Luther.

Newsletter IP/IT

4. Ausgabe 2020

Inhalt

EuGH erklärt EU-US Privacy Shield für unwirksam – Datentransfers in Staaten außerhalb der EU auf dem Prüfstand

Max Schrems hat wieder zugeschlagen. Nachdem auf sein Betreiben schon 2015 das Safe Harbor Abkommen für Datentransfers in die USA gekippt wurde, stand nun das EU-US Privacy Shield auf der Agenda: Der Europäische Gerichtshof („EuGH“) hat in seinem Urteil entschieden, dass das EU-US Privacy Shield ungültig sei. Das alternative Mittel der Standardvertragsklauseln bleibe jedoch wirksam - wenn auch mit Zweifeln behaftet.

EuGH, Urteil vom 16. Juli 2020, Az. C-311/18

Hintergrund: Drittlandtransfer und geeignete Garantien

Nach der seit Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO) dürfen personenbezogene Daten nur dann in Länder außerhalb der EU bzw. des Europäischen Wirtschaftsraums (sog. Drittländer) übermittelt werden, wenn der Verantwortliche für den Datentransfer sog. geeignete Garantien vorsieht. In Betracht kamen bisher:

- **Standarddatenschutzklauseln (vormals Standardvertragsklauseln)**:
  Bei den Standarddatenschutzklauseln handelt sich um von der Europäischen Kommission vorformulierte Vertragsklauseln, die in der Regel zwischen dem Verantwortlichen in der EU (Datenexporteur) und dem Datenempfänger im Drittland (Datenimporteur) vereinbart werden. Sie verpflichten den Datenempfänger auf die Einhaltung des Datenschutzes, um so ein angemessenes Datenschutzniveau zu gewährleisten.

- **EU-US-Privacy Shield (seit dem 16.07.2020 nicht mehr anwendbar!)**:
  Im Falle eines internationalen Datentransfers in die USA kam neben den Standardvertragsklauseln auch das sog. EU-US-Privacy Shield als geeignete Garantie in Betracht. Beim Privacy Shield handelte es sich um einen Beschluss der Kommission. Der Nachfolger des Safe Harbor Abkommens, das bereits 2015 ebenfalls auf Initiative von Max Schrems gekippt wurde, stand unter Datenschützern aus den gleichen Gründen massiv in der Kritik.

Vorlagefragen: Schrems vs. Facebook

Der irische oberste Gerichtshof hat dem EuGH eine Reihe von Fragen vorgelegt, mit denen er im Wesentlichen die Wirksamkeit der Standarddatenschutzklauseln in Frage stellte. Hintergrund ist ein Rechtsstreit zwischen dem irischen Datenschutzbeauftragten sowie Facebook Ireland Ltd. und Maximilian Schrems, betreffend der Übermittlung von personenbezogenen Daten an die US-amerikanische Muttergesellschaft von Facebook. Ausgangspunkt war die Feststellung der gezielten und massenhaften Ermittlungsbefugnisse durch die amerikanischen Regierungsbehörden, insbesondere auf Basis des sog. CLOUD Acts (Clarifying Lawful Overseas Use of Data Act), unter gleichzeitigem Mangel von Rechtsbehelfen für EU-Bürger. Angesichts dieser Feststellungen könnte nach Ansicht des irischen Gerichts eine Verletzung der Europäischen Grundrechte (Recht auf Achtung des Privatlebens, Schutz personenbezogener Daten, Recht auf einen wirksamen Rechtsbehelf) durch die Übertragung von Daten auf Grundlage der Standarddatenschutzklauseln in die USA in Betracht kommen. Die Standarddatenschutzklauseln gelten nur zwischen dem Datenexporteur und dem Datenimporteur und entfalten gegenüber nationalen Behörden eines Drittlandes keine Bindungswirkung. Dies könnte in Verbindung mit den weitreichenden Befugnissen der amerikanischen Behörden dazu führen, dass die Standarddatenschutzklauseln keine geeigneten Garantien für den Schutz der personenbezogenen Daten bieten können. Konsequenz hieraus wäre aus Sicht des irischen Gerichtshof letztlich die Unwirksamkeit der Standarddatenschutzklauseln.

Wirksamkeit der Standardvertragsklauseln

Anders als der irische oberste Gerichtshof sieht der EuGH allerdings keinen Anlass von der Unwirksamkeit der Standardvertragsklauseln auszugehen. Dabei stellt er, wie bereits der Generalanwalt in seinen Schlussanträgen, fest, dass die Wirksamkeit der Standarddatenschutzklauseln von dem Datenschutzniveau des Drittlands unabhängig sei. Die Klauseln sollen nämlich gerade eventuelle Unzulänglichkeiten im Vergleich mit dem europäischen Datenschutzniveau ausgleichen, indem sie geeignete Garantien für den Schutz personenbezogener Daten bieten.

Die Tatsache, dass die Sicherheitsbehörden in den USA weitreichenden Zugriff auf personenbezogene Daten haben, könne die Wirksamkeit der Standarddatenschutzklauseln daher nicht generell in Frage stellen. Vor allem da die Klauseln der EU-Kommission die Möglichkeit vorsehen, einzelne Datenübertragungen auszusetzen oder zu verbieten („Not-Stopp-Regelung“). Demnach könne der Verantwortliche oder – falls dieser nicht handelt – die jeweilige Datenschutzaufsichtsbehörde die Datenübermittlung aussetzen oder verbieten, wenn ein Verstoß gegen die Standardvertragsklauseln vorliegt. Das wäre ebenfalls der Fall, wenn sich ergibt, dass die Rechtsordnung des Drittlandes der Anwendung der Standarddatenschutzklauseln widerspricht und kein angemessener Schutz für die übermittelten Daten mehr besteht.

Wichtig ist, dass die Vertragspartner im EU-Ausland darauf hinweisen müssen, wenn sie die Vorgaben der Standarddatenschutzklauseln, zum Beispiel aufgrund lokaler gesetzlicher Vorgaben, nicht einhalten können. Europäische Unternehmen tun daher gut daran, ausdrücklich eine Bestätigung ihrer Vertragspartner zu verlangen, dass die Regelungen der Standarddatenschutzklauseln eingehalten werden können.

Wirksamkeit des Privacy Shield

Obgleich es hauptsächlich um die Standarddatenschutzklauseln ging, hat der EuGH sich auch zur Wirksamkeit des EU-US Privacy Shields geäußert. Erwartungsgemäß wurde dies nun für ungültig erklärt. Grundlage hierfür sind unter anderem die durch Edward Snowden aufgedeckten Überwachungsmaßnahmen der US-Behörden. Sie begründen Zweifel an dem Bestehen eines der DSGVO im Wesentlichen vergleichbaren Schutzniveaus für personenbezogene Daten. Gerade dies war aber Grundlage des Beschlusses zum Privacy Shield. Die Rechtsgrundlagen für die Überwachungsmaßnahmen im US-amerikanischen Recht sind nach Ansicht des EuGH nicht klar und präzise genug formuliert, um Rechtssicherheit zu bieten und um Missbrauch vorzubeugen. Insbesondere ist problematisch, dass die Maßnahmen der US-Behörden weder im Vorfeld noch im Nachhinein von einer unabhängigen Stelle überprüft werden. Eine Benachrichtigung der betroffenen

Person erfolgt nicht und ein wirksamer Rechtsbehelf gegen die Maßnahmen ist nicht vorgesehen. Auch die im Privacy Shield vorgesehene Einrichtung einer Ombudsperson ändert diese Einschätzung nicht – dieser mangele es an ausreichend wirksamen Befugnissen.

Der Druck steigt - Max Schrems, noyb und Datenschutzaufsichtsbehörden gehen an allen Fronten verstärkt gegen Unternehmen vor

Unmittelbar nach dem EuGH-Urteil hat die – von Max Schrems mitgegründete – Datenschutzorganisation noyb („none of your business“) gegen 101 europäische Unternehmen Beschwerden wegen des Datentransfers in die USA unter dem nun unwirksamen Privacy Shield eingereicht. Betroffen sind in Deutschland zum Beispiel die Betreiber reichweitenstarker Webseiten wie chefkoch.de, express.de oder wiwo.de. Weil diese Unternehmen personenbezogene Daten an Google oder Facebook und damit in ein Drittland übermitteln, fordern die Aktivist/innen ein Einschreiten der Datenschutzbehörden und die Verhängung von Bußgeldern. Ihrer Ansicht nach gibt es für den Datentransfer keine Grundlage mehr, nachdem der EuGH die Unwirksamkeit des *Privacy Shields* und ggf. auch der Standarddatenschutzklauseln bei US-Unternehmen festgestellt habe. Daneben will noyb aber auch die US-Unternehmen selbst in die Pflicht nehmen: Sie hätten ihre Partner in der EU informieren müssen, wenn sie die Standarddatenschutzklauseln nicht einhalten können und seien dementsprechend für Schäden haftbar.

Tracking auf dem Prüfstand

Ärger droht deutschen Medienunternehmen darüber hinaus aufgrund des Einsatzes von Tracking-Technologien, insbesondere durch Cookies, auch von Seiten der Datenschutzaufsichtsbehörden. Nach dem Urteil des BGH vom Mai 2020 ist der Einsatz von Cookies nur noch mit Einwilligung möglich – von wenigen, eng umfassten Ausnahmen abgesehen. Die Einwilligung muss informiert und freiwillig erfolgen. Die deutschen Datenschutzaufsichtsbehörden hegen schon länger Zweifel an der datenschutzkonformen Ausgestaltung dieser Anwendungen. Daher haben sich zehn der insgesamt 16 Landesdatenschutzbehörden dazu entschieden, Medienunternehmen, die in der Regel einen Großteil ihrer Online-Tätigkeiten über Werbung finanzieren, auf die Einhaltung der gesetzlichen und gerichtlichen Vorgaben hin zu überprüfen. Von besonderem Interesse ist dabei das sogenannte Kopplungsverbot. Demnach kann eine Einwilligung

in die Verarbeitung personenbezogener Daten unwirksam sein, wenn sie für die Dienstleistung selbst nicht erforderlich ist, der Anbieter ohne Einwilligung aber den Zugriff verweigert. Ob dieses Verbot umgangen werden kann, indem Nutzer/innen vor die Wahl gestellt werden, entweder die Einwilligung zu erteilen oder aber für das Angebot zu bezahlen, wie es einige journalistische Online-Angebote handhaben, ist noch ungeklärt. Auch die Rechtsprechung hierzu ist nicht einheitlich, traditionell vertreten aber die deutschen Datenschutzaufsichtsbehörden eher strenge und damit ablehnende Positionen.

Verlautbarungen der Aufsichtsbehörden

Angesichts dieser verstärkten Prüftätigkeit und der damit verbundenen zunehmenden Risiken ist es misslich, dass konkrete Hilfestellungen und Äußerungen der deutschen Datenschutzaufsichtsbehörden zu diesen Themen weiterhin eher spärlich zu finden sind. So hat hinsichtlich des Datentransfers außerhalb der EU/des EWR inzwischen immerhin der Landesdatenschutzbeauftragte Baden Württembergs (LfDI BW) eine Handreichung mit Hinweisen veröffentlicht. Denkbare Ausnahmen vom Übermittlungsverbot seien danach beispielsweise ausreichend verschlüsselte Übertragungen, wenn nur der Datenexporteur den Schlüssel hat oder anonymisierte/pseudonymisierte Daten, wenn nur der Datenexporteur eine Zuordnung vornehmen kann. Darüber hinaus schlägt der LfDI BW eine Anpassung der Standardvertragsklauseln vor. Solche Änderungen sind jedoch nur in wenigen Fällen zulässig. So dürfen die Klauseln selbst nicht modifiziert oder durch Zusatzvereinbarungen aufgeweicht, sondern nur zusätzliche oder strengere Vorgaben gemacht werden. Es ist daher fraglich, ob tatsächlich alle Vorschläge des LfDI BW umsetzbar sind. Der LfDI BW zeigt dabei zwar Verständnis für die vom Urteil betroffenen Unternehmen und will sich daher am Grundsatz der Verhältnismäßigkeit orientieren. Dabei darf man sich aber keinen Illusionen hingeben. Ausdrücklich kündigt die Behörde an, mit dem jüngsten Urteil unvereinbare Datentransfers zu unterbinden, wenn das Unternehmen nicht überzeugend darlegen kann, warum der aktuelle Datenimporteur für sie kurz- oder mittelfristig unersetzlich ist. Unternehmen sollten sich daher entsprechend vorbereiten und nachvollziehbar vermitteln, warum sie auf bestimmte Dienstleister außerhalb der EU/des EWR nicht verzichten können. Mag dies für tief verwurzelte, viel genutzte oder „alternativlose“ Anwendungen wie Computer-Betriebssysteme, Office-Programme oder bestimmte Cloud-Services unter Umständen noch gelingen, dürfte dies im Bereich der Cookies, des Trackings und des Online-Marketings ungleich schwerer zu begründen sein.

Handlungsempfehlung

Datenübermittlungen in die USA, die noch auf Grundlage des Privacy Shield erfolgen, müssen grundsätzlich sofort eingestellt werden. Der EuGH hat insoweit keine „Schonfrist“ eingeräumt. Aber auch die Standardvertragsklauseln dürften in ihrer Standardversion anhand des vom EuGH präzisierten, strengen Prüfungsmaßstabs in der Regel nicht ausreichend sein.

Unternehmen sollten daher ihre Datenverarbeitungen und Prozesse daraufhin überprüfen, ob eine Übermittlung personenbezogener Daten in die USA oder andere möglicherweise unsichere Drittstaaten (z. B. Großbritannien nach dem Brexit, China, Russland, Mittlerer Osten, etc.) stattfindet und auf welcher Rechtsgrundlage eine solche Übermittlung erfolgt. Im Anschluss daran sollte eine Risikobewertung erfolgen, die sowohl den Verarbeitungsprozess an sich, als auch die Art der verarbeiteten Daten sowie die vertraglichen Regelungen umfassen kann.

Checkliste

Die nachfolgende Checkliste bietet hierfür einen ersten Anhaltspunkt, wie bestimmte Datenverarbeitungen einzuordnen sein können. Mithilfe der Risikomatrix kann auf Grundlage der Ergebnisse der Checkliste das Risikoniveau bestimmt werden. Aus diesem Risiko-Assessment können dann umzusetzende Maßnahmen abgeleitet werden. Dies können neben der Ergreifung zusätzlicher vertraglicher (z. B. Ergänzung Standardvertragsklauseln) oder technisch-organisatorischer Maßnahmen (z. B. stärkere Verschlüsselung) auch alternative Übermittlungsgrundlagen wie Einwilligungen nach Art. 49 DSGVO (bspw. für Cookies) sein. Durch diese ersten Schritte kann gegenüber den Datenschutzaufsichtsbehörden dokumentiert werden, dass man die Folgen des EuGH-Urteils zumindest erkannt und erste Maßnahmen eingeleitet hat.

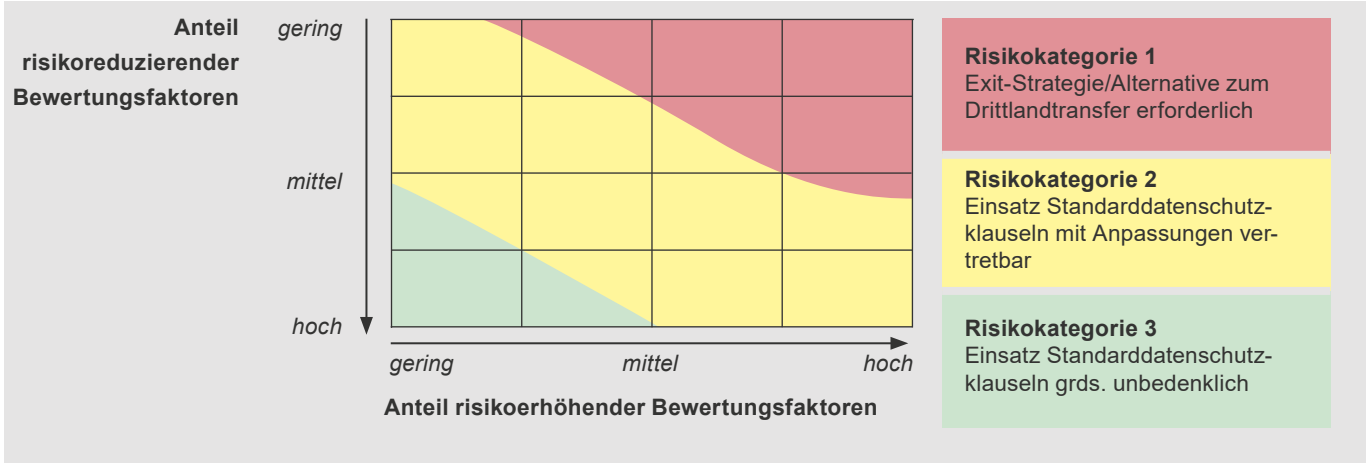
Self Assessment Checkliste - Risikobewertung Internationaler Datentransfer nach Schrems II

Risikofaktoren (Beispiele)

Risikoerhöhende Faktoren / Maßnahmen	**Risikofaktor „Zielland“**	**Auswirkung Risiko***
	Kritisches Drittland wie bspw. USA, China, Russland, Mittlerer Osten (ggf. zukünftig auch UK)	
	Besondere Risiken für staatliche Zugriffe aufgrund nationaler Sicherheitsgesetze (z. B. FISA 702, EO 12333)	
	Eingeschränkte Rechtsschutzmöglichkeiten für EU-Betroffene	
	Risikofaktor „Dienstleister/Datenimporteur“	
	Telekommunikationsdiensteanbieter	
	Anbieter elektronischer Kommunikationsleistungen (E-Mail, Video, Messenger, etc.)	
	Cloud-Provider	
	Dienstleister/Datenimporteur war in der Vergangenheit bereits Adressat staatlicher Zugriffsmaßnahmen	
	Analyse-/Trackingdienstleister (z. B. Webseiten-Tracking)	
	Anbieter nachrangiger IT-Services (Wartung/Pflege, Support, etc.)	
	Gruppeninterner Datentransfer / Dienstleister	
	Risikofaktor „Art der Daten“	
	Besondere Kategorien personenbezogener Daten (Gesundheit, Religion, etc.)	
	Sensible Bank- und Finanzdaten	
	HR-Daten	
	Bestandsdaten von Arbeitnehmern oder Endkunden (Kontaktdaten, E-Mail-Adresse, User-Name)	
	Nutzungsdaten (LogIn-Daten, Webtracking-Daten, ohne Standortlokalisation)	
Risikoreduzierende Faktoren / Maßnahmen	Standarddatenschutzklauseln mit erweiterten Verpflichtungen/Sicherungsmaßnahmen, insb. transparente Information und ggf. Genehmigung durch Datenexporteur bei behördlichen Zugriffen	
	Erweiterung Betroffenenrechte / Ausgleich Rechtsschutzdefizite	
	Compliance-Bestätigung Dienstleister	
	Zertifizierungen des Dienstleisters zu Datenschutz/Datensicherheit	
	Einbindung Betroffener - Einwilligungslösung	
	Binding Corporate Rules (BCR)	
	Verhaltensregeln/Code of Conducts	
	Beschränkung auf pseudonyme Daten / Tokenization	
	Datenlokalisation EU/EWR (Container-Lösung, Treuhänder-Modell)	
	Verschlüsselungsmaßnahmen	
	Sonstige technische oder organisatorische Sicherheitsvorkehrungen zur Einschränkung von Zugriffen	

*** Legende Risikoauswirkung**	*- risikoerhöhend -*	*- risikoneutral - Risiko vorhanden, aber nicht erhöht*	*- risikoreduzierend -*

Die Einstufung der Risikoauswirkungen erfolgt auf Grundlage von Best Practices und ohne Übernahme einer Haftung.



Bundesgerichtshof: Cookies (fast) nur noch mit Einwilligung möglich – Webseitenbetreiber müssen beim Einsatz von Cookies eine Einwilligung einholen

Die Entscheidung (BGH, Urteil vom 28. Mai 2020, Az. I ZR 7/16) betrifft u. a. auch Cookies, die der bloßen Analyse der Zugriffs- oder Klickzahlen dienen, sofern diese Nutzungsprofile der Website-Besucher erstellen. Ausnahmefälle, in denen auf die Einholung einer Einwilligung verzichtet werden kann, dürften damit nur noch eng begrenzt sein. Cookie-Banner und Consent-Tools bleiben damit weiterhin Pflicht für eine ordnungsgemäße Umsetzung der rechtlichen Vorgaben.

BGH, Urteil vom 28. Mai 2020, Az. I ZR 7/16

Verbraucherverbände treiben die Rechtsentwicklung voran

Das Verfahren fand seinen Anfang in einem Streit des Bundesverbands der Verbraucherzentralen und Verbraucherverbände (vzbz) mit dem Gewinnspielanbieter Planet49. Im Fokus stand dabei ursprünglich die Art und Weise der Einholung von datenschutzrechtlichen Einwilligungen. Der Anbieter hatte auf seiner Website die Zustimmung zum Setzen von Cookies dadurch einholen wollen, dass eine entsprechende Einwilligungserklärung für den Nutzer vorausgefüllt, wenn auch abwählbar war. Der BGH legte im Verfahren dem EuGH diesbezüglich diverse Fragen zur Auslegung des EU-Rechts im Rahmen der ePrivacy-Richtlinie und der Datenschutzgrundverordnung (DSGVO) vor:

- Liegt eine wirksame Einwilligung vor, wenn ein vorhandenes Kästchen zur Cookie-Setzung bereits angekreuzt ist?
- Inwiefern ist der Nutzer durch den Seitenbetreiber bezüglich der Verwendung von Cookies aufzuklären? Umfasst dies auch die Zugriffsmöglichkeit von Dritten auf die Cookies sowie die Funktionsdauer der Cookies?
- Ergeben sich durch die Einführung der DSGVO Änderungen gegenüber der älteren ePrivacy-Richtlinie?

Die EuGH-Cookie-Entscheidung

Das Urteil des EuGH aus Oktober 2019 war mit Blick auf diese Fragen eindeutig: Ein vorangekreuztes Kästchen, das nicht abgewählt wird, ist für eine Einwilligung nicht ausreichend. Die Nutzer/-innen müssten aktiv handeln. Dies gelte erst recht seit Inkrafttreten der DSGVO, durch den größeren Regelungsumfang der ePrivacy-Richtlinie jedoch nicht nur für personenbezogene Daten. Zudem müssten Website-Betreiber über Cookies informieren, insbesondere über Zugriffsmöglichkeiten Dritter und Funktionsdauer.

Der EuGH hat allerdings nicht explizit entschieden, dass alle Cookies einer ausdrücklichen Einwilligung bedürfen. Das Urteil wurde aber dennoch oft als Fingerzeig aufgefasst, dass Cookies ganz überwiegend nur noch mit Einwilligung des jeweiligen Nutzers eingesetzt bzw. gespeichert werden können. Denn der EuGH bezog sich bei seiner Beurteilung der Zulässigkeit der Cookie-Nutzung insbesondere auf die ePrivacy-Richtlinie, weniger auf die DSGVO. Die Richtlinie geht jedoch grundsätzlich von einem Einwilligungserfordernis aus, während die DSGVO auch andere Rechtsgrundlagen für die Verarbeitung personenbezogener Daten kennt.

Welches Recht gilt in Deutschland?

Hier kommt zudem ein speziell „deutsches“ Problem zum Tragen: Ees war bisher unklar, welche Rechtsgrundlage für die Nutzung von Cookies bzw. der Einholung entsprechender Einwilligungen gilt. Der deutsche Gesetzgeber ging wohl von einer ausreichenden Umsetzung der ePrivacy-Richtlinie durch § 15 Abs. 3 Telemediengesetz (TMG) aus, nach dessen Wortlaut auch eine sogenannte „Opt-Out“-Lösung über einen Widerspruch des Nutzers zulässig wäre. Die deutschen Datenschutzaufsichtsbehörden stellten sich hingegen bisher auf

den Standpunkt, dass § 15 Abs. 3 TMG aufgrund des zur ePrivacy-Richtlinie widersprüchlichen Wortlauts nicht mehr anzuwenden sei. Die DSGVO sei vorrangig anzuwenden, als Rechtsgrundlage für die Nutzung von Cookies komme nur Art. 6 DSGVO in Betracht. Diesbezüglich gingen die Aufsichtsbehörden bisher jedoch ebenfalls davon aus, dass regelmäßig eine Einwilligung erforderlich sei. Nur bei sehr datenschutzfreundlichen Cookies könne von einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO abgesehen und die Datenverarbeitung auf ein überwiegendes berechtigtes Interesse des Websitebetreibers nach Art. 6 Abs. 1 lit. f DSGVO gestützt werden.

Die Entscheidung des BGH

Der BGH stand nun vor der der schwierigen Aufgabe, den Wortlaut des § 15 Abs. 3 TMG mit den Vorgaben des EuGH in Einklang zu bringen und dabei auch die DSGVO im Blick zu behalten. Im Ergebnis hält der BGH eine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG für möglich. Dieser sei mit Blick auf die ePrivacy-Richtlinie und die Vorabentscheidung des EuGH so auszulegen, dass für Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung (und nach dem Wortlaut des § 15 Abs. 3 TMG auch für die „bedarfsgerechte Gestaltung“ der Website) die Einwilligung des Nutzers erforderlich ist. Durch die richtlinienkonforme Auslegung gehe § 15 Abs. 3 TMG in Verbindung mit Art. 95 DSGVO zudem den Regelungen der DSGVO vor und sei vorrangig anzuwenden. Im Übrigen bestätigte der BGH auch die weiteren Vorgaben des EuGH zur Ausgestaltung der Einwilligung und deren Einholung.

Was bedeutet das Urteil für Webseiten-Betreiber?

Webseiten-Betreiber sollten zukünftig für alle Cookies in den Bereichen Analyse, Statistik und Tracking eine Einwilligung einholen. Diese darf nicht vorausgewählt sein und muss aktiv und freiwillig durch den Nutzer erteilt werden. Der Nutzer ist zudem über das jeweilige Cookie zu informieren, insbesondere hinsichtlich des Datenzugriffs durch Dritte sowie die Speicherdauer des Cookies. Dies kann durch ein entsprechendes Cookie-Banner oder Consent-Tool geschehen. Die Informationen sollten zudem auch in der Datenschutzerklärung enthalten sein.

In Übereinstimmung mit den Vorgaben der ePrivacy-Richtlinie und des TMG (bzw. seiner richtlinienkonformen Auslegung) dürfte eine Einwilligung jedoch nicht erforderlich sein für Cookies, die zur technischen Bereitstellung der Website und deren Funktionen bzw. für einen vom Nutzer angeforderten und diesem bereitgestellten Dienst unbedingt erforderlich sind. In diesen eng begrenzten Ausnahmebereich können beispielsweise Cookies für die Sprach der Website oder ggf. auch Warenkörbe in Webshops fallen. Die Bewertung dieser Cookies muss jedoch einzelfallabhängig anhand der jeweils umgesetzten Funktion und – bei Rückgriff auf einen Drittanbieter – auch anhand der jeweils eingesetzten Anwendung und deren Konfiguration erfolgen.

Nicht zuletzt müssen Website-Betreiber sicherstellen, dass Einwilligungen zu Cookies gesetzeskonform dokumentiert und aufbewahrt werden. Zudem muss eine einfache Widerrufsmöglichkeit zur Verfügung gestellt und die entsprechenden Löschprozesse bei einem ordnungsgemäßen Widerruf eines Nutzers umgesetzt werden.

Aufgepasst: Ausgestaltung von Cookie-Bannern und Consent-Tools

Doch damit nicht genug: Auch die Ausgestaltung von Cookie-Bannern und Consent-Tools sollte kritisch im Blick behalten werden. Um beim schnellen Wegklicken lästiger Banner und Pop-Ups doch noch möglichst viele Einwilligungen zu erhalten, sind viele Anbieter dazu übergegangen, den Nutzer durch das Design des Banners oder Tools in Richtung einer Einwilligung zu „führen“ (oft auch „Nudging“ genannt). Diese Ausgestaltung ist bei den europäischen Datenschutzaufsichtsbehörden jedoch umstritten: So haben sich u. a. der europäische Datenschutzausschuss (EDSA) sowie die dänische Datenschutzaufsichtsbehörde (Stellungnahme bisher nur auf Dänisch verfügbar) äußerst kritisch zu solchen Vorgehensweisen beim Design von Cookie-Bannern und Consent-Tools geäußert. Der Nutzer werde zu stark beeinflusst und die Einwilligung erfolge daher nicht mehr freiwillig. Andere Aufsichtsbehörden sind abweichender Ansicht und setzen ihrerseits selbst Analyse- und Statistik-Tools nicht entsprechend diesen Vorgaben ein. Die deutschen Aufsichtsbehörden haben sich zu diesem Thema noch nicht explizit geäußert, es dürfte jedoch aufgrund der bisher eher strengen Handhabung der DSGVO davon auszugehen sein, dass diese eine ähnliche Auffassung vertreten. Eine konservativere Herangehensweise dürfte daher zu empfehlen sein, will man kritische Nachfragen oder gar Datenschutzverstöße vermeiden.

Lösung ePrivacy-Verordnung?

Die Entscheidung des BGH ist zunächst zu begrüßen: Sie bestätigt das Einwilligungserfordernis für den Einsatz von Cookies auf höchstrichterlicher nationaler Ebene und bringt da-

Web browser cookies

durch Klarheit für die Umsetzung von Analyse- und Tracking-Anwendungen für deutsche oder in Deutschland niedergelassene und tätige Website-Betreiber.

Für Website-Betreiber bedeutet dies jedoch auch Nachteile: sie dürften zukünftig über Analyse- und Tracking-Tools weniger Daten von ihren Nutzern erhalten, eine Optimierung der Website und des eigenen Angebots dürfte dadurch erheblich erschwert werden. Es liegt nahe, dass unter den Voraussetzungen des Einwilligungserfordernisses und der ausführlichen Information nur ein kleiner Teil der Nutzer diese Möglichkeit wahrnehmen wird.

Eine Lösung für diese unbefriedigende Lage ist derzeit nicht erkennbar. Die ePrivacy-Verordnung, die u. a. konkret den Einsatz von Cookies gleichzeitig mit Inkrafttreten der DSGVO regeln sollte, lässt noch auf sich warten. Mehrere Entwürfe wurden abgelehnt, erst mit der deutschen EU-Ratspräsidentschaft ab dem zweiten Halbjahr 2020 wird mit einem Fortschritt gerechnet. Eine Umsetzung könnte aber auch in diesem Fall bis 2025 dauern – sofern das Vorhaben überhaupt noch weiter vorangetrieben und nicht doch vollständig verworfen wird.

Bis dahin sollten Website-Betreiber in der Regel Einwilligungen für Analyse- Statistik- und Tracking-Cookies einholen und nur in sehr eng begrenzten Ausnahmefällen – und auch dann nur gut begründet und dokumentiert – darauf verzichten. Anderenfalls drohen Rechtsverstöße, die insbesondere hinsichtlich der DSGVO mit erheblichen Bußgeldern einhergehen können. Von Interesse dürften zudem die in den nächsten Wochen zu erwartenden Stellungnahmen der deutschen Datenschutzaufsichtsbehörden sein – möglicherweise können daraus weitere praxisrelevante Hinweise und Beispiele abgeleitet werden.

Das BGH-Urteil zeigt bereits Wirkung – Datenschutzaufsichtsbehörden prüfen großflächig Medienunternehmen

Die deutschen Datenschutzaufsichtsbehörden haben das Urteil des BGH zudem unmittelbar zum Anlass genommen, darauf basierende Prüfungen und Befragungen durchzuführen. Der Einsatz von Tracking-Technologien, insbesondere Cookies, wird nun in einem ersten Schritt durch zehn der insgesamt 16 Landesdatenschutzbehörden bei größeren Medienunternehmen, die in der Regel einen Großteil ihrer Online-Tätigkeiten über Werbung finanzieren, unter die Lupe genommen. Von besonderem Interesse ist dabei das sogenannte Kopplungsverbot. Demnach kann eine Einwilligung in die Verarbeitung personenbezogener Daten unwirksam sein, wenn sie für die Dienstleistung selbst nicht erforderlich ist, der Anbieter ohne Einwilligung aber den Zugriff verweigert. Ob dieses Verbot umgangen werden kann, indem Nutzer/innen vor die Wahl gestellt werden, entweder die Einwilligung zu erteilen oder aber für das Angebot zu bezahlen, wie es einige journalistische Online-Angebote handhaben, ist noch ungeklärt. Auch die Rechtsprechung hierzu ist nicht einheitlich, traditionell vertreten aber die deutschen Datenschutzaufsichtsbehörden eher strenge und damit ablehnende Positionen. Es ist zudem zu erwarten, dass die Behörden zukünftig ihre Prüfungen ausweiten und deutlich strenger auf Hinweise von Betroffenen und Wettbewerbern reagieren werden. Dies gilt ganz besonders vor dem Hintergrund, dass viele Cookies Daten außerhalb der EU (z. B. in die USA) übermitteln, diese Datentransfers aber nach dem aktuellen EuGH-Urteil nicht mehr unter dem EU-US Privacy Shield stattfinden dürfen (wie z. B. bisher bei Google Analytics der Fall) und kritisch überprüft werden müssen.

Microsoft Teams und Office 365 – Aufsichtsbehörden bemängeln den Datenschutz

Sowohl die Berliner Beauftrage für Datenschutz und Informationsfreiheit als auch der Europäische Datenschutzbeauftragte (European Data Protection Supervisor – EDPS) haben – unabhängig voneinander – die datenschutzrechtliche Ausgestaltung der cloudbasierten Microsoft Produkte untersucht und kommen zu dem Ergebnis, dass diese teilweise nicht den datenschutzrechtlichen Anforderungen der DSGVO genügen.

Berliner Aufsichtsbehörde untersucht Videokonferenzsysteme

Videokonferenzsysteme, wie Microsoft Teams, Zoom, boomen. Dass diese Dienste dadurch auch in den Fokus der datenschutzrechtlichen Aufsichtsbehörden geraten, war nur eine Frage der Zeit. Die Berliner Aufsichtsbehörde hat nun die Ergebnisse ihrer Kurzprüfung von Videokonferenz-Diensten veröffentlicht, bei der der Fokus vor allem auf der Ausgestaltung der Auftragsverarbeitungsverträge lag. Die Ergebnisse sind für die Cloud-Anbieter sehr negativ ausgefallen. Kaum einer der geprüften Videokonferenz-Dienste könne nach Ansicht der Behörde datenschutzkonform eingesetzt werden. Insbesondere bei Microsoft Teams, als wohl eine der am meisten verwendeten Anwendungen, hat die Behörde zahlreiche Mängel im Auftragsverarbeitungsvertrag von Microsoft identifiziert.

Konsequenzen für den Einsatz von Office 365

Indem Microsoft Teams fester Bestandteil von Microsoft 365 (ehemals Office 365) ist und deren Bestimmungen (Online Services Terms und DPA) unterliegt, führe dies u. a. dazu, dass auch der Einsatz der cloudbasierten Versionen von Word, PowerPoint und Co. sowie Microsoft Azure zum jetzigen Zeitpunkt laut der Behörde nicht rechtskonform möglich sei. Obwohl Microsoft die Nutzungsbedingungen erst kürzlich überarbeitet hatte, enthalte der Auftragsverarbeitungsvertrag noch immer unklare und widersprüchliche Regelungen und weiche damit von den gesetzlichen Mindestanforderungen ab. In diesem Zusammenhang kündigte die Behörden ferner an, die bemängelten Punkte bei Prüfungen von Unternehmen besonders berücksichtigen zu wollen. Vor diesem Hintergrund sollten Unternehmen, die cloudbasierte Videokonferenzsysteme und Microsoft 365 einsetzen, prüfen, inwiefern sie selbst nachbessern oder vorerst auf den Einsatz verzichten können.

Stellungnahme von Microsoft

Eine Stellungnahme von Microsoft zu diesen Punkten ließ nicht lange auf sich warten. Darin widerspricht Microsoft der Behörde deutlich. Microsoft sei überzeugt, dass die Produkte im Allgemeinen und auch Microsoft Teams im Speziellen datenschutzkonform eingesetzt werden können. Dabei geht Microsoft im Detail auf die von der Behörde kritisierten Punkte ein. Insbesondere die Mängel im Auftragsverarbeitungsvertrag seien hauptsächlich auf Übersetzungsfehler zurückzuführen. Dabei kritisiert Microsoft auch, dass sich die Behörde nicht mit den von Microsoft zur Verfügung gestellten Informationen beschäftigt hätte und daher zu einem falschen Ergebnis komme. Ob diese Reaktion von Microsoft die Aufsichtsbehörde zu einer anderen datenschutzrechtlichen Bewertung gelangen lässt, ist fraglich. Gleichzeitig scheint Microsoft auf der eigenen Einschätzung zu beharren und die von der Aufsichtsbehörde bemängelten Punkte nicht nachbessern zu wollen. In diesem Streit haben die Kunden von Microsoft zunächst das Nachsehen – denn diese tragen als datenschutzrechtlich Verantwortliche das Risiko, dass die Datenverarbeitung rechtskonform erfolgt und z. B. der Auftragsverarbeitungsvertrag den gesetzlichen Anforderungen genügt.

Europäischer Datenschutzbeauftragter prüft Microsoft Produkte und Dienste

Parallel zu der Prüfung durch die Berliner Aufsichtsbehörde prüfte auch der europäische Datenschutzbeauftragte im Rahmen einer Eigeninitiative die Nutzung der Microsoft Produkte und Dienste durch die EU-Institutionen. Das Ergebnis dieser Untersuchung veröffentlichte er nun in einem knapp 30 Seiten langen Bericht. Die Ergebnisse und Empfehlungen aus der Untersuchung dürften nicht nur für die EU-Institutionen von großem Interesse sein. Er kritisiert im Wesentlichen die folgenden fünf Punkte:

- **Die eigenständige Verarbeitung durch Microsoft**

  Microsoft behält sich nach den eigenen Bestimmungen für Online-Dienste das Recht vor, die Parameter der Auftragsverarbeitung und der vertraglichen Verpflichtungen zu ändern und selbst zu definieren. Hiermit würde Microsoft in unangemessener Weise die Rolle als Auftragsverarbeiter verlassen und selbst zum Verantwortlichen zu werden.

- **Die fehlende Kontrollmöglichkeit über Unterauftragsverarbeiter**

  Die Microsoft-Kunden haben weder die Kontrolle darüber, wer als Subunternehmer in Bezug auf die Auftragsverarbeitung eingesetzt wird, noch bestehen entsprechende Prüfungsrechte gegenüber den Unterauftragsverarbeitern.

- **Internationaler Datentransfer**

  Die Microsoft-Kunden können nicht vollständig nachvollziehen, wo die eigenen Daten gespeichert werden. Damit verbunden ist das Risiko einer unrechtmäßigen Offenlegung der Daten. Teilweise fehle es an geeigneten Garantien, die den internationalen Datentransfer DSGVO-konform absichern.

- **Datenerhebung durch Microsoft (Diagnosedaten)**

  Indem die Cloud-Produkte teilweise eigenständig Daten erheben und an Microsoft übermitteln, fehle es zudem an der notwendigen Transparenz der Dienste. Dies hatte im vergangenen Jahr auch das Niederländische Ministerium für Justiz und Sicherheit im Rahmen seiner Datenschutz-Folgenabschätzung für Microsoft Office 365 festgestellt.

- **Intransparente Verarbeitung**

  Ferner fehle es an der ausreichenden Klarheit der Informationen über Art, Umfang und Zweck der Verarbeitung sowie über die Risiken für die betroffenen Personen. Somit könnten die Kunden ihren Transparenzverpflichtungen gegenüber den Betroffenen nicht vollständig nachkommen.

Hinsichtlich all dieser Punkte gab der Datenschutzbeauftragte den europäischen Institutionen gleichzeitig Handlungs- und Lösungsempfehlungen an die Hand, durch die die bemängelten Punkte beseitigt werden könnten. Bestimmte Mängel könnten durch entsprechende Konfiguration der Produkte behoben werden. Andere wiederum sollten mit Microsoft ausgehandelt werden.

Handlungsoptionen für Microsoft-Kunden

Offen ist, welche Optionen ein Microsoft-Kunde nunmehr hat. Zum einen kann er darauf verzichten, Microsoft-Produkte einzusetzen. Dabei handelt es sich allerdings eher um eine theoretische Handlungsoption, denn die Produkte von Microsoft sind in vielen Fällen Marktstandard (z. B. Office-Programme wie Word und Excel). Alternativ kann der Kunde versuchen, Anpassungen der Vertragsbedingungen von Microsoft zu erreichen. Inwiefern für Kunden aber überhaupt Verhandlungsspielraum hinsichtlich der Ausgestaltung der vertraglichen Grundlagen besteht, ist allerdings mehr als fraglich. Diese Option dürfte allenfalls dann bestehen, wenn der jeweilige Kunde eine ausreichende Marktmacht hat, um Microsoft zu Verhandlungen zu bewegen. Für die meisten Unternehmen dürfte dies jedoch nicht zutreffen. Als weitere Option könnte der Kunde versuchen, anstelle einer Auftragsverarbeitung eine andere Rechtsgrundlage für die Datenübermittlung an Microsoft zu nutzen. Dies liefe allerdings auf eine Einzelfallprüfung hinaus, die in der Praxis kaum zu leisten sein wird – gerade in Anbetracht der Vielzahl der Datenverarbeitungen, die mit Microsoft-Anwendungen durchgeführt werden. Schließlich kann der Kunde stellvertretend für Microsoft einen Rechtstreit über die Rechtmäßigkeit der tatsächlichen und vertraglichen Ausgestaltung führen, um feststellen zu lassen, ob die von Microsoft vorgebrachten Punkte vor Gericht überzeugen. Dies beinhaltet jedoch naturgemäß ein hohes (Kosten-)Risiko.

Unser Kommentar

Im Ergebnis bleibt festzuhalten, dass die Einschätzung der Berliner Datenschutzbehörde und des europäische Datenschutzbeauftragten zwar in der Sache richtig sein mag. Tatsächlich hilft diese Erkenntnis den Unternehmen, die Microsoft-Produkte nutzen, jedoch nicht weiter. Denn es bleibt völlig offen, wie diese Unternehmen sich verhalten sollen, um die Anforderungen der DSGVO im Umgang mit Windows, Office & Co. umzusetzen. Zu hoffen bleibt, dass Microsoft Anpassungen an den Vertragsbedingungen vornimmt und die kritisierten Punkte schnell behebt. Um weitestgehend datenschutzkonform zu handeln, sollten Unternehmen bis dahin Ihren Einsatz von Microsoft 365 überprüfen und erste Maßnahmen zur Verringerung von Risiken umsetzen.

Per Video zum Doktor – Wissenswertes zur Videosprechstunde

Durch Corona und die zunehmende Digitalisierung erlangt die Telemedizin (z. B. über Videosprechstunden) immer größere Bedeutung. Sie kann dabei helfen, Infektionen zu vermeiden und den Ärztemangel auf dem Land zu verringern. Ärzte müssen sich dabei nicht nur mit dem relevanten Berufsrecht, sondern auch mit Datenschutz und IT-Sicherheit auseinandersetzen.

Hintergrund

Vor etwas mehr als einem Jahr, im März und April 2019, führte die Kassenärztliche Bundesvereinigung (KBV) eine repräsentative Versichertenbefragung zu ihrer Einschätzung der Versorgungssituation in Deutschland durch. Im Ergebnis gaben 37 % der Befragten an, sie wären grundsätzlich bereit, das Angebot einer Videosprechstunde zu nutzen. Aufgrund der Corona Pandemie ist das Interesse stark gestiegen. So hat sich die Zahl der zertifizierten Anbieter von Plattformen für solche Videosprechstunden in den letzten Wochen in etwa verdoppelt. Auch die bisher für Ärzte geltende Begrenzung für die Videosprechstunde auf 20 % der Behandlungsfälle wurde bis zum Ende des zweiten Quartals 2020 ausgesetzt. Den mit der Videosprechstunde einhergehenden Vorteilen für Ärzte und Patienten stehen jedoch auch Nachteile gegenüber. Es gibt zudem regulatorische Vorgaben, die eingehalten werden müssen.

Vor- und Nachteile der Videosprechstunde

Die Videosprechstunde ist Teil der Telemedizin, die sich dadurch auszeichnet, dass medizinische Leistungen über räumliche Distanz unter Einsatz von Informations- und Kommunikationstechnologien erbracht werden. Die möglichen Leistungen erfassen dabei Diagnose, Therapie und Rehabilitation sowie ärztliche Konsile. Die Videosprechstunde ist ein geeignetes Mittel, die Infektionsgefahr von Arzt und Patienten zu senken und kann gerade bei Ärztemangel den Zugang zu ärztlicher Versorgung verbessern. Dagegen kann die Gefahr von Behandlungsfehlern steigen, weil der Arzt sich ohne den persönlichen Eindruck vom Patienten möglicherweise nur ein unzureichendes Bild des Patienten und dessen Krankheitssymptomen machen kann. Er muss sich insoweit auf die Angaben des Patienten verlassen. Dadurch kann der Aufwand für die Arztpraxen auch steigen, soweit sich nach einer Videosprechstunde herausstellt, dass der Patient doch persönlich vorstellig werden muss. Hinzu kommen die Risiken im Hinblick auf den Schutz der Patientendaten und die damit einhergehende Vertraulichkeit des Arzt-Patienten-Verhältnisses.

Ablauf der Videosprechstunde

Für die Durchführung der Videosprechstunde benötigen Arzt und Patient grundsätzlich nur eine Kamera, ein Mikrofon und Lautsprecher sowie eine Internetverbindung. Die Praxis kooperiert mit einem entsprechenden Videodienstanbieter („Anbieter“), der Gewähr für die Einhaltung besonderer Standards bietet. Die Kassenärztliche Bundesvereinigung stellt hierzu eine Liste zertifizierter Anbieter bereit. Der Patient erhält dann entweder von der Praxis oder von dem Anbieter einen Termin zur Videosprechstunde, einen Link zur Internetseite des Anbieters sowie einen Einwahlcode für die Sprechstunde. Nachdem der Patient sich eingewählt hat, wartet er im virtuellen Wartezimmer, bis er vom Arzt in die Videosprechstunde geladen wird.

Eine gesonderte Registrierung beim Anbieter ist für den Patienten in der Regel nicht erforderlich. Für die richtige Zuordnung durch den Arzt muss er jedoch seinen Namen korrekt angeben. Bei Patienten, die bisher noch nicht in der Praxis vorstellig waren, kann es erforderlich sein, die Gesundheitskarte in die Kamera zu halten, damit die Identität überprüft und die notwendigen Daten erfasst werden können.

Zu Beginn der Sprechstunde erfolgt eine Vorstellung aller anwesenden Personen. Der Arzt ist zudem verpflichtet, den Patienten über den Ablauf der Videosprechstunde zu informieren. Hierzu gehört neben der Tatsache, dass die Teilnahme an der Videosprechstunde freiwillig ist, auch das Verbot von Aufzeichnungen jeglicher Art. Nach Beendigung der Sprechstunde melden sich Arzt und Patient von der Internetseite ab.

Berufsrechtliche Vorgaben und medizinrechtliche Voraussetzungen

Die Videosprechstunde ist u. a. in der Musterberufsordnung-Ärzte (MBO-Ä) geregelt. Die MBO-Ä enthält die berufsrechtlichen und ethischen Grundlagen des Arztberufs. Sie regelt die Rechte und Pflichten der Ärzte gegenüber den Patienten, Kollegen und Landesärztekammern. Sie dient den Landesärztekammern als Muster und fördert so die einheitliche Entwicklung des Berufsrechts, ist jedoch kein geltendes Recht. Sie entfaltet nur dann Rechtswirkungen, wenn die Landesärztekammern sie als Satzung beschließen. Die Landesärztekammern können auch abweichende Regelungen treffen.

§ 7 Abs. 4 Satz 3 MBO-Ä erlaubt die ausschließliche Beratung oder Behandlung über Kommunikationsmedien im Einzelfall, wenn dies ärztlich vertretbar ist, die erforderliche Sorgfalt gewahrt wird und der Patient entsprechend aufgeklärt wird. Es handelt sich dabei um eine Ausnahmeregelung zum Grundsatz des persönlichen Kontakts zwischen Arzt und Patient, dem „Goldstandard“ nach § 7 Abs. 4 Satz 1 MBO-Ä.

Die Einschätzung der ärztlichen Vertretbarkeit obliegt der Beurteilung durch den Arzt und muss insbesondere berücksichtigen, ob eine Behandlung aus der Ferne den Bedürfnissen der Behandlung gerecht wird. Dies kann sich auch im Laufe der Behandlung ändern, z. B. wenn eine körperliche Untersuchung erforderlich wird. Die Voraussetzung der ärztlichen Vertretbarkeit fordert im Grunde eine medizinische Indikation für die Fernbehandlung. Der Verweis auf die erforderliche Sorgfalt stellt klar, dass der Arzt auch bei der Telemedizin an das Gebot der gewissenhaften Ausübung des Berufs, §§ 2 Abs. 2 und 3, 11 MBO-Ä gebunden ist. Er muss also insbesondere die notwendige fachliche Qualifikation aufweisen und die anerkannten Standards einhalten. Das Erfordernis der Patientenaufklärung soll das Selbstbestimmungsrecht des Patienten stärken. Nur so kann dieser eine informierte Entscheidung treffen und eine wirksame Einwilligung erteilen. Einzelheiten zur Information des Patienten sind auch in § 630e BGB geregelt.

Einzelheiten zur Videosprechstunde sind zudem in der Anlage 31b zum Bundesmantelvertrag-Ärzte i.V.m. § 291g Abs. 4 S. 1 SGB V geregelt. Hierbei handelt es sich um eine Vereinbarung zwischen der KBV und dem Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband). Die KBV nimmt die politische Interessenvertretung der in Praxen ambulant tätigen Ärzte und Psychotherapeuten wahr. Der GKV-Spitzenverband vertritt die Interessen der gesetzlichen Kranken- und Pflegekassen. Das Regelwerk stellt Anforderungen an die Teilnehmer der Videosprechstunde auf und verweist ausdrücklich auf die Einhaltung der Bestimmungen zum Datenschutz und der Informationssicherheit.

Datenschutzrechtliche Anforderungen

Im Rahmen der Videosprechstunde kommt es sowohl auf Seiten der Arztpraxis als auch beim Anbieter, zu einer Verarbeitung personenbezogener Daten des Patienten. Die Datenverarbeitung muss daher den Anforderungen der DSGVO genügen. Insbesondere muss den Patienten eine Datenschutzerklärung zur Verfügung gestellt werden, die hinsichtlich aller Verarbeitungsvorgänge im Rahmen der Videosprechstunde informiert, Art. 12 ff. DSGVO.

Bei der Verarbeitung von Gesundheitsdaten gelten zudem besondere Regelungen, da diese Daten besonders schutzbedürftig sind. Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung von Gesundheitsdaten grundsätzlich untersagt, es sei denn, es liegt eine Legitimierung vor, z. B. nach Art. 9 Abs. 2 DSGVO oder § 22 BDSG. Hier dürften in der Regel die Erlaubnistatbestände der Einwilligung nach Art. 9 Abs. 2 lit. a, Art. 7 DSGVO und der Versorgung bzw. Behandlung im Gesundheitsbereich, Art. 9 Abs. 2 lit. h, Abs. 3 DSGVO, § 22 Abs. 1 lit. b BDSG einschlägig sein.

Der Arzt ist also grundsätzlich verpflichtet, vor Durchführung der Videosprechstunde eine Einwilligungserklärung des Patienten bzgl. der im Rahmen der Videosprechstunde stattfindenden Datenverarbeitungsvorgänge einzuholen. Dies kann auch auf elektronischem Wege geschehen. Die Einwilligung muss allerdings die Anforderungen des Art. 9 Abs. 2 lit. a

i.V.m. Art. 7 DSGVO erfüllen: Sie muss ausdrücklich, freiwillig, informiert und für einen konkreten Zweck erfolgen.

Der Anbieter wird in der Regel als Auftragnehmer und somit als Auftragsverarbeiter im Sinne der DSGVO für den Arzt tätig, Art. 28 DSGVO. Dies hat zur Folge, dass eine vertragliche Vereinbarung in Form einer Auftragsverarbeitungsvereinbarung zwischen Arzt und Anbieter erforderlich ist, die die datenschutzrechtlichen Pflichten der beiden Parteien regelt. Gemäß den Regelungen der DSGVO ist der Arzt dabei dafür verantwortlich, dass er sich nur solcher Anbieter bedient, die hinreichende Garantien für die Einhaltung des Datenschutzes bieten. § 4 Abs. 4 Anlage 31b BMV-Ä verschärft die Pflichten der DSGVO für den Arzt zudem dahingehend, dass der Arzt nur solche Anbieter nutzen darf, die ein Datenschutzzertifikat oder ein von einer Datenschutzbehörde vergebenes bzw. anerkanntes Gütesiegel vorweisen können.

Während der Videosprechstunde ist sicherzustellen, dass eine angemessene Privatsphäre gewährleistet ist. So sollten sich beispielsweise keine Zuhörer im Raum befinden, von denen der Patient keine Kenntnis hat. Aufzeichnungen jeglicher Art sind während der Videosprechstunde nicht erlaubt. Zudem gilt die ärztliche Schweigepflicht, die auch strafrechtlich abgesichert ist, § 203 StGB.

IT- und Datensicherheit

Arzt und Anbieter müssen im Rahmen der Videosprechstunde die IT- und Datensicherheit gewährleisten. Der Anbieter muss dies auch durch ein Zertifikat nachweisen können. Sie müssen also technische und organisatorische Maßnahmen treffen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen. Besonders wichtig ist in diesem Zusammenhang auch, dass die eingesetzte Technik und die elektronische Datenübertragung eine angemessene und störungsfreie Kommunikation ermöglichen. Hierfür ist neben einer Bandbreite von mindestens 2.000 kbit/s auch die Ende-zu-Ende-verschlüsselte Übertragung vorgeschrieben.

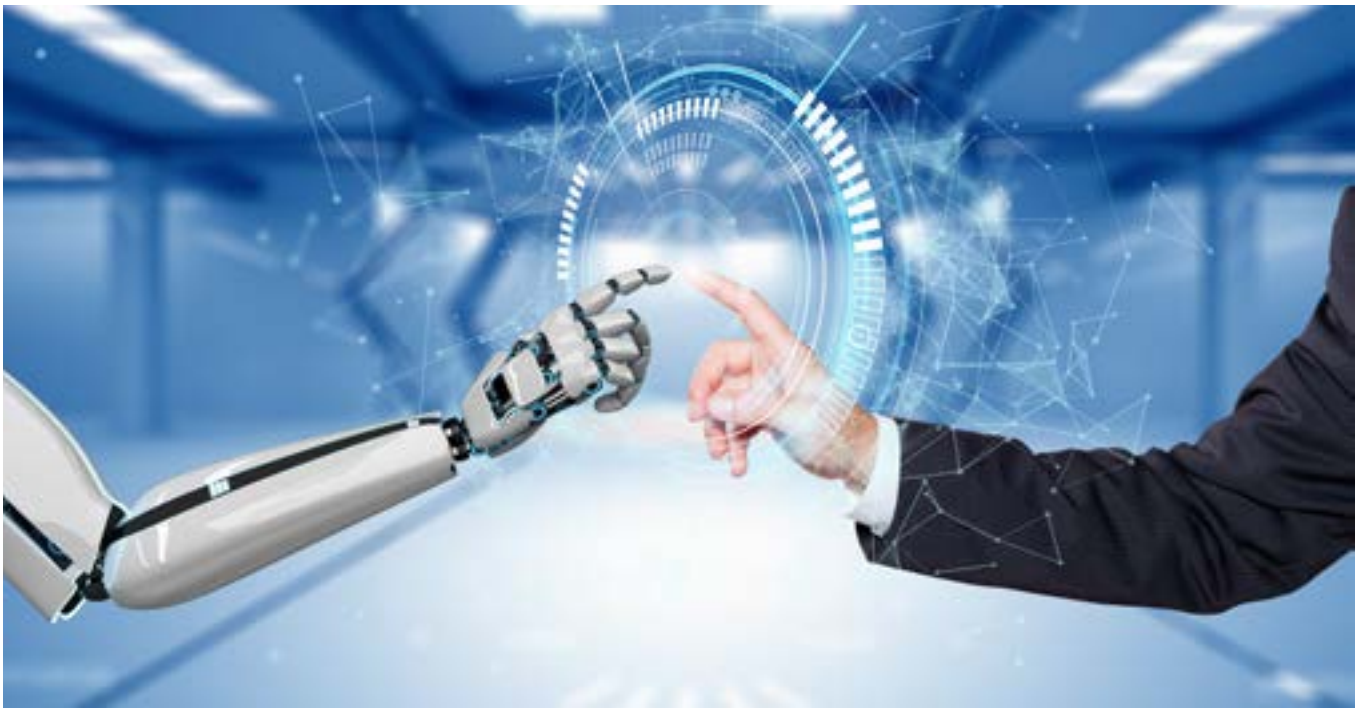
Robotic Process Automation: Welche Rechtsfragen stellen sich?

„Digitalisierungs-Turbo“ – so wird Robotic Process Automation (RPA) von Mittelstand und Großunternehmen bezeichnet. Dies ergab die Studie „Robotic Automation 2020“ von IDG. Damit hat RPA das Potential, den Arbeitsalltag in vielen Unternehmen effizienter zu gestalten und nachhaltig zu verändern. Doch mit dem Effizienzversprechen steigt auch das Konfliktpotential: Arbeitnehmerrechte, Datenschutz und Urheberrechte können betroffen sein, wenn ein Unternehmen RPA einführen möchte. Doch was bedeutet RPA genau?

Hintergrund

Mit Hilfe von RPA können die Unternehmensprozesse effizienter gestaltet und umgesetzt werden. Bevor ein Unternehmen RPA einsetzt, müssen die bestehenden Prozesse zunächst erfasst und analysiert werden. Dabei werden regelmäßig digitale Abbilder (sog. Digital Twins) der Prozesse erzeugt. Man spricht vom „Process Mining“. Die Analyse dieser Prozesse gibt Aufschluss darüber, welche Prozessschritte automatisiert und damit effizienter umgesetzt werden können. Die lückenhafte oder fehlende Dokumentation der eigenen Prozesse wird von den befragten Unternehmen der IDG Studie als eine der größten Herausforderung bei der Einführung von RPA und Process Mining eingeschätzt. Ohne eine solche vollständige Dokumentation kann RPA aber nicht sinnvoll umgesetzt werden.

Insbesondere wiederholbare, gleichförmige Aufgaben können im Wege des RPA durch Software-Roboter (sog. Bots) übernommen werden. Der Bot führt einen vorher definierte Prozess-Workflow aus. Dies führt dazu, dass eine Reihenfolge von Prozessschritten automatisiert ausgeführt werden kann, ohne dass ein Mensch involviert sein muss. Beispiele sind u.a. dass Rechnungen automatisiert erfasst und abgelegt, Kundenanfragen mit Hilfe von Chatbots beantwortet, Bestel-



lungen automatisiert prozessiert oder Daten von einem System in eine anderes System überführt werden, ohne dass eine unmittelbare Schnittstelle besteht. RPA kann aber auch eingesetzt werden, um ein Unternehmen dabei zu unterstützen, Gesetze und Richtlinien einzuhalten und die Compliance zu gewährleisten. Ein Beispiel sind Know-Your-Customer Prozesse im Rahmen der Geldwäscheprävention.

Rechtliche Bewertung von RPA

Will ein Unternehmen RPA einführen, müssen neben den vielen Vorteilen jedoch auch rechtliche Anforderungen und Risiken beurteilt werden. Dabei sollten insbesondere die nachfolgenden Punkte berücksichtigt werden.

Arbeitsrecht

Neben RPA verbessert und optimiert das Process Mining die Unternehmensprozesse. Mit Hilfe des Process Mining werden Geschäftsprozesse systematisch erfasst, analysiert und ausgewertet. Auf dieser Grundlage kann das Unternehmen seine Prozesse bewerten, korrigieren, optimieren oder neu erstellen. Nach der IDG-Studie betrifft dies nicht nur die Prozesse in der IT-Abteilung, sondern auch im Management, der Finanzabteilung und der Produktion.

Arbeitsrechtliche Probleme treten auf, wenn durch das Process Mining nachgewiesen werden kann, dass einzelne Mitarbeiter die definierten Prozessabläufe nicht einhalten oder – im Vergleich zum Rest der Mitarbeiter – mit Ihrer Arbeitsleistung abfallen. Wird ein Tool eingeführt, durch das eine solche Verhaltenskontrolle möglich ist, steht dem Betriebsrat ein Mitbestimmungsrecht zu. Dieses Mitbestimmungsrecht besteht bereits, wenn die technische Einrichtung, die eingeführt werden soll, grundsätzlich die Möglichkeit bietet, dass Verhalten der Mitarbeiter zu überwachen. Unerheblich ist, ob das Unternehmen die technische Einrichtung zu diesem Zweck tatsächlich einsetzen möchte – es kommt ausschließlich auf die bloße Geeignetheit zur Mitabeiterkontrolle an. Die Studie zeigt auch, dass Betriebsräte vereinzelt Widerstand leisten, wenn ein Unternehmen RPA einführt. Dies geht natürlich mit der Befürchtung des Betriebsrats einher, dass Mitarbeiter abgebaut werden, wenn die Unternehmensprozesse optimiert und automatisiert werden.

Neben den Mitbestimmungsrechten des Betriebsrats sind aber auch datenschutzrechtliche Vorgaben zu beachten, wenn im Wege des Process Mining mitarbeitergenau Informationen gesammelt werden. Die datenschutzrechtlichen Vorgaben können umgangen werden, wenn die Informationen anonymisiert erhoben werden und – auch nachträglich – nicht mehr einem bestimmten Mitarbeiter zugeordnet werden können, z. B. in dem sich die Informationen stets auf Gruppen von Mitarbeitern beziehen. Ob und inwieweit dies möglich ist, hängt natürlich von den Unternehmensprozessen ab, die analysiert, und den Zielen, die damit verfolgt werden.

Haftung

Kommt es durch RPA zu einem Schaden, z. B. weil Daten falsch zugeordnet wurden oder Kundenfragen fehlerhaft beantwortet wurden, stellt sich die Frage, wer diesen Schaden ersetzen muss. In aller Regel wird zunächst das handelnde Unternehmen den Schaden begleichen müssen, da es in einer unmittelbaren Rechtsbeziehung zum Geschädigten steht. Das Unternehmen kann aber gegebenenfalls Regress nehmen, wenn der Schaden nicht durch einen eigenen Fehler verursacht wurde.

Ob und inwieweit ein Regress möglich ist, hängt davon ab, wie der zugrundeliegende Vertrag über die RPA-Software ausgestaltet ist. Insofern kommen insbesondere drei vertragliche Konstellation in Betracht:

- **Standalone-Erwerb von RPA Software:** das Unternehmen erwirbt die Software, implementiert und konfiguriert diese selbst;
- **Erwerb der RPA Software und Implementierung durch einen Dienstleister:** hier definiert das Unternehmen die Anforderungen und der Dienstleister setzt diese um; oder
- **RPA Outsourcing:** hierbei wird der komplette RPA Prozess auf einen externen IT Dienstleistern ausgelagert, welcher die RPA Software selbst betreibt und in die Prozesse des Unternehmens einbindet.

Wird nun durch den Einsatz der RPA Software ein Schaden verursacht, muss zunächst geklärt werden, wer den Schaden verursacht hat. Dies hängt von der Vertragskonstellation ab. In der Praxis kommt es aber entscheidend darauf an, die Schadensursache nicht nur behaupten, sondern auch nachweisen zu können. Grundsätzlich muss der Anspruchssteller beweisen, dass der Schaden durch eine Pflichtverletzung des Anspruchsgegners verursacht wurde. Damit dies möglich ist, muss beim RPA darauf geachtet werden, dass die einzelnen, automatisierten Prozessschritte, Aufgaben und Aktionen detailliert dokumentiert sind und somit nachgeprüft werden können. Die Log-Files sollten Aufschluss darüber geben, ob Fehler aufgetreten sind oder versucht wurde, den automatisierten Prozess von außen zu manipulieren.

Ebenso müssen die automatisierten Prozesse durch ein Rollen- und Berechtigungskonzept gesichert sein, damit nur Personen Änderungen vornehmen können, die dazu auch legitimiert sind. Gleichzeitig sollte protokolliert werden, wann welche Person welche Änderung durchgeführt hat. Ungeachtet angemessener Sicherheitsvorkehrungen sollten die Prozesse, die durch RPA automatisiert sind, von geschulten Mitarbeitern überwacht und kontrolliert werden.

Urheberrecht

Durch RPA können Schnittstellen ersetzt und Daten automatisiert zwischen zwei Systemen ausgetauscht werden. Ebenso ist es möglich, automatisiert bestimmte Aktionen in einer Software auszulösen. Weil das RPA-Tool und die Software zwei unterschiedliche Computerprogramme sind, stellt sich die Frage, ob für diese automatisierten Vorgänge eine Lizenz erforderlich ist. In dieser Konstellation weist die Verwendung von RPA Parallelen zur sog. „indirekten Softwarenutzung“ auf. Hat die Aufgabe, die durch das RPA Tool ersetzt wird, vormals ein Mensch durchgeführt, benötigte der Mensch in der Regel eine Lizenz, um die Software nutzen zu dürfen. Wird der Mensch nun durch einen Bot ersetzt, stellt sich die Frage, ob auch der Bot eine Lizenz benötigt. Zumindest der Softwareanbieter wird dies bejahen. Anderenfalls wird sein Geschäftsmodell ernsthaft in Frage gestellt. Dies wird deutlich, wenn man sich vorstellt, dass der Bot nicht nur einen Menschen – und damit eine Lizenz -, sondern eine Vielzahl von Menschen – und damit eine Vielzahl von Lizenzen – ersetzt. Viele Softwareanbieter untersagen in ihren Lizenzbestimmungen daher dieses sog. Pooling oder Multiplexing. Auf der anderen Seite möchte das Unternehmen, dass RPA einsetzt, gerade Kosten sparen. Zusätzliche Lizenzkosten oder gar ein Rechtsstreit mit den Softwareanbieter stellen ein Risiko für das Unternehmen und den Erfolg der RPA-Strategie dar.

Ob und unter welchen Voraussetzungen eine indirekte Nutzung von Software ein zusätzliches Nutzungsrecht erfordert, ist aktuell nicht abschließend geklärt. Die juristische Diskussion ist komplex. Die rechtliche Bewertung hängt dabei u. a. davon ab, wie die eingesetzten Computerprogramme in technischer Hinsicht miteinander interagieren. Gerichtsurteile in Deutschland, die eine Tendenz vorgeben, liegen leider noch nicht vor.

Vor diesem Hintergrund sollte das betroffene Unternehmen einzelfallabhängig untersuchen, ob mit Blick auf die eingesetzte Software und das dahinterstehende Lizenzmodell überhaupt ein Risiko besteht, dass eine Diskussion über die indirekte Nutzung geführt werden muss. Hat der Lizenzgeber z. B. ausdrücklich geregelt, ob und wie eine indirekte Nutzung möglich ist, kann RPA eingeführt werden, wenn diese Voraussetzungen eingehalten und umgesetzt werden. Im Zweifelsfall sollte juristisch überprüft werden, ob hier ein Problem bestehen kann.

Datenschutzrecht

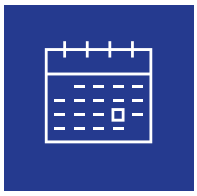
Das Datenschutzrecht ist dann zu beachten, wenn durch Process Mining und RPA personenbezogene Daten verarbeitet werden. In der Regel stehen datenschutzrechtliche Vorgaben dem Einsatz von RPA nicht im Weg. Probleme können auftreten, wenn das Verhalten von Mitarbeitern überwacht wird oder besonders sensitive personenbezogene Daten, z. B. Gesundheitsdaten, verarbeitet werden. Sind Dienstleister in den Prozess eingebunden, muss in der Regel ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Datenschutzrechtliche Probleme können aber auftreten, wenn durch die Prozessautomatisierung Entscheidungen getroffen werden, die unmittelbar gegenüber einem Menschen wirken, z. B. durch einen Chatbot. Nach Art. 22 DSGVO hat eine betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dieses Verbot automatisierter Entscheidung kann einer Automatisierung eines Prozesses entgegenstehen. Verboten sind danach Systeme, die automatisch Verträge ablehnen, wenn bestimmte Parameter nicht erfüllt sind. Allerdings ist dieses Verbot nicht so strikt, wie es auf den ersten Blick zu sein scheint: das Gesetz lässt verschiedene Möglichkeiten und Ausgestaltungen zu, solche Prozess dennoch umzusetzen.

Unser Kommentar

Zusammenfassend ist festzuhalten, dass durch die Verwendung von RPA in Verbindung mit Process Mining ein großes Prozessoptimierungspotenzial für Unternehmen besteht. Dieses Potenzial wird ausweislich der IDG-Studie auch von den meisten Unternehmen erkannt, so erwarten sowohl große und mittelständische als auch kleine Unternehmen, dass sich RPA bis 2025 zu einer bedeutenden Technologie entwickelt. Die aufgeführten Vorteile können dabei nicht nur dazu führen, dass redundante Aufgaben zuverlässig und schnell ausgeführt werden, um Mitarbeiter zu entlasten, sondern auch, dass rechtliche Voraussetzungen zuverlässig eingehalten werden. Um dies zu gewährleisten, müssen die einschlägigen rechtlichen Voraussetzungen vorab erkannt und idealerweise von Anfang an in den Prozess-Workflow integriert werden. Mit Blick in die Zukunft bleibt zu beobachten, wie sich RPA unter einer möglichen KI-Implementierung und den damit einhergehenden rechtlichen Anforderungen weiterentwickelt.

Veranstaltungen, Veröffentlichungen und Blog



Eine Übersicht mit unseren Veranstaltungen finden Sie hier.

Eine Liste unserer aktuellen Veröffentlichungen finden Sie hier.

Unseren Blog finden Sie hier.

Impressum

Verleger: Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 0
Telefax +49 221 9937 110, contact@luther-lawfirm.com
V.i.S.d.P.: Dr. Michael Rath, Partner
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22, 50678 Köln, Telefon +49 221 9937 25795
michael.rath@luther-lawfirm.com

Bildnachweis: MR.Cole_Photographer/Getty Images: Seite 1; metamorworks/iStockphoto: Seite 3; anyaberkut/iStock: Seite 6; Lindheim23/iStock: Seite 10; metamorworks/iStock: Seite 13; Alexander Limbach/Adobe Stock: Seite 16

Haftungsausschluss

Obgleich dieser Newsletter sorgfältig erstellt wurde, wird keine Haftung für Fehler oder Auslassungen übernommen. Die Informationen dieses Newsletters stellen keinen anwaltlichen oder steuerlichen Rechtsrat dar und ersetzen keine auf den Einzelfall bezogene anwaltliche oder steuerliche Beratung. Hierfür stehen unsere Ansprechpartner an den einzelnen Standorten zur Verfügung.

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Jakarta, Köln, Kuala Lumpur, Leipzig, London, Luxemburg, München, Shanghai, Singapur, Stuttgart, Yangon

Weitere Informationen finden Sie unter
www.luther-lawfirm.com
www.luther-services.com

JUVE AWARDS 2019
Kanzlei des Jahres