Luther.

Newsletter IP/IT

3. Ausgabe 2020

Inhalt

Digitale Archivierung – Was gilt es zu beachten?

Nicht nur bei einer Tätigkeit vor Ort im Büro, sondern insbesondere auch bei der Arbeit im Homeoffice sind ein digitales Dokumentenmanagement und eine digitale Archivierung von großer Bedeutung. Unternehmen müssen jedoch die rechtlichen Rahmenbedingungen beachten, um rechtskonform zu agieren.

Hintergrund

Mit der fortschreitenden Digitalisierung gehen immer mehr Unternehmen dazu über, Systeme zur digitalen Archivierung zu nutzen. Dadurch lassen sich Ressourcen, Geld und Zeit einsparen sowie Fehler reduzieren. Mit Blick auf die Coronakrise ist auch nicht zu unterschätzen, dass ein digitales Dokumentenmanagement die Arbeit im Homeoffice nicht nur erleichtern, sondern in vielen Fällen sogar erst ermöglichen kann.

Neben den technischen Herausforderungen, die eine Umstellung auf eine digitale Archivierung mit sich bringt, müssen auch die gesetzlichen Anforderungen erfüllt werden. Diese ergeben sich insbesondere aus den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) sowie den Vorschriften aus der Datenschutzgrundverordnung (DSGVO) und dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).

Grundsätze aus den GoBD

Die GoBD stellen diverse allgemeine Grundsätze für alle Unternehmen auf, die in konkrete Maßnahmen umgesetzt werden müssen. Insbesondere mit Blick auf die bevorstehende Pflicht zur Stellung von elektronischen Rechnungen bei Auftragserfüllung gegenüber der öffentlichen Hand sollten die Grundsätze in die internen Prozesse eingebettet werden. Für

die Digitalisierung von archivierten Dokumenten dürften insbesondere die nachfolgenden Grundsätze zu beachten sein:

- **Grundsatz der Unveränderbarkeit:** Eine Buchung oder eine Aufzeichnung darf nicht in der Art verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Insofern müssen Änderungen stets nachvollziehbar und das Original noch vorhanden/einsehbar sein.
- **Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit:** Die einzelnen Geschäftsvorfälle und angewandten Buchführungs- oder Aufzeichnungsverfahren müssen für einen sachverständigen Dritten nachvollziehbar und nachprüfbar sein.
- **Grundsätze der Richtigkeit, der Vollständigkeit und der Ordnung:** Die Geschäftsvorfälle müssen richtig, vollzählig und lückenlos sowie geordnet aufgezeichnet werden.
- **Internes Kontrollsystem:** Die GoBD fordert die Einrichtung und die Vorhaltung eines internen Kontrollsystems, durch das die Einhaltung der Grundsätze und steuerrechtlicher Pflichten überwacht werden soll.
- **Grundsatz des Datenschutzes:** Die Datenverarbeitungssysteme müssen gegen Unauffindbarkeit, Vernichtung, Untergang oder Diebstahl der Daten bzw. des Systems an sich sowie gegen unberechtigte Eingaben und Veränderungen gesichert werden.

Konkrete Grundanforderungen aus den GoBD

Für die digitale Archivierung ergeben sich aus den angeführten Grundsätzen diverse konkrete Anforderungen:

- Alle Unterlagen, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen von Bedeutung sind, sind in einem Ordnungssystem mit Indexierung aufzubewahren.
- Die elektronische Archivierung muss die Unveränderbarkeit sowie Lesbarkeit und maschinelle Auswertbarkeit der Dokumente sicherstellen. Finden Veränderungen statt, müssen diese protokolliert werden. Durch den Archivierungsvorgang darf zudem keine Verkleinerung der Datenmengen erfolgen.
- Es muss gewährleistet werden, dass Hardware und Software durch Sicherheitsmaßnahmen vor Angriffen geschützt sind.
- In Datenverarbeitungssystemen erzeugte Dokumente sowie elektronische Handels- und Geschäftsbriefe sind im Ursprungsformat aufzubewahren. Beispiel: eine Rechnung in Form einer PDF-Datei muss auch als PDF-Datei aufbewahrt werden, eine Umwandlung (Konvertierung) in ein unternehmenseigenes Format führt in der Regel nicht zur Löschbarkeit der Ursprungsdatei.
- Papierdokumente können vernichtet werden, wenn eine ordnungsgemäße elektronische Archivierung sichergestellt ist und keine gesetzlichen Gründe dagegen sprechen.

Dokumentenaufbewahrung im Rahmen der DSGVO

Geschäftliche Unterlagen enthalten in aller Regel auch personenbezogene Daten. Diese werden von der DSGVO geschützt, sodass bei der Digitalisierung von archivierten Dokumenten auch datenschutzrechtliche Vorgaben zu beachten sind; insbesondere Aufbewahrungs- und Löschfristen sind zu nennen. Denn eine über den ursprünglichen Zweck (z. B. Abwicklung eines Vertrages, Bearbeitung einer Rechnung, etc.) hinausgehende Speicherung ist nur erlaubt, sofern hierfür eine Rechtsgrundlage existiert. Gängige Aufbewahrungspflichten für Unternehmen ergeben sich aus dem Handels- und Steuerrecht (in der Regel zwischen sechs und zehn Jahren für Geschäftsbriefe, Vertragsunterlagen, o. Ä.), aber auch Verjährungsfristen von Schadensersatzansprüchen (zwischen drei und 30 Jahren) sollten beachtet werden. Die Aufbewahrung ist jedoch stets abhängig von der jeweiligen konkreten Dokumentenart und daher für jedes Dokument im Einzelfall zu bestimmen und zu dokumentieren.

Nicht zuletzt müssen die allgemeinen Datenschutzgrundsätze beachtet werden: die Richtigkeit, Verfügbarkeit und Integrität (=Unveränderbarkeit) von personenbezogenen Daten sowie die Dokumentation der Datenverarbeitung sind zentrale Prinzipien der DSGVO. Diese sollen u. a. über sog. technisch-organisatorische Maßnahmen („TOM“, z. B. Zugriffsberechtigungen und -kontrollen) gewährleistet werden. Insofern ergeben sich Überschneidungen und damit auch Synergieeffekte mit den GoBD.

Geschäftsgeheimnissen in den Blick nehmen

Zuletzt sollten bei der Umsetzung einer digitalen Archivierung auch die Vorgaben aus dem GeschGehG beachtet werden. Diese wirken sich nicht unmittelbar auf die Archivierung aus, eine Implementierung in die Archivierungsprozesse kann aber einen effizienten Schutz von Geschäftsgeheimnissen gewährleisten. So muss insbesondere eine Identifizierung und Klassifizierung von Informationen als Geschäftsgeheimnis im Sinne des § 2 GeschGehG erfolgen, um gesetzlichen Schutz zu erhalten. Dazu bietet sich die Einführung folgender Prozesse an:

- Abschluss von aktuellen Vertraulichkeitsvereinbarungen mit den Geschäftspartnern, soweit noch Geschäftsbeziehungen bestehen
- Informationsklassifizierung nach Vertraulichkeitsgraden
- Definition von entsprechenden Berechtigungskonzepten in Abhängigkeit der Informationsklassifizierung

- Implementierung von entsprechenden Schutzmaßnahmen, z. B. technischer und organisatorischer Art (dies überschneidet sich mit den datenschutzrechtlichen Anforderungen zu TOM)
- Umsetzung einer organisatorischen Sensibilisierung, bspw. durch die Schulung von Mitarbeitern
- Zusammenfassung aller Maßnahmen zum Geheimnisschutz in einem Schutzkonzept.

Fazit

Eine rechtssichere Umsetzung eines digitalen Archivs bzw. einer digitalen Aktenverwaltung bietet letztlich die Möglichkeit, Ressourcen, Zeit und Geld zu sparen, da Mitarbeiter durch automatisierte Archivierungsprozesse ihre Verwaltungsaufgaben effizienter gestalten können. Zudem kann so auch die Arbeit im Homeoffice ermöglicht oder deutlich erleichtert werden.

Die Fülle an zu beachtenden Normen macht aber deutlich: Die bloße Anschaffung eines Scanners und Einstellung einer Bürokraft zur Digitalisierung von Akten reicht in der Regel nicht aus, um den vielfältigen gesetzlichen und technischen Vorgaben gerecht zu werden. Viele der Maßnahmen zur Einhaltung der GoBD, der DSGVO und des GeschGehG überschneiden sich jedoch. Sofern bei der Konzeption und Einführung der digitalen Archivierung alle gesetzlichen Anforderungen im Blick behalten werden, können daher – beispielsweise durch den Rückgriff auf Dokumentenmanagementsysteme – erhebliche Synergieeffekte erzielt und hohe Bußgelder (z. B. bei Datenschutzverstößen) vermieden werden.

Etablierter Standard für Cloud-Sicherheit: Der C5-Kriterienkatalog des BSI

Die Informationssicherheit spielt bei Cloudsystemen eine große Rolle. Je kritischer die Anwendungen und Daten, desto höher sind die Anforderungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen C5-Kriterienkatalog „Cloud Computing Compliance Criteria Catalogue“ aktualisiert, an dem sich Anwender und Cloud-Anbieter orientieren können. Auch rechtliche Fragestellungen rücken weiter in den Vordergrund.

Hintergrund

Im Kontext der fortschreitenden Digitalisierung setzen viele Unternehmen zunehmend auf Cloud-Computing. Bei der Auswahl eines Cloud-Anbieters müssen sich Anwender mangels eigener IT-Expertise oftmals auf etablierte Zertifikate verlassen. Das BSI gibt mit dem aktualisierten C5-Katalog eine Grundlage an die Hand, mit der die Cloud-Sicherheit besser bemessen werden kann. „C5“ bedeutet in Langform „Cloud Computing Compliance Criteria Catalogue“. Durch diesen Standard sollen Anbieter und Nutzer in die Lage versetzt werden, gängige Compliance-Anforderungen zu erfüllen. Von der Arbeit des BSI können nicht nur Cloud-Anbieter bei der Umsetzung und Bewertung der eigenen Cloud-Struktur, sondern auch Anwender bei der Beurteilung und Auswahl eines Anbieters profitieren.

Bündelung gängiger Zertifikate und Richtlinien in einem Werk

Der Kriterienkatalog C5 ist kein von Grund auf neues Werk, vielmehr nutzt und ergänzt der Katalog etablierte Prüfschemata und Richtlinien und deckt die nachfolgenden Zertifikate ab:

- ISO/IEC 27001
- CSA Cloud Controls Matrix 3.01 (CSA – Cloud Security Alliance)

- AICPA Trust Services Principles and Criteria 2014 (AICPA – American Institute of Certified Public Accountants)
- ANSSI Référentiel Secure Cloud v2.0 (Entwurf) (ANSSI – Agence nationale de la sécurité des systèmes d'information)
- IDW ERS FAIT 5 (Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud-Computing)
- BSI IT-Grundschutz-Kompendium
- BSI SaaS Sicherheitsprofile.

Der Kriterienkatalog C5 vereint durch die umfassende Abbildung gängiger Zertifikate diverse Mindestanforderungen für ein sicheres Cloud-Computing in einem Dokument, welches sich in erster Linie an professionelle Cloud-Anbieter sowie deren Prüfer und Kunden richtet. Für die verschiedenen Anforderungsbereiche (wie bspw. Compliance und Datenschutz) werden konkrete Zielsetzungen formuliert, wobei zur Umsetzung dieser Zielsetzungen jeweils konkrete Basisanforderungen festgelegt wurden. So müssen nachvollziehbare und transparente Systembeschreibungen mit bestimmten inhaltlichen Vorgaben vorgehhalten werden. Darin sollte u. a. festgehalten werden, welche Infrastruktur-, Netzwerk- und Systemkomponenten für Entwicklung und Betrieb des Cloud-Dienstes verwendet werden, welche Kontrollen und Maßnahmen sowie Prozesse für einen ordnungsgemäßen Betrieb und für den Fall von Ausnahmen des Regelbetriebs (z. B. bei Ausfällen oder Angriffen) vorgesehen sind oder auch die Konzeption und Verteilung von Rollen und Zuständigkeiten. Nicht zuletzt sollen auch Unterauftragnehmer, die Dienste erbringen oder Hardware liefern, in den Blick genommen werden.

Cloud-Anbieter sollen zudem nachvollziehbare und transparente Angaben machen zu

- Gerichtsbarkeit und Ort der Datenspeicherung, -verarbeitung und -sicherung
- Offenbarungs- und Ermittlungsbefugnissen staatlicher Stellen, die Zugriff auf Daten des Cloud-Kunden ermöglicht;
- vorhandenen und gültigen Zertifizierungen oder Bescheinigungen unabhängiger Dritter.

Die Bestimmung der Gerichtsbarkeit und der staatlichen Zugriffsmöglichkeiten ist häufig nicht auf den ersten Blick möglich, da relevante Regelungen nicht nur aus den Verträgen (bzw. AGB) zwischen Cloud-Anbieter und Cloud-Nutzer, sondern auch aus dem Vertragsverhältnis zwischen Cloud-Anbieter und dessen Unterauftragnehmern und Lieferanten folgen können. Hierüber können weitere vertragliche oder regulatorische Vorgaben (z. B. von Aufsichtsbehörden im Datenschutz oder dem Bank- und Finanzbereich), insbesondere aber auch staatliche/gesetzliche Besonderheiten (z. B. CLOUD-Act bei Bezug zu den USA) schnell eine Rolle spielen.

Der Nachweis, dass ein Cloud-Anbieter diese Anforderungen des Katalogs einhält und die Aussagen zur Transparenz korrekt sind, kann durch den Bericht nach dem Wirtschaftsprüferstandard ISAE 3402 bzw. IDW PS 951 erbracht werden.

Der überarbeitete Kriterienkatalog C5:2020

Nachdem sich der Kriterienkatalog C5 zum etablierten und vielfach national und international umgesetzten Standard der Cloud-Sicherheit entwickelte, wurde er im Jahr 2019 im Dialog mit Nutzern, Prüfern, Regulatoren und Cloud-Anbietern grundlegend überarbeitet und als neue Version am 21. Januar 2020 vorgestellt. Die Testierung nach C5 gemäß C5:2020 ist grundsätzlich den Wirtschaftsprüfungsgesellschaften vorbehalten. Die aktuelle Version des C5-Katalogs wurde auf den neuen Stand der Technik gebracht, ebenso wurden auch die Anforderungen des 2019 in Kraft getretenen EU Cybersecurity Act integriert. Im Einzelnen können die Erneuerungen in drei Gruppen unterteilt werden:

1. Zwei neue Bereiche für Sicherheitskriterien

Der neue Bereich Produktsicherheit berücksichtigt die Regelungen und Anforderungen des 2019 in Kraft getretenen EU Cybersecurity Act. Er bezieht sich, abweichend von den anderen Teile des C5-Katalogs, auf die Verwendung durch den Kunden der Cloud-Provider und nicht auf die Sicherheit der Cloud-Plattform selbst. Insofern wird gefordert, dass der Cloud-Anbieter Leitfäden zur sicheren Konfiguration des Dienstes bereitstellt. Ebenso werden Kriterien an das Session-Management formuliert, die u. a. die Identifikation von Schwachstellen des Cloud-Dienstes, Vertraulichkeit von Authentisierungsinformationen, Rollen- und Rechtekonzepte sowie Autorisierungsmechanismen umfassen.

Darüber hinaus wurde der Bereich „Umgang mit Ermittlungsanfragen staatlicher Stellen“ neu geregelt. Mit dem C5:2020 soll ein angemessener Umgang mit solchen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten (z. B. durch Anonymisierung oder Pseudonymisierung, sofern möglich) gewährleistet werden. Insofern müssen C5:2020-zertifizierte Cloud-Provider zwar auch weiterhin staatlichen Ermittlungsanfragen stattgeben und ihre Kunden ggf. nicht einmal über solche Anfragen informieren, allerdings sind sie im Gegenzug dazu verpflichtet, nachzuweisen, dass juristische Beurteilungen kompetent und korrekt erfolgen.

2. Überarbeitung von Sicherheitskriterien

Die bestehenden Sicherheitskriterien wurden zudem zum Teil grundlegend überarbeitet, um den Standard des Katalogs zu verbessern und aktuelle Entwicklungen in der Technik zu berücksichtigen. Als Beispiel nennt das BSI hier das Thema „DevOps“. Die Kriterien wurden zudem mit konkreten Hinweisen zur Prüfung im Rahmen von fortlaufenden Auditierungsverfahren versehen.

Eine weitere Neuerung stellt die Aufnahme sog. „korrespondierender Kriterien“ dar. Hierüber soll verdeutlicht werden, welche Verantwortung und Pflichten den Cloud-Kunden selbst treffen. Denn an den Schnittstellen von Cloud-Diensten muss auch der Kunde entsprechende Maßnahmen, z. B. zur IT-Sicherheit, treffen.

3. Ermöglichung einer direkten Prüfung

Das bislang im C5:2020 vorgesehene Prüfungsverfahren wurde außerdem um die Möglichkeit einer direkten IT-Prüfung erweitert. Musste der Cloud-Anbieter bisher vor einer Prüfung eigenständig eine Systembeschreibung erstellen und vorlegen, genügt es nun, wenn der Prüfer eine solche Beschreibung während des Prüfvorganges erstellt. Die Systembeschreibung umfasst dabei eine formale Beschreibung der eigenen Umgebung zusammen mit den ergriffenen Maßnahmen. Empfehlenswert ist die direkte Prüfung insbesondere für Cloud-Anbieter, die die vollständige Beschreibung des dienstleistungsbezogenen internen Kontrollsystems noch nicht abgeschlossen beziehungsweise ausreichend detailliert dargestellt haben.

Rechtliche Aspekte rücken weiter in den Vordergrund

Neben den rein operativen Überarbeitungen lässt sich somit feststellen, dass rechtliche Aspekte immer weiter in den Vordergrund rücken. Dies folgt aus den immer komplexeren und komplizierteren Voraussetzungen aus diversen Anforderungskatalogen, gesetzlichen Regulierungen und behördlichen Regelungen sowie letztendlich auch vertraglichen Vorgaben.

Am Anfang steht dabei eine solide vertragliche Grundlage sowohl seitens Cloud-Anbietern als auch Cloud-Anwendern. Diese sollte u. a. Themen wie Vertragslaufzeit, Kündigung, Haftung sowie die konkrete Leistungsbeschreibung (bzw. Service Level Agreements) abdecken, stets abhängig von der Kritikalität der zu verarbeitenden Daten und der Eigenschaften und Funktionen der zu betreibenden Anwendungen. Bereits hier müssen sich aber insbesondere Cloud-Anwender im Vorfeld Gedanken über spezifische gesetzliche oder regulatorische Grenzen machen. Ohne eine fundierte Kenntnis dieser Vorgaben droht der Abschluss von Vertragswerken, die nicht mit diesen Anforderungen übereinstimmen und daher sowohl von Auftraggebern als auch von Aufsichtsbehörden beanstandet werden könnten – bis hin zur Verweigerung der

Inbetriebnahme oder der Untersagung der Fortsetzung des Betriebs einer Cloud-Anwendung. Je nach Fortschritt der Planungen bzw. der Umsetzung kann die Korrektur solcher Fehler erhebliche Kosten nach sich ziehen, dieses Risiko sollte daher bereits im Vorfeld durch eine ausführliche rechtliche Analyse verringert werden.

Aber auch während des Betriebs von Cloud-Anwendungen muss die sich stetig weiter entwickelnde Rechtslage beobachtet werden, da der Gesetzgeber und die Verwaltung ihre Einschätzungen und Anforderungen regelmäßig den technischen Entwicklungen anpassen.

Nicht zuletzt muss auch ein (noch) stärkerer Fokus auf die fortlaufende rechtliche Bewertung von Anfragen der Verwaltung, von Aufsichtsbehörden oder auch Mitarbeitern und Kunden gelegt werden. Neben der im C5:2020 erwähnten Beurteilung von staatlichen Ermittlungsanfragen sind hier insbesondere auch datenschutzrechtliche Themen (Datenpannen, Anfragen zu Auskunft, Löschung; etc.) von Relevanz.

Unser Kommentar

Der C5:2020 bietet eine gute und bewährte Grundlage, die immer komplexer werdenden Sicherheitsanforderungen, die an das Cloud-Computing und der damit verbundenen Compliance gestellt werden, zu erfüllen. Auch wenn das Verfahren nach dem Kriterienkatalog C5 derzeit nicht nach ISAE 3000 akkreditiert ist und somit Zertifizierungen gemäß Art. 42 f. DSGVO noch nicht möglich sind, darf die Bedeutung des Katalogs nicht unterschätzt werden. Denn er umfasst nicht nur gängige Zertifizierungen wie ISO/IEC 27001, sondern wird von vielen Behörden auch als Grundlage für eigene regulatorische Werke, Standards und Maßnahmen herangezogen. Sowohl Cloud-Anbietern als auch Cloud-Anwendern ist daher zu empfehlen, dieses Werk zu beachten – entweder durch eine unmittelbare Zertifizierung, zumindest aber als Orientierung bei der Umsetzung eigener Prozesse. Dadurch besteht die Chance, die immer stärkere Regulierung und die stetig steigende Relevanz von rechtlichen Aspekten beim Betrieb bzw. der Nutzung von Cloud-Services rechtskonform umzusetzen und entsprechende Compliance-Risiken zu vermindern.

Änderungen im MarkenG zum 1. Mai 2020 – Neue Alternative zur Erklärung des Verfalls und der Nichtigkeit

Zum 1. Mai 2020 traten die letzten Änderungen des Markenrechtsmodernisierungsgesetzes (MaMoG) in Kraft. Durch ein neues Verfalls- und Nichtigkeitsverfahren vor dem Deutschen Patent- und Markenamt (DPMA) wird eine Alternative zur Klage vor den ordentlichen Gerichten eingeführt. Dies kann als die bedeutendste verfahrensrechtliche Änderung des MaMoG – und somit der letzten Jahre – angesehen werden.

Hintergrund

Das MaMoG trat – bis auf wenige Ausnahmen – am 14. Januar 2019 in Kraft. Es dient der Umsetzung der EU-Markenrechtsrichtlinie 2015/2436 in das deutsche Recht. Wir hatten hierzu bereits im vergangenen Jahr ausführlich zu den bevorstehenden Änderungen in unserem Blog berichtet und die damaligen Änderungen bereits umfassend zusammengefasst.

Nach Art. 5 Abs. 3 MaMoG traten am 1. Mai 2020 die letzten Änderungen in Kraft. Diese beziehen sich auf die Neuregelungen der §§ 53 f. MarkenG. Hintergrund der §§ 53 f. MarkenG n. F. ist Art. 45 Abs. 1 der EU-Markenrechtsrichtlinie 2015/ 2436. Dieser sieht vor, dass die einzelnen Mitgliedsstaaten neben der Einlegung von Rechtsmitteln auch ein effizientes und zügiges Verwaltungsverfahren für die Erklärung der Nichtigkeit und des Verfalls zur Verfügung stellen müssen.

Wen betrifft die Änderung?

Die Änderungen betreffen jeden, der vor der Gesetzesänderung ausschließlich die Möglichkeit eines Löschungsverfahrens vor den ordentlichen Gerichten gehabt hätte.

Seit dem 1. Mai 2020 können nun – durch gem. § 53 Abs. 2 MarkenG n. F. benannte Personen und Interessenverbände – in einem Verfalls- bzw. Nichtigkeitsverfahren gem. § 53 MarkenG vor dem DPMA auch relative Schutzhindernisse (ältere Rechte) als Nichtigkeitsgrund geltend gemacht werden. Bisher war dies nur für absolute Schutzhindernisse möglich.

Dieses amtliche Verfahren ist dabei nicht zwingend. In § 53 Abs. 1 S. 1 MarkenG n. F. ist ausdrücklich geregelt, dass ein Wahlrecht zwischen dem Verwaltungsverfahren und dem Klageweg besteht. **Nicht möglich ist es jedoch, beide Verfahren parallel zu betreiben.** Der § 53 Abs. 1 S. 4 - 6 MarkenG n. F. schließt parallele Verfahren über denselben Streitgegenstand aus. Damit dies in praktischer Hinsicht vermieden wird, werden Anträge auf Erklärung des Verfalls oder der Nichtigkeit einer eingetragenen Marke sowie entsprechende Klagen gem. § 25 Nr. 24 MarkenV in das Register beim DPMA eingetragen.

Zu beachten ist außerdem die Übergangsvorschrift des § 158 Abs. 6 MarkenG n. F.. Demnach sind bei Anträgen auf Löschung einer eingetragenen Marke wegen Verfalls, welche vor dem 14. Januar 2019 gestellt worden sind, sowie bei entsprechenden Löschungsklagen wegen Verfalls oder älterer Rechte die §§ 49 Abs. 1, 51 Abs. 4 Nr. 1, 55 Abs. 3 und 26 MarkenG in ihrer jeweils alten Fassung – vor dem MaMoG – anzuwenden. In diesen Fällen kann u. a. eine Löschung der Marke wegen Nichtigkeit nicht durch das „neue Verwaltungsverfahren“ erreicht werden. Das o. g. Wahlrecht besteht insofern nicht.

Welche (neuen) Anforderungen werden gestellt?

Das neue Verfahren ist vor dem DPMA zu beantragen. Der Antrag ist nach Satz 1 schriftlich zu stellen und muss nach Satz 2 die zur Begründung dienenden Tatsachen und Beweismittel beinhalten. Antragsberechtigt sind nach § 53 Abs. 2 MarkenG n.F. jede natürliche oder juristische Person sowie jeder Interessenverband von Herstellern, Erzeugern, Dienstleistungsunternehmern, Händlern oder Verbrauchern, der am Verfahren beteiligt sein kann.

Um den o. g. Anforderungen zu entsprechen, sollte für den Antrag das auf der Homepage des DPMA zu findende Formular verwendet werden. Insgesamt sind für dieses Verfahren EUR 400 zu entrichten, wobei sich diese Gebühr aus einer Einreichungsgebühr von 100 Euro und – im Falle eines Wiederspruches – einer Weiterverfolgungsgebühr von EUR 300 zusammensetzt.

Unser Kommentar

Durch die oben aufgezeigten Änderungen besteht nun ein Wahlrecht zwischen einem Verfahren vor dem DPMA und einem Verfahren vor den ordentlichen Gerichten. Hierbei kann mit Spannung erwartet werden, für welchen Weg sich die Berechtigten entscheiden werden. Für das neue Verfahren spricht dabei die günstige Gebühr von lediglich EUR 400 und die unbestrittene Sachkenntnis der Mitarbeiter des DPMA, die über den Antrag zu entscheiden haben. Zudem soll dieses Verfahren – zumindest nach dem Sinn und Zweck des Gesetzgebers – effizient und zügig sein. Ob dieser Sinn und Zweck auch in der Praxis erreicht wird, bleibt dabei abzuwarten.

Die neue Wahlmöglichkeit ist aus Praktikersicht vollumfänglich zu begrüßen, da sie keinerlei Nachteile mit sich bringt. Insgesamt erfolgt durch das MaMoG eine weitere notwendige und richtige Harmonisierung im Markenrecht, dessen Anfänge bereits 1988 in der ersten europäischen Markenrechtsrichtlinie lagen.

Halloumi – Ein Grillkäse vor Gericht: EuGH zur Verwechslungsgefahr von „Halloumi“ und „BBQLOUMI“

Die Inhaberin der Unionskollektivmarke „Halloumi“ ist im Streit um die Eintragung der Unionsmarke „BBQLOUMI“ bis vor den Europäischen Gerichtshof (EuGH) gezogen. Dort hat die Klägerin einen Etappensieg erzielt: Der EuGH hat das Verfahren an das Gericht der Europäischen Union (EuG) zurückverwiesen, da dieses die Verwechslungsgefahr nicht ausreichend geprüft habe.

Urteil vom 5. März 2020, Az. C-766/18 P

Die „Stiftung zum Schutz des traditionellen zyprischen Käses namens Halloumi“ ist seit etwa 20 Jahren Inhaberin der u. a. für Käse eingetragenen Unionskollektivmarke „Halloumi“. Im Jahr 2014 hat ein bulgarisches Unternehmen den Namen seines eigenen Grillkäses – „BBQLOUMI“ – als Unionsmarke u. a. für Käse eintragen lassen. Hierin sah die Stiftung eine Verletzung ihrer Markenrechten und legte Widerspruch gegen die Markeneintragung beim Amt der Europäischen Union für geistiges Eigentum (EUIPO) ein.

Das Amt hat jedoch den Widerspruch – und später auch die gegen den Widerspruch eingereichte Beschwerde – mangels Verwechslungsgefahr mit der älteren Kollektivmarke „Halloumi“ zurückgewiesen. Gegen diese Entscheidung hat die „Halloumi-Stiftung“ sodann Klage vor dem EuG erhoben – bislang jedoch ohne Erfolg.

Das EuG hat die Auffassung vertreten, dass dem Kennzeichen „Halloumi“ lediglich eine beschreibende Bedeutung zukomme, da es eine Käsesorte beschreibe und der Begriff zudem nur eine schwache Unterscheidungskraft aufweise. Deshalb würden die streitgegenständlichen Marken aufgrund des geringen Grads der bildlichen, klanglichen und begrifflichen Ähnlichkeit – trotz teilweise identischer und teilweise ähnlicher Waren – keine Verwechslungsgefahr bei den maßgeblichen Verkehrskreisen hervorrufen. Die Klage wurde folglich abgewiesen.

Daraufhin hat die Stiftung Rechtsmittel auch gegen diese Entscheidung eingelegt.

Die Entscheidung

Am 5. März 2020 hat der EuGH entschieden, dass die Vorinstanz die Verwechselungsgefahr der streitigen Marken nicht ausreichend geprüft habe. Anders als das EuG geht der Gerichtshof davon aus, dass die schwache Unterscheidungskraft einer älteren Marke das Vorliegen einer Verwechslungsgefahr nicht ausschließe. Nach Ansicht des EuGH soll die Rechtsprechung zu den Kriterien, anhand derer bei Unionsindividualmarken konkret zu beurteilen sei, ob eine solche Gefahr besteht, auch auf Rechtssachen übertragbar sein, die eine ältere Kollektivmarke betreffen. Eine Unionskollektivmarke ist eine Markenart, die auf eine betriebliche Herkunft einer bestimmten Ware oder Dienstleistung hinweist, indem sie den Verbraucher darüber informiert, dass der Hersteller der Ware bzw. der Dienstleistungserbringer einem bestimmten Verband angehört und berechtigt ist, die Marke zu benutzen. Die Merkmale von Unionskollektivmarken können also nicht zur Rechtfertigung herangezogen werden, um von den Kriterien zur Beurteilung der Verwechslungsgefahr abzuweichen. Vielmehr müsse das Bestehen der Verwechslungsgefahr unter Einbeziehung aller relevanten Umstände des Einzelfalls beurteilt werden. Aus diesem Grund hätte das EuG prüfen müssen, ob der geringere Ähnlichkeitsgrad der einander gegenüberstehenden Marken durch den höheren Ähnlichkeitsgrad bzw. die Identität der mit ihnen gekennzeichneten Waren ausgeglichen werde.

Da das EuG die Verwechselungsgefahr nicht umfassend unter Einbeziehung aller relevanten Faktoren geprüft habe, unterliege die Entscheidung einem Rechtsfehler. Aus diesem Grund hat der EuGH die Entscheidung aufgehoben und den Sachverhalt zur erneuten Überprüfung des Vorliegens einer Verwechslungsgefahr an das Gericht zurückverwiesen. Es bleibt abzuwarten, wie das Gericht in dieser Rechtssache entscheiden wird.

Unser Kommentar

Die Klarstellung des EuGH, dass die auf Individualmarken anzuwendenden Kriterien zur Beurteilung der Verwechslungsgefahr auch für Kollektivmarken gelten, ist zu begrüßen. Zwar enthält das Urteil keine neuen Erkenntnisse zur Beurteilung der Verwechslungsgefahr als solche, es stärkt jedoch die Rechte der Inhaber von Kollektivmarken, da Gerichte nunmehr auch bei Kollektivmarken die Verwechslungsgefahr anhand sämtlicher für den konkreten Einzelfall relevanten Umstände bewerten müssen.

BGH: Prüfung der Unterscheidungskraft eines Markenzeichens (#darferdas?)

Mit Beschluss vom 30. Januar 2020 hat der Bundesgerichtshof (BGH) festgestellt, dass bei der Prüfung der Unterscheidungskraft im Eintragungsverfahren einer Marke sämtliche praktisch bedeutsamen und naheliegenden Verwendungsformen des Zeichens miteinbezogen werden müssen. Einzig in Fällen, in denen in der betroffenen Branche lediglich eine einzige Verwendungsart praktisch bedeutsam ist, kann die Prüfung auf diese wahrscheinlichste Verwendung reduziert werden.

BGH, Beschluss vom 30. Januar 2020 – I ZB 61/1

Hintergrund

Am 17. November 2015 hat die Klägerin die Wortmarke „#darferdas?“ beim Deutschen Patent- und Markenamt (DPMA) für Waren der Klasse 25 (Bekleidungsstücke, insbesondere T-Shirts, Schuhwaren, Kopfbedeckungen) angemeldet. Die Markenanmeldung wurde jedoch im Rahmen des Eintragungsverfahrens vom DPMA wegen mangelnder Unterscheidungskraft des Zeichens (§ 8 Abs. 2 Nr. 1 MarkenG) zurückgewiesen.

Auch die von der Klägerin daraufhin eingereichte Beschwerde beim Bundespatentgericht (BPatG) blieb erfolglos (Beschluss vom 3. Mai 2017 – 27 W (pat) 551/16). Die zuständigen Richter haben sich vielmehr der Auffassung des Amtes angeschlossen und die Markenanmeldung wegen fehlender Unterscheidungskraft abgelehnt. Nach Auffassung des BPatG handele es sich bei der Bezeichnung „#darferdas?“ um eine als Frage formulierte Wortfolge gebräuchlicher Wörter der deutschen Sprache, die durch den Hashtag zur Diskussion auffordern soll. Deshalb nehme der Verkehr diese Frage als Aufdruck auf der Vorder- oder Rückseite von Bekleidungsstücken lediglich als dekoratives Element, nicht aber als Herkunftshinweis wahr.

Mit eingelegter Rechtsbeschwerde verfolgte die Klägerin ihr Eintragungsbegehren vor dem BGH weiter. Nach Ansicht des zuständigen Senats sei nicht auszuschließen, dass die Verwendung des Zeichens „#darferdas?“ als Aufdruck auf der Vorder- oder Rückseite von Kleidungsstücken nur eine von mehreren Verwendungsformen darstelle. Ebenso könne das Zeichen nämlich auf einem Etikett in der Innenseite des Bekleidungsstückes angebracht und somit als Herkunftshinweis wahrgenommen werden. Nach der Rechtsprechung des BGH genüge es, wenn naheliegende und praktisch bedeutsame Verwendungsmöglichkeiten bestehen, infolge derer das Zeichen vom Verkehr ohne Weiteres als Herkunftshinweis verstanden werde. Die Karlsruher Richter zweifelten jedoch an der Vereinbarkeit dieser Rechtsprechung mit den einschlägigen unionsrechtlichen Regelungen und legten deshalb dem Gerichtshof der Europäischen Union (EuGH) folgende Frage zur Auslegung vor: „*Hat ein Zeichen Unterscheidungskraft, wenn es praktisch bedeutsame und naheliegende Möglichkeiten gibt, es für die Waren oder Dienstleistungen als Herkunftshinweis zu verwenden, auch wenn es sich dabei nicht um die wahrscheinlichste Form der Verwendung des Zeichens handelt*?“ (BGH, Beschluss vom 21. Juni 2018 – I ZB 61/17).

Mit Urteil vom 12. September 2019 bejahte der EuGH die Vorlagefrage im Grundsatz und verwies die Sache zurück nach Karlsruhe. Nach Auffassung der Luxemburger Richter sei die Unterscheidungskraft eines angemeldeten Zeichens unter Berücksichtigung aller relevanten Tatsachen und Umstände, einschließlich sämtlicher wahrscheinlicher Verwendungsarten der angemeldeten Marke zu prüfen. Wahrscheinliche Verwendungsarten seien dabei solche, die in der Branche üblich und praktisch bedeutsam sein können. Ein Markenanmelder müsse jedoch bei Anmeldung der Marke noch nicht genau wissen, wie er das Zeichen künftig benutzen wird. Bei der Prüfung der Unterscheidungskraft solle in diesen Fällen an das angeknüpft werden, was in der entsprechenden Branche üblich ist. Dabei müsse jede in Betracht kommende praktische Verwendungsart daraufhin überprüft werden, ob der Verkehr das Zeichen als Herkunftshinweis auffasst (EuGH, Urteil vom 12. September 2019 – C-541/18).

Die Entscheidung

Unter Beachtung dieser Grundsätze stellte der BGH daraufhin fest, dass die Auffassung des BPatG, dass es der angemeldeten Marke für die betroffene Waren an Unterscheidungskraft fehle, einer rechtlichen Nachprüfung nicht standhalte. Das BPatG sei unzutreffend davon ausgegangen, dass bei Prüfung der Unterscheidungskraft auf die wahrscheinlichste Verwendungsform des angemeldeten Zeichens abzustellen sei.

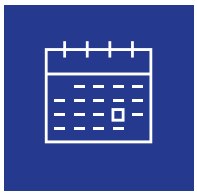
Deshalb habe das BPatG die Zeichenfolge „#darferdas?“ lediglich als sichtbaren Aufdruck auf der Vorder- oder Rückseite von Bekleidungsstücken, Kopfbedeckungen oder Schuhwaren, der Beurteilung zugrunde gelegt. Andere weniger wahrscheinliche und praktisch bedeutungslosere Verwendungsmöglichkeiten, wie z. B. die Verwendung des angemeldeten Zeichens auf Warenetiketten im Inneren des Bekleidungsstücks, haben die Richter des BPatG hingegen außer Acht gelassen.

Die Karlsruher Richter argumentierten, dass der Verkehr ein Zeichen auf einem Bekleidungsstück je nach Art und Platzierung sowohl als Herkunftshinweis aber auch als dekoratives Element wahrnehmen kann und deshalb eine Beurteilung der Unterscheidungskraft anhand der Umstände des Einzelfalls erfolgen müsse. Dafür seien insbesondere die Kennzeichnungsgewohnheiten im maßgeblichen Warensektor relevant. Der BGH weist in seiner Entscheidung ferner darauf hin, dass grundsätzlich solche Verwendungsarten, die in der betreffenden Branche zwar denkbar, aber praktisch bedeutungslos und somit unwahrscheinlich erscheinen, für die Prüfung der Unterscheidungskraft irrelevant seien. Sofern der Markenanmelder jedoch konkrete Anhaltspunkte geliefert hat, die eine unübliche Verwendungsart wahrscheinlich machen, gelte es von diesem Grundsatz abzuweichen, so die Richter. Im Übrigen könne die Prüfung der Unterscheidungskraft nur dann auf die wahrscheinlichste Verwendungsform beschränkt werden, wenn in der betreffenden Branche nur eine Verwendungsart von praktischer Bedeutung ist. Deshalb hob der BGH den Beschluss auf und verwies die Sache zurück an das BPatG. Im wiedereröffneten Beschwerdeverfahren soll das BPatG nun überprüfen, ob der Verkehr das Zeichen „#darferdas?“ unter Berücksichtigung der verschiedenen Verwendungsarten – insbesondere auch auf dem Etikett eines Kleidungsstücks – als Herkunftshinweis auffassen könnte.

Unser Kommentar

Insbesondere im Bereich der Bekleidungsstücke stellt sich immer wieder die Frage, ob Aufdrucke sogenannter „Fun-Sprüche“ markenrechtliche Unterscheidungskraft besitzen. Oftmals geben solche Zeichen keinen Hinweis auf die Herkunft der Ware, sondern sind rein dekorativer Natur. Daneben besteht die – wenn auch ungewöhnlichere – Möglichkeit, den Spruch auf einem Etikett in der Innenseite des Kleidungsstücks anzubringen, auf dem meist Angaben zum Hersteller zu finden sind. Bislang ging der EuGH davon aus, dass die Unterscheidungskraft eines Zeichens abzulehnen ist, sofern die wahrscheinlichste Benutzungsform nicht markenmäßig ist, obgleich in der jeweiligen Branche weitere praktisch bedeutsame markenmäßige Verwendungsarten existieren. Nun hat sich die Auffassung des Gerichtshofs jedoch gewandelt: Mit dem vorliegenden Urteil erkennt der EuGH sämtliche Verwendungsformen der betreffenden Branche als relevant an. Dementsprechend kann auch die Benutzungsmöglichkeit eines „Fun-Spruches“ in der Bekleidungsbranche auf dem Einnähetikett ausreichen, um die Unterscheidungskraft eines Zeichens wie „#darferdas?“ zu bejahen. Es bleibt nun abzuwarten, wie das BPatG die Vorgaben des EuGH und des BGH in die Praxis umsetzen wird.

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: Getty Images/MR.Cole_Photographer: Seite 1; istock.com/Rawf8: Seite 3; istock.com/Traitov: Seite 5; istock.com/Dilok Klaisataporn: Seite 6; istockphoto.com/Warchi: Seite 9; istock.com/etiennevoss: Seite 10; istockphoto.com/foto-ianniello: Seite 12

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.

Aus Gründen der besseren Lesbarkeit verzichten wir auf die gleichzeitige Verwendung geschlechterspezifischer Sprachformen. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat redaktionelle Gründe und beinhaltet keine Wertung.

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 2019 AWARDS
Kanzlei des Jahres

Rechts- und Steuerberatung | www.luther-lawfirm.com