50. Jahrgang
datenschutz-berater.de
DSB 04/2026

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

Service

ISSN 0170-7256

dfv Mediengruppe

Dr. Carlo Piltz und Ilia Kukin

Werbung mit „DSGVO-konform“: Wo liegen die Grenzen des Zulässigen?

Die Werbung mit Datenschutz-Compliance ist vor allem im Softwaremarkt oder bei Cloud- und Online-Diensten allgegenwärtig. Doch was bedeutet „DSGVO-konform“ eigentlich und wann wird eine solche Aussage lauterkeitsrechtlich problematisch? Das Zertifizierungsregime der DSGVO ist bis heute kaum praxistauglich und der Markt behilft sich mit freien Siegeln und eigenen Prüfstandards. Der Beitrag ordnet die bestehenden Zertifizierungsmechanismen ein und zeigt auf, wo die wettbewerbsrechtlichen Grenzen pauschaler Konformitätsaussagen liegen.

Die Aussage „unsere Software ist DSGVO-konform“

Mit dem Versprechen, dass eine Lösung „DSGVO konform“ sei, werben zahlreiche Anbieter von Software und Cloud-Diensten. Auch im KI-Bereich bezeichnen insbesondere kleinere Anbieter ihre Lösungen in Werbematerialien als „100 % DSGVO-konform“. Diese Aussage wird häufig zur Abgrenzung zu Modellen großer Unternehmen getroffen – wie etwa OpenAI oder Anthropic – deren Einsatz im Geltungsbereich der DSGVO je nach Verwendungszweck und Konfiguration mit erheblichen datenschutzrechtlichen Risiken verbunden sein kann. Was hinter solchen Werbeaussagen steht, ist nicht immer leicht herauszufinden. Die DSGVO kennt zwar ein eigenes Zertifizierungsregime, doch die dafür vorgesehenen Mechanismen sind bis heute kaum operabel. Was der Markt stattdessen bietet, ist ein Nebeneinander aus akkreditierten Gütesigeln, branchenintern Eigenkreationen und bloßen Marketingaussagen. In einigen Fällen werden Zertifizierungen aus anderen Bereichen herangezogen, um DSGVO-Compliance als Wettbewerbsvorteil zu vermarkten, auch wenn sie nur einen Teil der DSGVO-Anforderungen abdecken.

Wer als Anbieter mit Datenschutz-Compliance wirbt, muss nicht nur die Grenzen der jeweiligen Zertifizierungen kennen, sondern auch die wettbewerbsrechtlichen Grenzen pauschaler oder inhaltlich nicht gedeckter Aussagen im Blick haben. Nachfolgend werden die Zertifizierungen nach der DSGVO im Überblick dargestellt, ihr Anwendungsbereich eingeordnet und die lauterkeitsrechtlichen Grenzen von Werbeaussagen beleuchtet.

Zertifizierungen nach DSGVO

Art. 42 DSGVO enthält den generellen Rahmen für Zertifizierungen nach der DSGVO. Die Vorgaben sind denkbar abstrakt gehalten. Den Mitgliedstaaten, den Aufsichtsbehörden und der Kommission wird keine Verpflichtung auferlegt, Zertifizierungskriterien oder -mechanismen zu entwickeln. Vielmehr sind sie angehalten, die Einführung datenschutzspezifischer Prüfverfahren, Siegel und Zeichen zu fördern, die DSGVO-Compliance ausweisen. Nach welchen Kriterien Zertifizierungsverfahren zu genehmigen sind, regelt die Vorschrift nicht. Sie ist (wie von der Konferenz der deutschen Datenschutzbehörden im Kurzpapier Nr. 9 zutreffend feststellt) nur ein rechtlicher Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, aber zu unbestimmt, um auf ihrer Basis allein konkrete Mechanismen zu entwickeln. Dieser Umstand ist der Kommission und dem Europäischen Datenschutzausschuss (EDSA) seit Jahren bekannt. Der EDSA hat daher bereits 2018 die Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien veröffentlicht (EDSA, Leitlinien 1/2018, V. 3.0) und darin die Anforderungen an DSGVO-Zertifizierungsverfahren konkretisiert. Weitere Präzisierungen erfolgten mit den Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen nach Art. 43 DSGVO (EDSA, Leitlinien 4/2018, V. 3.0) sowie 2023 mit den Leitlinien 7/2022 über Zertifizierungen als Instrument für Übermittlungen in Drittstaaten (EDSA, Leitlinien 7/2022, V. 2.0).

Können Unternehmen sich nach der DSGVO zertifizieren lassen? Grundsätzlich ja, allerdings mit einigen Einschränkungen. Eine Zertifizierung bezieht sich stets auf konkrete Verarbeitungsvorgänge, nicht auf das Unternehmen insgesamt. Zudem genügt eine Zertifizierung allein nicht als Nachweis der DSGVO-Konformität, sondern ist lediglich ein Indiz für die Einhaltung der Vorgaben (EDSA, Leitlinien 1/2018, V. 3.0, Rn. 13). In Bußgeldverfahren führen weder eine Zertifizierung noch der Umstand, dass die eingesetzte Software als „DSGVO-konform“ beworben wird, zu einer Exkulpation des Unternehmens (so auch HessBfDI, Tätigkeitsbericht 2021, S. 133). Hinzu kommt ein praktisches Problem: Der Markt akkreditierter Zertifizierungen ist nach wie vor dünn. In Deutschland operieren derzeit zwei akkreditierte Zertifizierungsstellen, die im Suchportal der Deutschen Akkreditierungsstelle zu finden sind. Eine weitere Zertifizierungsstelle befindet sich im Akkreditierungsverfahren. Der stagnierende Markt der Zertifizierungen dürfte weniger auf fehlendes Interesse zurückzuführen sein als auf die lange Dauer des Akkreditierungsverfahrens. Das spiegelt sich in der großen Zahl von An-

bietern wider, die sog. freie Datenschutzsiegel vergeben. Diese haben sich als Alternative zu akkreditierten Zertifizierungen etabliert (siehe auch Bauer, DSB 2024, 196). Unternehmen werden nach eigenen Kriterien der jeweiligen Zertifizierungsstelle geprüft und erhalten bei positivem Ergebnis eine Bestätigung der DSGVO-Konformität. Solche freien Datenschutzsiegel sind aus datenschutzrechtlicher Sicht nicht per se verboten, da die DSGVO andere Siegel nicht verbietet. Auch wettbewerbsrechtlich ist ihre Verwendung erst einmal eher unbedenklich, solange ausdrücklich auf die Zertifizierungskriterien des Ausstellers verwiesen und transparent kommuniziert wird, dass das Verfahren kein genehmigtes Verfahren im Sinne der Art. 42 und 43 DSGVO ist.

Wettbewerbsrechtliche Aspekte

Die entscheidenden Fragen der Zulässigkeit liegen auf der lauterkeitsrechtlichen Ebene, und zwar sowohl für Anbieter von Siegeln als auch für Unternehmen, die sich in ihrer Werbung auf erhaltene Zertifizierungen oder eine DSGVO-Konformität berufen. Beide können durch solche Werbung unlauter handeln. Um in den Anwendungsbereich des UWG zu gelangen, muss eine geschäftliche Handlung vorliegen. Diese ist stets unproblematisch gegeben, solange die Äußerung bzgl. der DSGVO-Konformität nach außen gerichtet und damit marktbezogen ist – also etwa auf einer Webseite oder einem Whitepaper, welches (potentielle) Kunden adressiert.

Irreführende Werbung

§ 5 UWG verbietet irreführende geschäftliche Handlungen. Gemeint sind damit Angaben, die entweder unwahr oder aus sonstigen Gründen zur Täuschung geeignet sind. Es müssen also zunächst Angaben (dies sind inhaltlich nachprüfbare Tatsachenbehauptungen) vorliegen. Nach der Rechtsprechung des BGH (BGH, Urt. v. 30.1.1963 – Ib ZR 183/61) ist der Begriff der Angabe im Sinne des UWG möglichst weit zu ziehen und erfasst jede Aussage, die auf ihren Inhalt hin nachprüfbar ist. Damit sind sämtliche Aussagen erfasst, die sich auf die DSGVO-Konformität beziehen. Sei es die Verwendung eines Konformitätssiegels oder bloße Angaben wie „unsere Software ist DSGVO-konform". Denn die Einhaltung rechtlicher Vorgaben (hier: der DSGVO) ist sicher nachprüfbar. Dass die Angaben zum Datenschutz die Verbraucher oder sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung veranlassen können, wird durch diverse Studien belegt (z. B. Cisco 2024 Data Privacy Benchmark Study). Bei Unternehmen ist auch bereits aufgrund der Verpflichtung in Art. 28 Abs. 1 DSGVO zur ordentlichen Auswahl von Auftragsverarbeitern davon auszugehen, dass die Angaben zum Datenschutz (genauer gesagt zu hinreichenden Garantien, dass die Verarbeitung im Einklang mit der DSGVO erfolgt) für die Entscheidung über den Vertragsschluss mit dem ein oder anderen Dienstleister wesentlich sind.

Unwahre Angaben

Eine Aussage zur hundertprozentigen DSGVO-Konformität wird typischerweise als Gesamtaussage über das Produkt und dessen Betrieb verstanden. Also dass sämtliche datenschutzrechtlichen Anforderungen vollständig und dauerhaft erfüllt sind. Dies kann aber aus mehreren Gründen objektiv unzutreffend und damit unwahr sein.

In der Realität dürfte es kaum Unternehmen geben, die DSGVO-Anforderungen immer absolut und vollständig erfüllen. Selbst wenn man unterstellt, dass das Unternehmen die Vorgaben weitgehend einhält, bleiben die (Unter-)Auftragsverarbeiter als Risikoquelle. Auch die Natur der DSGVO selbst spricht gegen solche Aussagen: Die Verordnung ist kein statischer Anforderungskatalog, sondern wird u. a. durch Behördenpositionen und den Stand der Technik ständig weiterentwickelt. Das erfordert laufende Beobachtungen und Anpassungen. Ob die DSGVO-Konformität gegeben ist, ist daher in der Regel keiner abschließenden und verifizierbaren Beurteilung zugänglich. Hinzu kommen teils erhebliche Diskrepanzen in der Auslegung zwischen den Aufsichtsbehörden. Als Beispiel kann die Zulässigkeit der sog. Warenkorberinnerungen mit oder ohne Einwilligung dienen. Die Sächsische Datenschutzaufsichtsbehörde bejaht die Möglichkeit, Daten hierfür ohne Einwilligung zu verwenden, während die Behörden aus Hessen und Nordrhein-Westfalen diese Form von Werbung ohne Einwilligung als unzulässig ablehnen. Die Pflichten der DSGVO sind zudem zwischen Verantwortlichem und Auftragsverarbeiter verteilt, sodass die Konformität ohne Berücksichtigung der jeweils anderen Partei nicht pauschal festgestellt werden kann. Das gilt umso mehr im Bereich der gemeinsamen Verantwortlichkeit.

Schließlich fehlt es an einem anerkannten Prüfmaßstab. Zertifizierungen nach Art. 42 DSGVO haben einen eng begrenzten Anwendungsbereich und bewerten nicht die Unternehmenscompliance insgesamt, sondern nur konkrete Datenverarbeitungsprozesse. Im Graubereich der „freien Siegel" sind die Bewertungskriterien oft intransparent oder decken nicht sämtliche Aspekte der DSGVO ab.

Werbung mit Selbstverständlichkeiten

Selbst, wenn man annimmt, dass eine Aussage wie etwa „100 % DSGVO-konform" zutrifft, stellt sich aus wettbewerbsrechtlicher Sicht das nächste Problem. Denn Werbung mit Selbstverständlichkeiten ist eine besondere Form der irreführenden geschäftlichen Handlung. Auch objektiv richtige Angaben können unzulässig sein, wenn die beworbenen Eigenschaften gesetzlich vorgeschrieben sind und besonders hervorgehoben werden. Solche Eigenschaften dürfen nicht als Vorteil der beworbenen Ware oder Dienstleistung dargestellt werden. Ob die Werbung mit DSGVO-Compliance als Werbung mit Selbstverständlichkeiten einzuordnen ist, bedarf einer differenzierten Be-

trachtung. Einerseits gilt die DSGVO unmittelbar für alle Verantwortlichen und Auftragsverarbeiter in ihrem Anwendungsbereich. Die Regelungen der DSGVO sind zwingende gesetzliche Vorgaben. Eine Werbung mit DSGVO-Konformität legt eine Differenzierung nahe, die rechtlich nicht existiert. Wer die gesetzlichen Anforderungen erfüllt, erbringt keine besondere Leistung, die eine werbliche Hervorhebung rechtfertigt, sondern tut nur das, was von ihm verlangt wird. Das Unternehmen hält sich an ein Gesetz.

Auf der anderen Seite lässt sich einwenden, dass die Rechtspflicht nicht mit dem Marktstandard gleichzusetzen ist. In einem Markt, in dem viele Anbieter ihre gesetzlichen Pflichten nicht erfüllen, ist die Compliance keine Selbstverständlichkeit. Das werbende Unternehmen könnte auf seine Konkurrenz verweisen, die auf die Einhaltung der DSGVO wenig Wert legt, und damit den Vorwurf der Werbung mit Selbstverständlichkeiten abschwächen. Zudem legt Art. 42 DSGVO nahe, dass DSGVO-Compliance als nachweisbares und kommunizierbares Merkmal konzipiert ist, mit dem ein Unternehmen auch nach außen auftreten darf.

Mehrdeutige Aussagen

Schließlich verbietet § 5 UWG mehrdeutige und missverständliche Aussagen. Eine Aussage gilt also auch als irreführend, wenn ein erheblicher Teil des Verkehrs sie in einem Sinne versteht, der nicht den objektiven Gegebenheiten entspricht. Spätere Richtigstellungen oder Klarstellungen im weiteren Verlauf der Werbung lassen die Irreführung nicht entfallen. Die Werbung mit DSGVO-Konformität lässt sich auf mindestens drei Weisen verstehen. Als Aussage über das Produkt selbst, als Aussage über den Anbieter als Organisation oder als Gesamtaussage. Auch hierbei wird es auf die konkrete Gestaltung ankommen. Selbst wenn eine Zertifizierung hinter der Aussage steht, muss das werbende Unternehmen aber sicherstellen, dass der Umfang der Zertifizierung der Werbeaussage tatsächlich entspricht und nicht der Eindruck entsteht, sämtliche Aspekte der DSGVO-Konformität seien abgedeckt.

Zwischenergebnis

Für welche „Art" unlauterer Werbung nach § 5 UWG man sich bei der Bewertung entscheidet, ist am Ende von geringer Relevanz. Wer argumentiert, die Marktlage sei tatsächlich so, dass viele Anbieter die DSGVO nicht einhalten, räumt damit ein, dass „100 % DSGVO-konform" eine konkrete, von der Realität abweichende Aussage über die eigene Compliance ist, und landet bei der Irreführung durch unwahre Angaben. Denn eine vollständige und dauerhaft verifizierbaren Konformität lässt sich – wie gezeigt – objektiv kaum belegen. Wer umgekehrt argumentiert, DSGVO-Konformität sei normativ wie faktisch als Marktstandard erreichbar, bestätigt gerade das Selbstverständlichkeitsargument. Beide Argumentationslinien schließen sich gegenseitig aus, aber sie bedingen gemeinsam, dass § 5 UWG in jedem Fall greift. Entweder die Aussage hebt sich von einer defizitären Marktlage ab, dann ist sie als konkrete Tatsachenbehauptung an ihrem Wahrheitsgehalt zu messen (und hält dieser Messung in aller Regel nicht stand). Oder der Markt ist tatsächlich konform, dann ist die Aussage eine Selbstverständlichkeit. Einen dritten Weg, auf dem „100 % DSGVO-konform" lauterkeitsrechtlich, zumindest in dieser Pauschalität, unbedenklich wäre, gibt es nicht. Ob darüber hinaus noch die Werbung mit mehrdeutigen Aussagen dazukommt, hat auf die Feststellung der Irreführung auf Basis anderer Handlungsmodalitäten keine Auswirkungen.

Zusammenfassung der Kernaussagen

Die pauschale Werbeaussage, ein Unternehmen oder ein komplexer Dienst sei „DSGVO-konform", ist aus mehreren lauterkeitsrechtlichen Richtungen angreifbar. Sie kann als irreführend gelten, weil sie eine abschließende Beurteilung suggeriert, die angesichts der dynamischen Natur der DSGVO nicht verlässlich getroffen werden kann. Sie kann auch als Werbung mit Selbstverständlichkeiten einzuordnen sein, weil sie lediglich die Erfüllung gesetzlicher Pflichten hervorhebt. Wer die eigene Datenschutz-Compliance kommunizieren will, sollte auf konkrete und nachprüfbare Angaben setzen Etwa durch den Verweis auf bestimmte technische und organisatorische Maßnahmen oder auf den Gegenstand und Umfang einer Zertifizierung. Gerade bei Zertifizierungen ist darauf zu achten, dass die Werbeaussage den tatsächlichen Prüfungsumfang widerspiegelt und nicht den Eindruck einer umfassenden DSGVO-Konformität erzeugt, die über das Zertifizierte hinausgeht.

Autoren: **Dr. Carlo Piltz ist Rechtsanwalt bei Piltz Legal in Berlin und spezialisiert im nationalen und internationalen Datenschutzrecht.**

Ilia Kukin ist Rechtsanwalt und Associate bei Piltz Legal in Berlin.