB ausgedrückt werden. Für die genannten Pflichten gilt als Stichtag der 19.4.2020. Weitere Pflichten – sie betreffen das Versenden elektronischer Mitteilungen zu den Währungsumrechnungen beim Einsatz von Zahlkarten – sind erst ein Jahr später bindend (ab dem 19.4.2021).

EU setzt auf Entwicklung von Vergleichsplattformen

Die Verordnung enthält zudem ausdrücklich die Verpflichtung, die Aufschläge auf einer „elektronischen Plattform“ - also auf Websites oder Apps - zugänglich zu machen. In den Erwägungsgründen ist davon die Rede, dass dies zur Entwicklung von Vergleichsplattformen beitragen solle, um den Verbrauchern den Preisvergleich auf Reisen oder beim Einkauf im Ausland zu erleichtern.

Umsetzung in der Praxis

Die Informationspflichten werden sich z.B. durch Anpassung der Vertragsdokumente und der Websites bzw. Preis- und Leistungsverzeichnisse umsetzen lassen. Technisch aufwändiger wird die Erfüllung der Pflichten an den Terminals. Die Deutsche Kreditwirtschaft (DK), also die Interessenvertretung der kreditwirtschaftlichen Spitzenverbände, hat zudem angekündigt, Hinweise und Einschätzungen zu den neuen gesetzlichen Regelungen der Preisverordnung auf ihrer Website veröffentlichen.

Christoph Krück, München
c.krueck@skwschwarz.de

Ist mein Unternehmen DSGVO konform?

In die Umsetzung der DSGVO haben Unternehmen viel Zeit und Geld investiert. Nachdem die erste Umsetzungshektik verflogen ist, sollten Unternehmen ihren Status quo nun einer kritischen Prüfung unterziehen. Die Aufsichtsbehörden unterstützen eine derartige kritische Selbstbetrachtung.

So hat der Landesbeauftragte für den Datenschutz Niedersachsen den „Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft 2018/19“ veröffentlicht.1 Darin wird nicht nur danach gefragt, wie sich das Unternehmen auf die DSGVO vorbereitet hat. Die Aufsichtsbehörde will auch wissen, wie das Unternehmen sicherstellt, dass alle Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden und das Verzeichnis laufend aktuell gehalten wird. Ebenso wird gefragt, wie die Rechte der Betroffenen sichergestellt werden.

Insgesamt werden in dem Fragebogen ca. 200 Einzelkriterien abgefragt. Dabei kommen auch unangenehmere Themen zur Sprache wie zum Beispiel die ergriffenen Maßnahmen zur Löschung von Daten und der sogenannte technische Datenschutz.

Hier muss das Unternehmen nicht nur nachweisen, dass technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten existieren. Dokumentiert werden muss auch, dass vorher das Verarbeitungsrisiko ermittelt wurde und die getroffenen Maßnahmen diesem Risiko entsprechen. Ebenso muss dargelegt werden, wie festgestellt wird, ob sogenannte Datenschutzfolgenabschätzungen bei bestimmten Verarbeitungen erforderlich sind oder eben nicht. Die Aufsichtsbehörde will wissen, wie die Fälle erkannt werden, die ein hohes Risiko für die Rechte und Freiheiten der Betroffenen darstellen. Die Erfahrung zeigt, dass bei diesen Themen im Unternehmen nicht alles dokumentiert ist. Außerdem werden zahlreiche Fragen zu den Verträgen mit Auftragsdatenverarbeitern gestellt.

Auch das bayerische Landesamt für Datenschutzaufsicht hat bereits mit der Prüfung der Umsetzung der DSGVO bei kleinen und mittelständischen Unternehmen begonnen. Ein entsprechender Fragenkatalog wurde ebenfalls veröffentlicht.2 Welche empfindlichen Zahlungsverpflichtungen bei Nichtbeachtung der DSGVO drohen, ist nachzulesen im kürzlich erschienenen Konzept der Datenschutzaufsichtsbehörden zur Bemessung von Bußgeldern.3

Praxistipp

Prüfen Sie die Umsetzung der DSGVO in Ihrem Unternehmen anhand der veröffentlichten Fragenkataloge. Gerne unterstützen wir Sie mit der fachkundigen Analyse der vorhandenen Abläufe und Dokumentationen.

Dr. Oliver M. Bühr, Frankfurt/Main
o.buehr@skwschwarz.de

Datenschutz mag keine Cookies

Gerade Liebhaber und Freunde von Süßwaren beschäftigen sich häufig mit dem Thema Cookies. Dieser Beitrag dreht sich allerdings (leider) nicht um leckere Kekse, sondern betrifft die kleinen Textdateien mit Informationen, die bei dem Besuch einer Webseite über den Browser auf dem Endgerät des Nutzers gespeichert werden können.

Der Europäische Gerichtshof hat sich in zwei aktuellen Urteilen zu datenschutzrechtlichen Fragen des Einsatzes von Cookies und Plugins geäußert.

Ausgangspunkt der EuGH-Entscheidung vom 29.07.20191 war ein Verfahren der Verbraucherzentrale NRW gegen den deutschen Online-Händler „Fashion ID“. Die Verbraucherzentrale hatte beanstandet, dass „Fashion ID“ auf der eigenen Webseite den Facebook-Like-Button eingebunden hatte, ohne dass die Benutzer der Webseite in die Datenübermittlung zu Facebook einwilligen mussten oder jedenfalls darüber aufgeklärt wurden. Der EuGH musste vor diesem Hintergrund entscheiden, ob der Online-Händler für die Datenübermittlung und möglicherweise die Datenverarbeitung durch Facebook (mit-)verantwortlich ist.

Beim Facebook-Like-Button bindet der Betreiber der Webseite einen kurzen Code in seine Webseite ein, der eine Anwendung auf Servern von Facebook startet. Dabei kann Facebook auch dann Daten vom Besucher der Webseite erheben, wenn dieser nicht auf den Like-Button klickt (IP-Adresse, Daten über das genutzte Gerät). Das Verfahren war noch nach dem Recht der alten EU-Datenschutzrichtlinie von 1995 (RL 95/46/EG) zu entscheiden; die Entscheidung ist aber auf die Rechtslage nach der DSGVO übertragbar.

Der EuGH hat entschieden, dass keine Mitverantwortung des Seitenbetreibers besteht, wenn er auf die tatsächliche Verarbeitung durch einen anderen Verantwortlichen keinen Einfluss hat, also die Zwecke und Mittel der Verarbeitung nicht bestimmt. Im konkreten Fall heißt das, dass der Online-Händler nicht für alle Datenverarbeitungen durch Facebook mitverantwortlich ist. Allerdings ist der EuGH der Ansicht, dass der Händler durch die Einbindung und Konfiguration des Plug-ins auf seiner Seite die Datenverarbeitung beeinflusst und daher die Mittel der Verarbeitung mit Facebook gemeinsam bestimmt hat. Hinsichtlich der Zwecke der Verarbeitung geht der EuGH davon aus, dass die Einbindung des Plug-ins der besseren Sichtbarkeit der Angebote des Händlers auf Facebook dient und daher der Händler und Facebook auch gemeinsam jedenfalls einen Zweck (Werbung) definiert haben.

Wenn schon die bloße Ermöglichung der Datenerhebung durch einen anderen Verantwortlichen zu einer gemeinsamen Verantwortung führt, läge eine solche wohl bei jeder Einbindung von Drittinhalten wie z. B. Videos, Bilder, Wetterberichten, Börsenkursen, etc. vor. Sofern die Datenverarbeitung auf ein berechtigtes Interesse gestützt werden soll, muss ein solches berechtigtes Interesse bei jedem der gemeinsam Verantwortlichen vorliegen. Wird die Verarbeitung auf eine Einwilligung gestützt, muss der Betreiber diese nur zu den Vorgängen einholen, für die er Verantwortlicher ist, also tatsächlich über die Zwecke und Mittel entscheidet.

Neuigkeiten für die konkrete Ausgestaltung einer Cookie-Einwilligung ergeben sich aus der Entscheidung des EuGH vom 1. Oktober 20192. Hiernach kann der Betreiber einer Website eine Einwilligung in das Setzen von Cookies für Werbezwecke nicht durch ein vorangekreuztes Häkchen einholen. Vielmehr müsse der Nutzer aktiv ein Häkchen setzen, um seine Einwilligung zu erteilen. Die Entscheidung des EuGH gilt unabhängig davon, ob die in dem Cookie gespeicherten Daten personenbezogene Daten darstellen oder nicht. Weitere Voraussetzung für eine wirksame Einwilligung ist nach dem Urteil, dass der Nutzer über die Funktionsdauer des Cookies und mögliche Zugriffsrechte Dritter auf den Cookie informiert wurde.

Leider erhöhen sich die Haftungsrisiken durch die dargestellten Entscheidungen beim Einsatz von Cookies erheblich. Wir raten daher dazu, sich erst einmal einen Überblick über den Umfang der eingesetzten Cookies auf der eigenen Webseite zu verschaffen. Sofern externe Inhalte wie Social-Media-Plugins, Kartendienste, Videos, Bilder, Webschriftarten etc. in Ihrer eigenen Webseite eingebunden bleiben sollen, sollten diese jedenfalls erst nach einer aktiven Handlung der Besucher nachgeladen werden (z. B. durch Einbettung von Vorschaubildern, die die aktiven Inhalte erst nach einem Klick laden). In jedem Fall sollte die Datenschutzerklärung geprüft und um Hinweise auf die Speicherdauer von Cookies und die Klarstellung von Dritten, die Zugriff auf die Cookies haben, ergänzt werden.

Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de
Hannah Mugler, Berlin
h.mugler@skwschwarz.de

Generalanwalt Henrik Saugmandsgaard Øe stellt Drittlandstransfers in Frage

Am 19. Dezember 2019 hat der Generalanwalt des Henrik Saugmandsgaard Øe seine Schlussanträge im Verfahren „Data Protection Commissioner / Facebook Ireland und Maximilian Schrems“ (C-311/18; sog. „Schrems II“) veröffentlicht. Unternehmen, die personenbezogene Daten in Drittländer übermitteln, sollten diesem Verfahren besondere Aufmerksamkeit widmen. Eine Aufsichtsbehörde könnte in Zukunft internationale Datenübermittlungen untersagen, obwohl EU Standardvertragsklauseln wirksam vereinbart (und eingehalten) wurden. Dies könnte auch für andere Garantien im Rahmen internationaler Datenübermittlungen gelten.

Diese Schlussanträge sind von zahlreichen prozessualen Fragen bzw. Weichenstellungen geprägt. Aus praktischer Sicht ist zunächst Folgendes relevant:

Der Generalanwalt empfiehlt dem EuGH, den Beschluss vom 5. Februar 2010 (2010/87/EU) zur Anwendbarkeit der sog. EU Standardvertragsklauseln weiterhin für rechtmäßig zu erachten. Der Generalanwalt sieht – im vorliegenden Verfahren – keinen Anlass diesen Beschluss für ungültig zu erklären.

Sollte der EuGH dem Generalanwalt folgen, können Unternehmen weiterhin grundsätzlich EU Standardvertragsklauseln verwenden, um internationale Datenübermittlungen zu rechtfertigen. Dieser Grundsatz könnte sich allerdings in eine Ausnahme verkehren. Wenn sich der EuGH der Ansicht des Generalanwalts anschließt, könnte ein Systembruch bei internationalen Datenübermittlungen folgen. Unternehmen könnten sich nicht mehr auf Garantien im Sinne der Datenschutz-Grundverordnung („DSGVO“) verlassen, wenn sie personenbezogene Daten in Drittländer übermitteln. Der Generalanwalt vertritt (wohl) die Ansicht, dass Aufsichtsbehörden im Einzelfall die Anordnung erlassen können, um Datenübermittlungen auszusetzen. Eine Aufsichtsbehörde könnte in der Zukunft

also internationale Datenübermittlungen untersagen, obwohl EU Standardvertragsklauseln wirksam vereinbart (und eingehalten) wurden.

I. Vorgeschichte und Hintergrund

Dieses Verfahren hat eine längere Vorgeschichte. Ausgangspunkt ist eine Beschwerde, die Herr Schrems bei der irischen Datenschutzaufsichtsbehörde eingereicht hat.

Herr Schrems hat im Kern die Rechtmäßigkeit der Übermittlung von personenbezogenen Daten durch die Facebook Ireland Ltd. an die Facebook, Inc. (mit Sitz in Kalifornien, USA) in Frage gestellt („Schrems I"). Aus Sicht von Herrn Schrems war in den USA kein angemessenes Datenschutzniveau durch das (inzwischen ungültige) Safe Harbor Abkommen gegeben. Unter anderem würden U.S. Behörden auf personenbezogene Daten von betroffenen Personen zugreifen, ohne dass diese Personen ausreichende Rechtsmittel ergreifen könnten. Die Übermittlung von personenbezogenen Daten auf der Grundlage des Safe Harbor Abkommens sei insbesondere daher unzulässig. Diese Ausgangsbeschwerde führte dazu, dass der EuGH die Entscheidung der EU-Kommission über das (damalige) Safe Harbor Abkommen vom 26. Juli 2000 für ungültig erklärt hat. Durch die Schrems I-Entscheidung wurden die Verhandlungen über das (aktuell gültige) Privacy Shield beschleunigt.

II. (Noch) Keine Auswirkung der Schrems I-Entscheidung auf EU Standardvertragsklauseln

Der Beschluss 2010/87/EU zur Anwendbarkeit der EU Standardvertragsklauseln war durch die Schrems I-Entscheidung nicht betroffen. Dieses Rechtsinstitut konnte weiterhin für internationale Datenübermittlungen genutzt werden. Die EU Kommission hatte mit Beschluss 2010/87/EU bestimmte Standardvertragsklauseln für internationale Datenübermittlungen formuliert. Wenn Parteien diese Klauseln vereinbaren, sind sie zur Einhaltung bestimmter Schutzanforderungen bezüglich personenbezogener Daten verpflichtet. Diese Verpflichtungen können zur Rechtfertigung einer internationalen Datenübermittlung herangezogen werden, z.B. um personenbezogene Daten von einem EU Unternehmen an ein U.S. Unternehmen zu übermitteln. Die EU Standardvertragsklauseln sind damit eine Möglichkeit, internationale Datenübermittlungen zu rechtfertigen (vgl. Art. 46 Abs. 2 lit. c) DSGVO).

III. Kernfrage im Schrems II-Verfahren

Die Facebook Ireland Ltd. verwendet EU Standardvertragsklauseln, abgeschlossen mit der Facebook, Inc., als Rechtfertigung für die entsprechenden internationalen Datenübermittlungen. Nachdem Facebook Ireland Ltd. dies Herrn Schrems mitgeteilt hatte, hat er seine Beschwerde umformuliert.

Die Kernfrage des vorlegenden Gerichts im Schrems II-Verfahrens ist, ob der Beschluss 2010/87/EU mit bestimmten europäischen Grundrechten vereinbar ist (vgl. Frage 11 in Rdnr. 76 der Schlussanträge). Herr Schrems stellt diese Gültigkeit insbesondere aufgrund der beschränkten Bindungswirkung der EU Standardvertragsklauseln in Frage. Diese binden nur die Parteien, zwischen denen eine entsprechende Vereinbarung getroffen worden ist. Wenn daher zwei private Unternehmen eine entspreche Vereinbarung abschließen würden, wären staatliche Behörden nicht verpflichtet, ein bestimmtes Schutzniveau zu gewährleisten. Für Datenübermittlungen aus der EU in die USA bedeutet dies, dass auch durch den Abschluss der EU Standardvertragsklauseln kein ausreichendes Schutzniveau gegeben wäre. Gegen ein ausreichendes Schutzniveau in den USA sprächen insbesondere diverse staatliche Überwachungsmaßnahmen und mangelnder Rechtsschutz für betroffene Personen.

IV. Kein Anlass für den EuGH, den Beschluss 2010/87/EU für ungültig zu erklären

Der Generalanwalt sieht im Ergebnis keinen Anlass für den EuGH, den Beschluss 2010/87/EU – im vorliegenden Fall – für ungültig zu erklären. Dieser Beschluss sei mit verschiedenen Grundrechten der Europäischen Union vereinbar.

Zum einen reiche der Umstand der mangelnden Bindungswirkung staatlicher Stellen nicht aus, um einen Grundrechtsverstoß anzunehmen. Staatliche Behörden seien nicht gehindert, dem Datenempfänger („Importeur") Pflichten aufzuerlegen. Dabei ist es möglich, dass der Importeur, bei Beachtung dieser Pflichten, wiederum gegen seine Verpflichtungen gegenüber dem Datenübermittler („Exporteur") verstößt. Dies allein rechtfertige nicht die Ungültigkeit des Beschlusses.

Zum andere sei zu prüfen, ob ausreichend wirksame Regelungen gegeben sind, um auf einen solchen Fall reagieren zu können (ohne zugleich das Rechtsinstitut der EU Standardvertragsklauseln in der aktuellen Fassung vollständig für ungültig zu erklären). Datenschutzaufsichtsbehörden haben nach Art. 58 Abs. 2 DSGVO verschiedene Abhilfebefugnisse. Sie können unter anderem nach Art. 58 Abs. 2 lit. f) DSGVO die Datenübermittlung des Exporteurs an den Importeur vorübergehend oder endgültig beschränken. Diese Abhilfebefugnis könne auch angewendet werden, wenn sich für den Importeur aufgrund einer gesetzlichen oder behördlichen Anordnung ein Konflikt mit der Einhaltung der vereinbarten EU Standardvertragsklauseln ergibt.

Dadurch können die Grundrechte betroffener Personen im Einzelfall gewahrt werden, ohne den Beschluss 2010/87/EU für ungültig zu erklären.

V. Fazit

Aus Sicht des Generalanwalts sollte der Beschluss 2010/87/EU weiterhin gültig bleiben. Unternehmen könnten daher auch künftig EU Standardvertragsklauseln anwenden. Im konkreten Einzelfall könne eine Datenschutzaufsichtsbehörde, gegebenenfalls nach Abstimmung im Rahmen des Europäischen Datenschutzausschusses, Maßnahmen treffen, um bestimmte Datenübermittlungen in ein Drittland zu unterbinden. Der Generalanwalt stellt die grundsätzliche Systematik der EU Standardvertragsklauseln als eine Rechtfertigungsmöglichkeit für internationale Datenübermittlungen nicht in Frage.

Die Richter am EuGH sind an die Schlussanträge eines Generalanwalts nicht gebunden. Sie folgen den Schlussanträgen jedoch regelmäßig. Es bleibt – insbesondere vor dem Hintergrund verschiedener prozessualer Fragen – abzuwarten, wie die Richter die Vorlagefragen beantworten werden.

Unabhängig von dem vorliegenden Vorabentscheidungsverfahren wird eine andere anhängige Entscheidung möglicherweise zu einer Neujustierung der internationalen Datenübermittlungen in die USA führen. Verfahrensgegenstand in Sachen La Quadrature du Net u.a./Kommission (T-738/16) ist die Frage, ob der Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016, zur Anwendbarkeit des EU-US Privacy Shields, gegen bestimmte Grundrechte verstößt oder nicht. Auf dieses Verfahren nimmt der Generalanwalt mehrfach Bezug.

EU Standardvertragsklauseln sind verhältnismäßig einfach in der Praxis einzusetzen. Ein Faktor, der auch beim anstehenden Brexit aus datenschutzrechtlicher Sicht relevant werden wird.

VI. Ausblick

Es ist Vorsicht geboten. Wird die Stellungnahme (insbesondere in Rdnr. 121 ff) des Generalanwalts weitergedacht – und vom EuGH in den maßgeblichen Punkten übernommen – steht die bisherige Systematik der Drittlandstransfers in Frage.

Dem Generalanwalt folgend wäre der Beschluss 2010/87/EU weiterhin gültig. Aufsichtsbehörden könnten im Einzelfall entsprechende Datenübermittlungen untersagen, wenn sie möglicherweise Defizite in einem Drittland erkennen. Dies könnte dazu führen, dass EU Standardvertragsklauseln für bestimmte Drittländer (oder vielleicht für Teile davon) nicht mehr angewendet werden können, obwohl der Beschluss 2010/87/EU weiterhin gültig ist.

Dies stellt die Systematik der Drittlandstransfers nach Art. 44 ff DSGVO in Frage. Ein Unternehmen könnte sich nicht mehr darauf verlassen, dass es mit dem Abschluss (und der Einhaltung) von EU Standardvertragsklauseln die entsprechenden datenschutzrechtlichen Anforderungen eingehalten hat (vgl. Art. 46 Abs. 2 lit. c) DSGVO). Die Datenübermittlung könnte dennoch aufgrund von Faktoren, die im Drittland begründet sind, untersagt werden. Demzufolge wären keine Garantien zwischen privaten Unternehmen mehr geeignet, um für die Unternehmen Rechtssicherheit zu schaffen. Strukturelle Defizite in einem Drittland würden z.B. auch Binding Corporate Rules in Frage stellen. Sinn und Zweck der Garantien für Drittlandstransfers würden wegfallen.

Dadurch könnte eine Aufsichtsbehörde Befugnisse erlangen, die ihr aufgrund der Gewaltenteilung nicht zustehen. Sie könnte de facto die Anwendbarkeit eines gültigen Rechtsaktes (Beschluss 2010/87/EU) beseitigen, indem sie Datenübermittlungen auf dieser Grundlage konsequent untersagt.

Diese Konsequenz wäre schon allein Folge der Selbstbindung der Verwaltung und des allgemeinen Gleichheitsgrundsatzes.

Die Stellungnahme des Generalanwalts wäre ein Pyrrhussieg für Unternehmen, die EU Standardvertragsklauseln einsetzen und die entsprechenden DSGVO-Anforderungen damit einhalten wollen.

Dr. Stefan Peintinger, Frankfurt/Main
s.peintinger@skwschwarz.de