Client Alert | Commercial Litigation / Germany

Produkthaftung im Hochsicherheitssektor: KI-bedingte Risiken nach deutschem und europäischem Recht sicher steuern

16 November 2025

Authors: Sara Vanetta, Christian Theissen, Isabelle Peltier

Neue Technologien treffen auf neue Haftungsfragen: Der rasante technologische Wandel und die zunehmende Komplexität der Regulierung verändern die Risikolandschaft für Unternehmen im Hochsicherheitssektor. Da digitale Komponenten, vernetzte Systeme und KI bei Hochsicherheitsprodukten eine immer zentralere Rolle spielen, können Ausfälle erhebliche betriebliche, wirtschaftliche und nationale Sicherheitsauswirkungen haben. Diese Entwicklungen werfen neue Fragen zur Haftung auf, insbesondere wenn autonome Systeme menschliche Eingriffe weitgehend ersetzen oder einschränken. Der erste offizielle Entwurf eines neuen deutschen Produkthaftungsgesetzes (ProdHaftG),[1] veröffentlicht im September 2025, zur Umsetzung der überarbeiteten Produkthaftungsrichtlinie (ProdHaftRL),[2] und der EU AI Act[3] werden die Art und Weise prägen, wie Unternehmen Produktsicherheit, digitale Innovation und Risikoverteilung entlang der Lieferkette steuern.

1 Siehe den Entwurf des neuen deutschen Produkthaftungsgesetzes (ProdHaftG), der hier erhältlich ist.

2 Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, erhältlich hier.

3 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), hier erhältlich.

Haftungsrisiken und rechtliche Rahmenbedingungen: Aktueller Ausgangspunkt

Traditionell unterliegen Produkte im Hochsicherheitsbereich strengen Vorschriften und einer engen Überwachung, da sie in risikoreichen Umgebungen eingesetzt werden, in denen Zuverlässigkeit, Kontrolle und Cybersicherheit von entscheidender Bedeutung sind. Dieser Sektor umfasst nicht nur Produkte wie Verteidigungs- und Militärsysteme, sondern auch Güter mit doppeltem Verwendungszweck (Dual-Use-Produkte[4]), die sowohl im zivilen als auch im militärischen Bereich eingesetzt werden, beispielsweise in den Bereichen sichere Kommunikation, Verschlüsselungstools, Überwachungstechnologien und moderne Zugangskontroll- und Cybersicherheitssysteme – allgemeiner gesagt in allen Systemen, deren Ausfall Auswirkungen auf die nationale Sicherheit, die öffentliche Sicherheit oder wesentliche Dienste haben könnte. Der Rechtsrahmen wird durch bestehende europäische und nationale Vorschriften geprägt, darunter das deutsche Produkthaftungsgesetz (ProdHaftG), das deutsche Produktsicherheitsgesetz (ProdSG) und branchenspezifische Anforderungen (wie die deutsche KRITIS-Verordnung,[5] oder die EU-NIS-2-Richtlinie,[6] oder der EU Cybersecurity Act[7]). Die Einhaltung dieser Vorschriften sowie allgemeiner vertraglicher und deliktischer Grundsätze ist von zentraler Bedeutung für die Feststellung der Haftung im Falle eines Produktfehlers oder -schadens. Die zunehmende Integration digitaler Komponenten und KI in Hochsicherheitsprodukten sowie komplexe Lieferketten bringen neue Risiken und Unsicherheiten mit sich, insbesondere in Bezug auf Kontrolle, Produktfehlerhaftigkeit, menschliche Aufsicht und Verantwortlichkeiten in der Lieferkette. Gleichzeitig schaffen regulatorische Entwicklungen wie der EU AI Act und die überarbeitete EU-ProdHaftRL neue Standards und Haftungsregeln, die von Unternehmen eine Anpassung ihrer Compliance-, Dokumentations- und Risikomanagementpraktiken erfordern.

Die sich wandelnde Haftungslandschaft

Die Neufassung der ProdHaftRL und der EU AI Act gestalten das Regulierungs- und Haftungsumfeld neu und führen erhebliche Anpassungen und Erweiterungen ein, um auf neue Technologien und Risiken zu reagieren. Insbesondere befassen sich beide Regelwerke mit der Digitalisierung und der Einführung KI-gestützter Systeme, jedoch mit unterschiedlichen Zielen und Anwendungsbereichen. Die Produkthaftung wird über die Hardware hinaus auf Software-Updates, Datenqualität, algorithmisches Verhalten und Aspekte der Cybersicherheit ausgeweitet, die alle zu Produktmängeln führen können, auch wenn keine physischen Produktfehler vorliegen. Folglich müssen Hochsicherheitsprodukte in komplexen Umgebungen zuverlässig funktionieren und eine nachweisbare Kontrolle über KI-gesteuerte Funktionen aufrechterhalten. Da Lieferketten immer stärker vernetzt sind, führt die Einbindung von Drittanbieter-Software und vortrainierten Modellen zu erhöhten Haftungsrisiken und macht eine verstärkte Sorgfaltspflicht über den gesamten Entwicklungs- und Bereitstellungsprozess hinweg erforderlich. Obwohl Verteidigungsverträge mit öffentlichen Auftraggebern aufgrund einsatzkritischer Risiken und Beschaffungsanforderungen häufig Haftungsbeschränkungen vorsehen, bleibt die Einhaltung gesetzlicher Vorgaben von entscheidender Bedeutung, da diese vertraglichen Beschränkungen die gesetzliche Haftung nach den geltenden Produktsicherheits- und Haftungsvorschriften nicht unbedingt außer Kraft setzen. Lieferanten

---

4 In diesem Zusammenhang ist es für Unternehmen auch wichtig zu prüfen, ob ihre (KI-)Anwendung in den Anwendungsbereich der EU-Verordnung über Güter mit doppeltem Verwendungszweck (Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Schaffung einer Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlungstätigkeiten, der technischen Unterstützung, der Durchfuhr und der Weitergabe von Gütern mit doppeltem Verwendungszweck (Neufassung)) fällt. Hier erhältlich).

5 KRITIS-Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz, hier erhältlich.

6 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), hier erhältlich.

7 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und die Cybersicherheitszertifizierung im Bereich der Informations- und Kommunikationstechnologie sowie zur Aufhebung der Verordnung (EU) Nr. 526/2013 ((Rechtsakt zur Cybersicherheit), hier erhältlich.

können somit potenziellen Risiken nach der ProdHaftRL, etwa für Ansprüche Dritter oder Risiken in der Lieferkette, ausgesetzt bleiben.

Zwei unterschiedliche Rechtsrahmen: EU AI Act und ProdHaftRL

Der **EU AI Act** ist ein weitreichender regulatorischer Rahmen, aber und kein Gesetz zur Haftungsregelwerk. Er soll sicherstellen, dass KI-Systeme vertrauenswürdig und sicher sind und die Grundrechte innerhalb der Europäischen Union gewahrt werden. Er verfolgt einen risikobasierten Ansatz, der KI-Systeme nach minimalem, begrenztem, hohem und verbotenem Risiko einteilt, und jeweils spezifische Compliance-Anforderungen vorsieht. Der EU AI Act gilt allgemein und erfasst auch Organisationen außerhalb der EU, sofern der von dem KI-System erzeugte Output innerhalb der EU verwendet wird. Ausgenommen von dem Anwendungsbereich des EU AI Acts sind jedoch KI-Systeme, die ausschließlich für militärische Zwecke eingesetzt werden,[8] nicht aber Dual-Use oder nicht-exklusiv militärisch genutzte KI-Systeme.

Die **ProdHaftRL** sieht eine verschuldensunabhängige Haftung für fehlerhafte Produkte vor, um natürliche Personen und Sachen zu schützen, die nicht „ausschließlich für berufliche Zwecke“ verwendet werden.“[9] Staatliche Einrichtungen oder gewerbliche Käufer sind nicht berechtigt, als Geschädigte Ansprüche nach der ProdHaftRL geltend zu machen. Ansprüche können jedoch entstehen, wenn diese Produkte in Umgebungen eingesetzt werden, in denen Zivilpersonen mit der Technologie interagieren, oder wenn Cybersicherheitsvorfälle kritische Infrastrukturen beeinträchtigen und dadurch Einzelpersonen betroffen sind. Darüber hinaus können solche Ansprüche in Dual-Use-Szenarien entstehen, beispielsweise wenn Sicherheitsprodukte von Zivilpersonen genutzt werden. Die ProdHaftRL muss von den Mitgliedstaaten bis Dezember 2026 umgesetzt werden. Der deutsche Gesetzentwurf zum neuen ProdHaftG entspricht im Wesentlichen der ProdHaftRL, jedoch befindet sich das Gesetzgebungsverfahren noch in einem frühen Stadium, sodass die endgültige Ausgestaltung und der Zeitplan derzeit noch ungewiss sind.

Wichtige Änderungen für den Hochsicherheitssektor:

- **Verpflichtungen bei Hochrisiko-KI:** Für Unternehmen, die im Hochsicherheitssektor tätig sind, bringt der EU AI Act erhebliche Compliance-Verpflichtungen mit sich, insbesondere wenn ihre KI-Systeme als hochrisikoreich eingestuft werden. Hochrisiko-KI-Systeme unterliegen strengen Anforderungen und müssen unter anderem ein fortlaufendes Risikomanagement, eine robuste Datenverwaltung, technische Dokumentation, Ereignisprotokollierung, Transparenz, menschliche Aufsicht und Cybersicherheitsmaßnahmen während des gesamten Lebenszyklus des KI-Systems gewährleisten. Die Nichteinhaltung dieser Anforderungen kann zu erheblichen finanziellen Bußgeldern und Reputationsrisiken führen. Ein KI-System gilt als hochrisikoreich, wenn es unter bestimmte in der Verordnung festgelegte Kategorien fällt, z. B. wenn es in kritischen Infrastrukturen, grundlegenden öffentlichen Diensten, der Strafverfolgung oder der Grenzkontrolle eingesetzt wird. Darüber hinaus gelten auch KI-Systeme, die Sicherheitskomponenten von Produkten sind, die unter bestimmte EU-Harmonisierungsgesetze fallen und eine Konformitätsbewertung durch Dritte erfordern, als hochrisikoreich. Die Einstufung basiert auf dem Verwendungszweck des KI-Systems und nicht ausschließlich auf seinen technischen Merkmalen oder dem tatsächlichen Risikoniveau.[10]

- **Erweiterter „Produkt“-Umfang:** Artikel 4 der ProdHaftRL erweitert die Definition des Begriffs „Produkt“ um Software[11] und „digitale Konstruktionsunterlagen“ und umfasst somit KI-Systeme und digitale Komponenten (eigenständig oder eingebettet), wie sie beispielsweise in Verteidigungsplattformen, Überwachungssystemen oder autonomen Fahrzeugen eingesetzt werden.

---

8 Artikel 2 (3) EU AI Act.

9 Artikel 6 (1) (b) iii ProdHaftRL.

10 Weitere Informationen finden Sie im White & Case EU AI Act Handbook, insbesondere in den Kapiteln 6 bis 8, hier erhältlich.

11 Ausgenommen sind freie und quelloffene Software, die außerhalb einer kommerziellen Tätigkeit entwickelt oder bereitgestellt wird, siehe Artikel 2 (2) ProdHaftRL

- **Fehlerhaftigkeit und Haftung über den Lebenszyklus:** Artikel 7 der ProdHaftRL erweitert den Begriff der Fehlerhaftigkeit in mehrfacher Hinsicht. Unter anderem verlangt er nun die Einhaltung aller relevanten Produktsicherheitsanforderungen, einschließlich sicherheitsrelevanter Cybersicherheitsanforderungen. Der vernünftigerweise vorhersehbare Gebrauch des Produkts ist nun ebenfalls abgedeckt, ebenso wie die vernünftigerweise vorhersehbaren Auswirkungen auf andere Produkte, auch durch deren Verbindung. Produkte können auch nach ihrem ersten Inverkehrbringen durch Updates, erneute Trainings, selbstlernende Prozesse oder spätere Integration fehlerhaft werden,[12] was zu einer fortdauernden Haftung führt.

- **Breiteres Haftungsnetz:** Artikel 8 der ProdHaftRL erweitert die Haftung auf Unternehmen, die ein Produkt wesentlich verändern, beispielsweise durch Upgrades oder die Integration neuer (digitaler) Komponenten (z. B. Verteidigungsplattformen mit KI-gestützten Entscheidungshilfetools oder Subunternehmer, die bestehende Plattformen um Analysemodule erweitern). Die gesamtschuldnerische Haftung erstreckt sich dabei auf die gesamte Lieferkette.[13]

- **Offenlegung neuer Beweise (mit der Folge einer Vermutung der Fehlerhaftigkeit)** Artikel 9 der ProdHaftRL erlaubt es Gerichten unter bestimmten niedrigschwelligen Voraussetzungen die Offenlegung relevanter technischer Informationen anzuordnen, was insbesondere bei KI-Systeme mit eingeschränkter Nachvollziehbarkeit von Bedeutung ist. Der Schutz vertraulicher Daten oder Geschäftsgeheimnisse bleibt möglich, unterliegt jedoch dem Ermessen des Gerichts. Stellt das Gericht fest, dass der Beklagte seiner Offenlegungspflicht nicht vollständig nachgekommen ist, wird die Fehlerhaftigkeit des Produkts vermutet.

- **Weitere niedrigschwellige Vermutungen zugunsten der Antragsteller:** Erstens wird gemäß Artikel 10 der ProdHaftRL die Fehlerhaftigkeit eines Produkts vermutet, wenn der Kläger (lediglich) nachweist, dass das Produkt nicht den zwingenden Anforderungen an die Produktsicherheit entspricht. Zweitens wird ein Kausalzusammenhang zwischen Produktfehler und Schaden vermutet, wenn der verursachte Schaden typischerweise mit dem betreffenden Produktfehler vereinbar ist. Drittens muss der Kläger, wenn es ihm trotz Offenlegung der Beweise aufgrund der technischen oder wissenschaftlichen Komplexität des Falles übermäßig schwerfällt, den Produktfehler **und/oder** die Kausalität nachzuweisen, lediglich nachweisen, dass es wahrscheinlich ist, dass das Produkt fehlerhaft war **und/oder** dass ein Kausalzusammenhang besteht. Diese dritte Vermutung ist aufgrund ihrer hohen Komplexität für den Verteidigungssektor besonders relevant und kann die Beweislast sowohl hinsichtlich des Produktfehlers als auch des Kausalzusammenhangs auf den Hersteller verlagern.

- **Erweitertes Schadenskonzept:** Die Haftung umfasst nicht nur Personen- und Sachschäden, sondern auch die Vernichtung oder Beschädigung von Daten, die nicht für berufliche Zwecke verwendet werden.[14] Dies kann beispielsweise der Fall sein, wenn Software- oder KI-Fehler personenbezogene Daten von natürlichen Personen beschädigen oder löschen, die mit Sicherheitssystemen interagieren, wie z. B. Mitarbeiter, Besucher, Reisende oder andere zivile Nutzer von Zugangskontroll-, Überwachungs- oder kritischen Infrastrukturtechnologien. Eine Entschädigung für immaterielle Schäden ist möglich, wenn dies nach nationalem Recht vorgesehen ist (wie in Deutschland).

Wichtige Aspekte des deutschen Haftungsrechts

Die Haftung für Hochsicherheits- und Verteidigungstechnologien unterliegt nach deutschem Recht in erster Linie dem Vertragsrecht, dem allgemeinen Deliktsrecht, dem ProdHaftG und branchenspezifischen Sicherheitsvorschriften. Software- und KI-bezogene Ausfälle geben zunehmend Anlass zur Sorge, insbesondere wenn es durch autonome Systeme oder komplexe Lieferketten zu sicherheitskritischen Fehlfunktionen kommt, wie z. B. fehlerhaften Zuordnungen durch KI-basierte Identifikationssysteme, Schwachstellen nach Software-Updates, unvorhersehbares Drohnenverhalten aufgrund schlechter Trainingsdaten oder nicht verifizierte Modelle von Drittanbietern. Die Haftung in diesem Bereich resultiert vorrangig aus Vertragsverletzungen im B2B- und

12 Artikel 7 (1), (2) (c) ProdHaftRL, siehe auch Erwägungsgründe 19, 50 und 52.

13 Artikel 12 (1) ProdHaftRL.

14 Artikel 6 (1) (c) ProdHaftRL.

B2G-Kontext. Wie oben dargelegt, kann jedoch auch eine Haftung gegenüber natürlichen Personen nach der ProdHaftRL bzw. dem ProdHaftG oder dem Deliktsrecht entstehen.

Vertragliche Haftung

Die vertragliche Haftung gemäß §§ 280 ff. BGB ist bei Hochsicherheitsprojekten von zentraler Bedeutung, da in der Regel detaillierte Vereinbarungen über die Leistung, Integrationspflichten oder Offenlegungspflichten zwischen den beteiligten Parteien wie Auftragnehmern, Lieferanten, Integratoren und staatlichen Stellen getroffen werden. Die Haftung entsteht in der Regel aus Verstößen gegen solche ausdrücklichen oder ergänzenden Vertragsbedingungen. Im deutschen Vertragsrecht wird bei einem nachgewiesenen Verstoß in der Regel ein Verschulden vermutet, sofern der Auftragnehmer keinen Entlastungsnachweis erbringt. Diese Vermutung erschwert es, eine Haftung auszuschließen, insbesondere bei dem Einsatz von komplexen KI-Systemen. Während ein „Verschulden" der KI nicht selbst zugeschrieben werden kann, kann das Unternehmen aufgrund organisatorischer Mängel, mangelnder Aufsicht oder unzureichender Compliance-Maßnahmen haften. Die Einhaltung der geltenden regulatorischen Anforderungen kann daher zu einem entscheidenden Faktor dafür werden, ob eine Pflichtverletzung vorliegt oder ob sich der Auftragnehmer entlasten kann. Auftragnehmer haften in der Regel für Mitarbeiter und Beauftragte (§ 278 BGB), einschließlich Subunternehmer und externe Anbieter, wie z. B. diejenigen, die an der Prüfung, Schulung oder dem Einsatz von KI-Modellen beteiligt sind. Regressvereinbarungen und Freistellungsklauseln können die Haftung verlagern, aber Ausschlüsse für Vorsatz oder grobe Fahrlässigkeit unterliegen strengen gesetzlichen Beschränkungen und erfordern besonderer Sorgfalt bei ihrer Ausgestaltung. Darüber hinaus kann die Produkthaftung nach dem ProdHaftG vertraglich nicht ausgeschlossen werden.

Zusätzlich erhöht das deutsche Deliktsrecht die Haftungsrisiken beim Einsatz von KI, insbesondere wenn Dritte betroffen sind. Die allgemeine deliktische Haftung nach § 823 Abs. 1 BGB erfasst Schäden an den dort geschützten Interessen (Leben, Gesundheit, Eigentum, Persönlichkeitsrechte). Dies kann relevant werden, wenn etwa Systemausfälle zu Verletzungen oder Schäden führen, z. B. wenn ein KI-gestütztes Identifizierungssystem eine Person falsch klassifiziert oder ein autonomes Überwachungsgerät Sachschäden verursacht. § 823 Abs. 2 BGB findet Anwendung, wenn Schäden durch die Verletzung gesetzlicher Schutzpflichten entstehen. Im Hochsicherheitskontext kann dies Verstöße gegen Cybersicherheitsanforderungen nach dem IT-Sicherheitsgesetz oder der NIS-2-Richtlinie, Datenschutzpflichten bei der Verarbeitung personenbezogener Daten, in technische Vorschriften aufgenommene Sicherheitsnormen oder die Anforderungen des EU AI Acts umfassen. Im Deliktsrecht muss zwar grundsätzlich ein Verschulden nachgewiesen werden, ein Verstoß gegen einschlägige Vorschriften kann jedoch unter Umständen bereits als Fahrlässigkeit angesehen werden und die Beweislast entsprechend reduzieren. Die Haftung erstreckt sich auch auf Personen, die Aufgaben unter der Kontrolle des Unternehmens ausführen (§ 831 BGB, Haftung für Verrichtungsgehilfen), wobei eine Entlastung nur möglich ist, wenn das Unternehmen eine angemessene Auswahl, Anleitung und Überwachung nachweisen kann. Die Einhaltung der einschlägigen regulatorischen Standards ist in diesem Zusammenhang somit ebenfalls von wesentlicher Bedeutung.

Risikominderung und strategische Empfehlungen

Um den Veränderungen in der Haftungslandschaft gerecht zu werden und Risiken zu mindern, sollten Unternehmen einen ganzheitlichen Risikomanagementansatz verfolgen, der Compliance-, operative und vertragliche Maßnahmen miteinander verbindet:

- **Umfassende Risikobewertung:** Regelmäßige Erfassung und Bewertung von Haftungsrisiken für alle Produkte und Systeme, mit Schwerpunkt auf digitalen und KI-Komponenten, Abhängigkeiten in der Lieferkette und Dual-Use-Szenarien.
- **Robuste Dokumentation und Rückverfolgbarkeit:** Stellen Sie eine lückenlose Dokumentation aller Lebenszyklusphasen des KI-Systems sicher, einschließlich seiner Entwicklung, Tests, Aktualisierungen und KI-gestützten Entscheidungsprozesse, um die Einhaltung regulatorischer Vorgaben nachzuweisen und die Verteidigung bei Ansprüchen oder behördlichen Anfragen zu erleichtern.

- **Integrierte Cybersicherheit und KI-Sicherheit:** Integrieren Sie Cybersicherheit und KI-Risikomanagement in Produktsicherheitsrahmenwerke. Überwachen Sie kontinuierlich Schwachstellen und stellen Sie sicher, dass Updates, Nachschulungen und Integrationen von Drittanbietern den gesetzlichen und vertraglichen Standards entsprechen.
- **Vertragliche und versicherungstechnische Absicherungen:** Aktualisieren Sie Vertragsvorlagen und Lieferkettenverträge, um neue Haftungsrisiken, Dokumentationsanforderungen und Verpflichtungen, die an Subunternehmer und andere Parteien innerhalb der Lieferkette weitergegeben werden müssen, angemessen zu erfassen. Überprüfen und aktualisieren Sie den Versicherungsschutz (z. B. E&O, Cyber-Haftpflicht) und stellen Sie eine eindeutige Zuweisung von Verantwortlichkeiten und Entschädigungsregelungen entlang der gesamten Lieferkette im Rahmen der gesetzlichen Vorgaben sicher.
- **Interne Compliance und Schulungen:** Implementieren Sie interne Richtlinien für das Incident Management, die Zusammenarbeit mit Aufsichtsbehörden und die ordnungsgemäße Sicherung von Beweismitteln. Schulen Sie Compliance-, Rechts- und Technikteams zu neuen gesetzlichen Anforderungen, insbesondere hinsichtlich Dokumentation, Cybersicherheit und KI-Sicherheit.
- **Prozess- und Verfahrensstrategie:** Binden Sie technische Experten frühzeitig in Streitfälle ein, insbesondere bei komplexen KI-bezogenen Ansprüchen, und seien Sie darauf vorbereitet, dass Gerichte im Rahmen von künftigen Klagen nach der ProduktHaftRL die Offenlegung sensibler technischer Informationen verlangen können, darunter Trainingsdaten, Modelldetails und Protokolle. Bereiten Sie sich proaktiv auf den Schutz vertraulicher Informationen und Geschäftsgeheimnisse vor, da Gerichte verpflichtet sind, Offenlegungspflichten gegen die berechtigten Interessen aller Parteien abzuwägen und gegebenenfalls Maßnahmen zur Wahrung der Vertraulichkeit zu ergreifen. Die frühzeitige Zusammenarbeit mit technischen und juristischen Experten stellt sicher, dass sensible Informationen im Streitfall angemessen geschützt sind.

White & Case LLP
Bockenheimer Landstraße 20
Frankfurt am Main
60323

T + 49 69 29994 0
F + 49 69 29994 1444

White & Case LLP
Rahel-Hirsch-Straße 10
Berlin
10557

T + 49 30 8809110
F + 49 30 880911 297