Newsletter IP/IT

Mai 2026

Inhalt

Claude Mythos: Wenn Künstliche Intelligenz die Spielregeln der Cybersicherheit neu schreibt

I. Hintergrund

Anfang April 2026 hat das US-amerikanische KI-Unternehmen Anthropic ein Modell vorgestellt, das die Fachwelt aufhorchen lässt: Claude Mythos Preview. Es handelt sich um ein KI-Modell der neuesten Generation, das darauf spezialisiert ist, bislang unbekannte Schwachstellen in Software zu identifizieren – sogenannte Zero-Day-Lücken. In internen Tests fand Mythos Tausende solcher Schwachstellen, darunter eine 27 Jahre alte Schwachstelle im Betriebssystem OpenBSD. Mythos ist bewusst noch nicht öffentlich verfügbar. Anthropic hat die Freigabe zurückgehalten, weil dieselbe Fähigkeit, die Verteidiger stärkt, in falschen Händen verheerende Konsequenzen haben könnte.

II. Project Glasswing als Antwort

Anstatt das Modell einfach zu veröffentlichen, hat Anthropic einen ungewöhnlichen Weg eingeschlagen: Project Glasswing bringt zwölf der einflussreichsten Technologie- und Finanzunternehmen weltweit zusammen – darunter AWS, Google, Microsoft, Apple, Cisco, CrowdStrike und JPMorgan Chase –, um Mythos kontrolliert für defensive Zwecke zu nutzen. Diese Partner erhalten exklusiven Zugang, um kritische Schwachstellen in ihren Systemen zu finden und zu schließen, bevor Angreifer dies tun. Dass Rivalen wie Google und Microsoft hier an einem Tisch sitzen, ist bemerkenswert. Es unterstreicht, wie ernst die Branche das Dual-Use-Dilemma dieser Technologie nimmt.

III. Mythos als zweischneidige Sicherheitstechnologie

Neue Sicherheitstechnologien sind immer zweischneidig. Das gilt auch für Mythos in einem bislang unbekannten Ausmaß. Dieselbe Fähigkeit, die Sicherheitsteams hilft, Schwachstellen in Stunden statt Monaten aufzudecken, kann auch von Angreifern genutzt werden, um Exploits – Programme, die Sicherheitslücken von Software, Hardware oder Betriebssystemen ausnutzen – in industriellem Tempo zu entwickeln. Dass dies keine abstrakte Gefahr ist, hat Anthropic selbst dokumentiert: Im September 2025 entdeckte das Unternehmen die erste vollständig KI-orchestrierte Cyberspionagekampagne. Die Angreifer nutzten KI-Systeme autonom

für die Identifikation von Angriffsflächen, die Extraktion sensibler Daten und die Kartierung kompletter Netzwerktopologien. Dies geschah ohne permanente menschliche Steuerung. KI-gestützte Angriffe sind damit keine Zukunftsvision mehr. Sie sind gegenwärtig – und sie werden schneller und präziser.

IV. Öffentlicher Sektor als Angriffsziel

Private Unternehmen können auf diese Entwicklung mit erheblichen Investitionen in modernste Sicherheitsarchitekturen reagieren. Behörden und öffentliche Unternehmen stehen vor einer strukturell anderen Ausgangslage: gewachsene IT-Infrastrukturen mit Legacy-Systemen, teils jahrzehntealte Softwarekomponenten in sicherheitskritischen Prozessen, und eine besondere Schutzwürdigkeit der verarbeiteten Daten – von Meldedaten über Sozialdaten bis hin zu behördeninternen Vorgängen. Gleichzeitig ist der öffentliche Sektor ein attraktives Angriffsziel. Kritische Infrastrukturen – Verwaltungsportale, Energieversorgung, Gesundheitseinrichtungen, Verkehrssteuerung – sind auf funktionierende digitale Systeme angewiesen. Ein erfolgreicher Angriff trifft nicht nur eine Organisation, sondern mittelbar die Bevölkerung, die auf staatliche Leistungen vertraut. Hinzu kommt: Legacy-Software enthält häufig genau jene Art von Schwachstellen, die ein Modell wie Mythos in kürzester Zeit identifizieren kann – sowohl für Angreifer als auch für Verteidiger. Bereits heute nutzen Hunderte von Organisationen KI-basierte Sicherheitsscans, um Schwachstellen zu finden, die herkömmliche Tools jahrelang übersehen haben.

V. Pflicht zur Sicherheitsüberprüfung

§ 30 Abs. 2 S. 1 BSIG verpflichtet besonders wichtige und wichtige Einrichtungen, ihre Sicherheitsmaßnahmen am Stand der Technik auszurichten. Das Gesetz verlangt ausdrücklich, dass Risikomanagementmaßnahmen dem Stand der Technik entsprechen, einschlägige europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen.

Das klingt statisch. Ist es aber nicht. Was gestern noch dem Stand der Technik entsprach, kann morgen bereits veraltet sein – insbesondere dann, wenn neue Angriffsmethoden entstehen, die bestehende Schutzkonzepte grundsätzlich überholen. Claude Mythos ist genau ein solcher Wendepunkt: Ein Modell, das Zero-Day-Schwachstellen in einem Tempo findet, das frühere Annahmen über das Angriffspotenzial von Dritten grundlegend verschiebt. Wer heute nicht prüft, ob seine Sicherheitsarchitektur dem aktuellen Stand der Technik entspricht, riskiert nicht nur erfolgreiche Angriffe – sondern auch regulatorische Konsequenzen nach § 30 BSIG. Für Behörden, kommunale Unternehmen und Träger kritischer Infrastrukturen bedeutet das konkret: Eine Überprüfung der bestehenden Sicherheitsmaßnahmen ist kein Luxus, sondern eine gesetzliche Pflicht. Wer dies versäumt, setzt sich im Falle eines Vorfalls dem Vorwurf aus, den gebotenen Sorgfaltsmaßstab nicht erfüllt zu haben.

VI. Ganzheitliche Sicherheitsberatung für Behörden und öffentliche Unternehmen

Luther Public Services begleitet Behörden und öffentliche Unternehmen dabei, auf diese veränderte Sicherheitslandschaft vorbereitet zu sein – rechtlich fundiert, strategisch durchdacht und mit einem Blick auf das Gesamtsystem. Unser Ansatz der Integralen Sicherheit betrachtet nicht isolierte Einzelaspekte, sondern die 360°-Perspektive: physische Sicherheit, Informationssicherheit, Personensicherheit, Wirtschaftsschutz und organisatorischer Schutz werden zusammengedacht. Denn ein ausgereiftes technisches Sicherheitskonzept nützt wenig, wenn organisatorische Schwachstellen oder unzureichende Governance-Strukturen eine Hintertür offenlassen. Im Bereich Governance, Risk & Compliance unterstützen wir Sie bei der Einbettung von Sicherheitsmaßnahmen in bestehende GRC-Strukturen: von der rechtlichen Bestandsaufnahme nach § 30 BSIG über die Bewertung Ihrer aktuellen Sicherheitsarchitektur im Lichte des sich verändernden Standes der Technik bis hin zur Entwicklung einer zukunftsfähigen Sicherheitsstrategie. Technologische Entwicklungen wie Claude Mythos werden die Frage, ob Ihre Systeme sicher sind, nicht leichter beantworten. Aber sie machen deutlich, warum diese Frage dringlicher ist als je zuvor.

Datenschutz in Sigapur: Wachsende Durchsetzungsbereitschaft der Aufsichtsbehörde – Worauf Unternehmen jetzt achten sollten

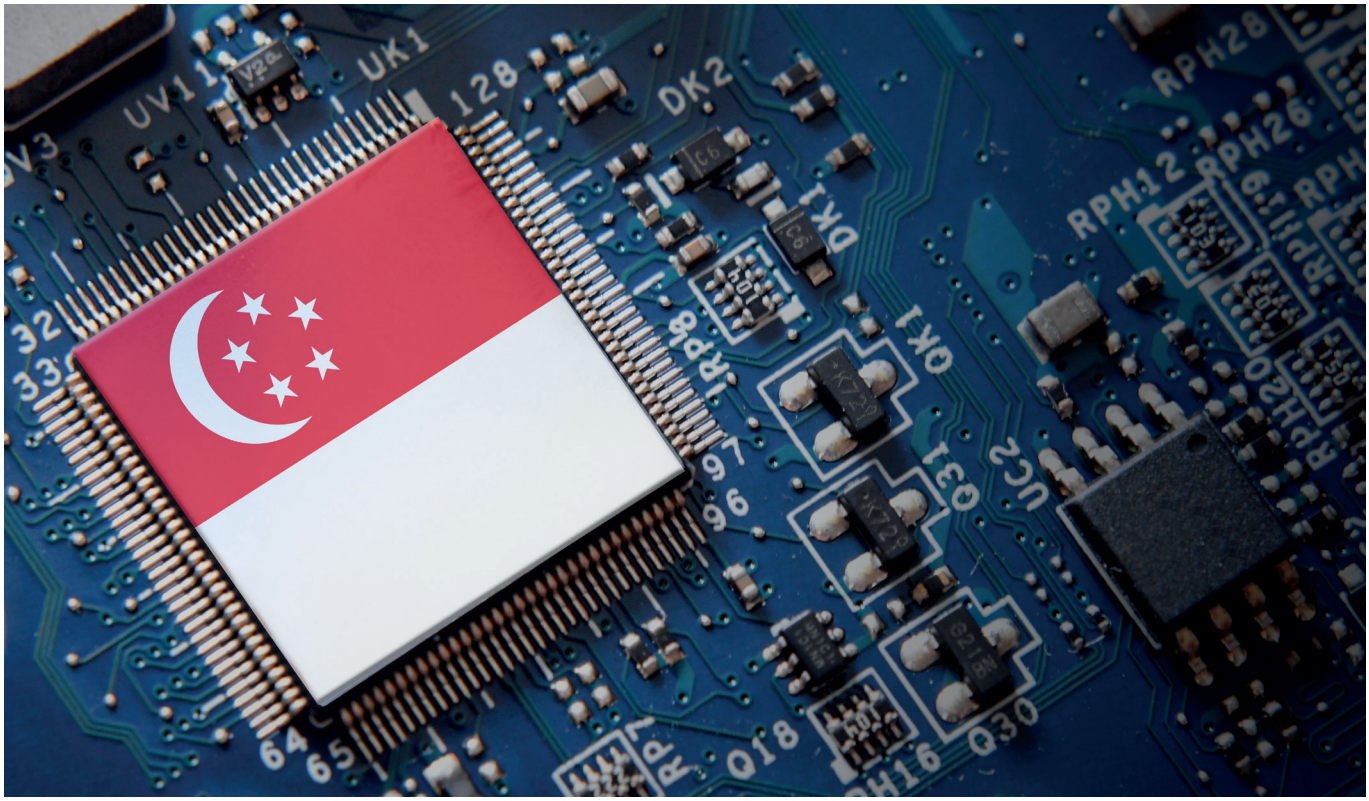
Das Datenschutzrecht in Singapur ist pragmatisch und wirtschaftsfreundlich ausgestaltet – gleichzeitig verfolgt die Personal Data Protection Commission (PDPC) einen zunehmend konsequenten Durchsetzungsansatz. Für Unternehmen mit Geschäftsaktivitäten in Singapur sind sowohl die formalen rechtlichen Compliance-Pflichten als auch die Erwartungen an technische und organisatorische Schutzmaßnahmen relevant. Jüngste Leitlinien und Bußgeldentscheidungen der PDPC zeigen, dass die Behörde beide Bereiche konsequent durchsetzt.

I. Anforderung an die Rechenschaftspflicht

Singapurs Datenschutzrecht, geregelt im Personal Data Protection Act (PDPA), ist in einigen Bereichen weniger streng ausgestaltet als die europäische Datenschutz-Grundverordnung (DSGVO). Viele Pflichten sind praxisorientierter formuliert und Unternehmen erhalten größere Spielräume bei der Umsetzung. Gleichwohl enthält der PDPA verbindliche formale Anforderungen. Zentral ist dabei die sogenannte „**Accountability Obligation**“ oder „**Rechenschaftspflicht**“ (Sections 11 und 12 PDPA), die Unternehmen verpflichtet, ihre Datenschutzpflichten nicht nur nach außen zu kommunizieren, sondern intern wirksam umzusetzen. Konkret verlangt Section 12 PDPA:

- **Datenschutzbeauftragter (Data Protection Officer, DPO):** Jedes Unternehmen muss mindestens eine Person benennen, die für die Einhaltung des PDPA verantwortlich ist, und deren Kontaktdaten öffentlich zugänglich machen. Der DPO spielt eine zentrale Rolle bei der Entwicklung von Datenschutzrichtlinien, der Erstellung eines Datenschutz-Inventars und der Meldung von Datenschutzrisiken.

- **Interne Datenschutzrichtlinien (Data Protection Policies):** Unternehmen sind verpflichtet, interne Richtlinien und Prozesse zu entwickeln, umzusetzen und an ihre Mitarbeitenden zu kommunizieren. Eine externe Datenschutzerklärung gegenüber Kunden genügt nicht. Sie muss durch entsprechende interne Policies und dokumentierte Abläufe untermauert sein – andernfalls bleibt sie, wie die PDPC formuliert hat, ein leeres Versprechen.



- **Beschwerdeprozess:** Es muss ein interner Prozess für die Entgegennahme und Bearbeitung von Datenschutzbeschwerden bestehen.

- **Datenschutz-Management-Programm (Data Protection Management Programme, DPMP):** Unternehmen werden ausdrücklich ermutigt, ein strukturiertes DPMP einzuführen, das die Bereiche Governance, Risikobeurteilung, Vorfallreaktion und laufende Überwachung umfasst.

Dies sind originär rechtliche Compliance-Anforderungen, bei deren Ausgestaltung und Umsetzung rechtliche Beratung unverzichtbar ist.

II. Umgang mit Ausweisdokumenten

Ein aktuell besonders relevantes Thema betrifft den Umgang mit der National Registration Identity Card (NRIC) – dem singapurischen nationalen Personalausweis für alle Staatsangehörigen und dauerhaft ansässigen Personen. Nach dem PDPC-Advisory vom Februar 2026 zählen NRIC-Nummern (in vollem und teilweisem Umfang) ausdrücklich zu den schutzwürdigen personenbezogenen Daten im Sinne von Section 24 PDPA. Private Unternehmen müssen die Verwendung von NRIC-Nummern zu Authentifizierungszwecken bis zum 31. Dezember 2026 einstellen; ab dem 1. Januar 2027 wird die Behörde entsprechende Verstöße konsequent verfolgen.

Reisepassnummern und die Foreign Identification Number (FIN) – die für ausländische Personen mit Langzeitaufenthaltsstatus in Singapur zugewiesene Identifikationsnummer – sind ähnlich schutzbedürftig. Die PDPC erwähnt sie im Advisory vom Februar 2026 zwar nicht ausdrücklich. Allerdings ergibt sich aus der Entscheidungspraxis, dass auch sie als sensible Daten behandelt werden sollten: In der Entscheidung *Air Sino-Euro Associates Travel Pte. Ltd.* [2025] SGPDPC 5 (Case No. DP-2312-C1857, 31. Oktober 2025) stellt die PDPC klar, dass NRIC- und Reisepassnummern als personenbezogene Daten gleich zu behandeln sind. Zugleich betont die Entscheidung, dass vollständige Bilder von Ausweisdokumenten – also Scans oder Fotos von NRIC-Karten und Reisepässen – eine besondere Gefahrenkategorie darstellen: Anders als die bloße Nummer enthält ein vollständiges Ausweisdokument eine Vielzahl personenbezogener Daten und wird häufig für Know-Your-Customer-Prozesse bei Finanztransaktionen eingesetzt. Seine Offenlegung ermöglicht daher in besonderem Maße Identitätsdiebstahl und kann zu konkreten finanziellen Schäden führen. Unternehmen, die solche Dokumente – etwa im Rahmen von Buchungsprozessen, Onboarding oder Compliance-Verfahren – erheben und speichern, sollten dieses erhöhte Risiko bei der Ausgestaltung ihrer Datenschutzmaßnahmen ausdrücklich berücksichtigen.

III. Technische und organisatorische Schutzmaßnahmen

Neben den formalen Compliance-Pflichten legt die PDPC besonderen Wert auf die technische und organisatorische Absicherung personenbezogener Daten (sogenannte „**Protection Obligation**“, Section 24 PDPA). Im Advisory vom Februar 2026 benennt die Behörde zwei wiederkehrende Schwachstellen: Sicherheitslücken bei Systemmigrationen – der Verbindung unterschiedlicher IT-Systeme, Anwendungen und Datenquellen – sowie das Fehlen von Mechanismen zur Erkennung und Verhinderung von Datenvorfällen.

Aus der Entscheidungspraxis lassen sich darüber hinaus konkrete Mindesterwartungen ableiten. Die Entscheidung *Air Sino-Euro Associates Travel* illustriert exemplarisch, welche technischen und organisatorischen Defizite die PDPC als Verstöße gegen die Protection Obligation wertet:

- **Patch Management und Systemwartung:** Das betroffene Unternehmen betrieb zum Zeitpunkt des Vorfalls einen Server mit Windows Server 2012 – einem Betriebssystem, dessen Hersteller-Support bereits im Oktober 2023 ausgelaufen war. Die PDPC wertete die Nutzung veralteter, nicht mehr unterstützter Software als eigenständiges Compliance-Versagen, das die Angreifer möglicherweise ausgenutzt haben.

- **Multi-Faktor-Authentifizierung (MFA):** Für administrative Konten mit Zugang zu sensiblen Daten oder großen Datenmengen betrachtet die PDPC MFA als Mindeststandard. Das Fehlen von MFA sowie unzureichende Passwortrichtlinien wurden ausdrücklich als Verstoß gewertet.

- **Vendor Management:** Das Unternehmen hatte IT-Dienstleister mit der Systembetreuung beauftragt, jedoch keine schriftlichen Verträge mit klaren Zuständigkeiten für Patch Management – die strategische Verwaltung und Implementierung von Software-Updates –, Sicherheitsreviews und Datenschutz abgeschlossen. Die PDPC stellt klar: Die Protection Obligation verpflichtet Unternehmen, die Leistungen ihrer Dienstleister vertraglich zu spezifizieren und deren Einhaltung aktiv zu überwachen. Die Auslagerung von IT-Funktionen entbindet nicht von dieser Verantwortung.

- **Regelmäßige Sicherheitsreviews und Penetrationstests:** Unternehmen müssen ihre Systeme regelmäßig auf Sicher-

heitslücken überprüfen – insbesondere vor dem Go-live nach Systemänderungen. Vulnerability Assessments und Penetrationstests (VAPT) werden von der PDPC ausdrücklich als empfohlene Maßnahme genannt.

- **Datenbankbasiertes Monitoring:** Standardmäßige Perimeter-Sicherheit (wie Firewalls) genügt nicht. Unternehmen sollten zusätzlich Systeme einsetzen, die ungewöhnliche Zugriffsmuster – etwa den massenweisen Download von Kundendaten – frühzeitig erkennen und melden.

- **Sicherung von Audit-Logs:** Die Entscheidung enthält auch einen ausdrücklichen Hinweis darauf, dass Audit- und Systemlogs im Nachgang eines Vorfalls zu sichern sind, um eine forensische Aufklärung des Vorfalls zu ermöglichen.

IV. Auswirkung auf die Praxis

Zwei aktuelle Entscheidungen verdeutlichen, wie ernst die PDPC diese Anforderungen nimmt.

In der Entscheidung gegen *Air Sino-Euro Associates Travel Pte. Ltd.* ([2025] SGPDPC 5, 31. Oktober 2025) verhängte die PDPC eine Geldbuße von SGD 47.000 wegen mehrfacher Verstöße gegen die Accountability Obligation und die Protection Obligation. Das Unternehmen hatte zwar eine externe Datenschutzerklärung für Kunden, aber weder einen DPO ernannt noch interne Datenschutzrichtlinien eingeführt. Technisch betrieb es ein veraltetes, nicht mehr unterstütztes Betriebssystem ohne MFA und ohne schriftliche Dienstleisterverträge. Die PDPC wertete das Zusammentreffen mehrerer Verstöße sowie den Umstand, dass kein DPO vorhanden war, der die Risiken hätte erkennen können, als systemisches Versagen.

Die Entscheidung gegen *Marina Bay Sands Pte. Ltd.* – das bekannte Resort- und Kasinogebäude am Ufer der Marina Bay in Singapur – (PDPC, 28. Oktober 2025) zeigt, dass auch ressourcenstarke Großunternehmen in den Fokus der Behörde geraten. Im Zuge einer Softwaremigration im März 2023 wurden die Daten von rund 665.000 Kunden durch unbekannte Dritte abgegriffen und anschließend im Darknet zum Kauf angeboten. Ein einzelner Mitarbeiter hatte manuell API-Konfigurationen in die neue Software übertragen – ohne zweite Kontrollinstanz. Die Sicherheitslücke blieb sechs Monate unentdeckt. Die PDPC verhängte eine Geldbuße von SGD 315.000. Sanktioniert wurde nicht ein außergewöhnlicher Cyberangriff, sondern das Fehlen grundlegender Prozesskontrollen – genau die Schwachstellen, die der Advisory vom Februar 2026 als typische Risikobereiche benennt. Als mildernde Umstände berücksichtigte die PDPC jeweils die Kooperation mit der Behörde während ihrer Ermittlungen und die unverzügliche Einleitung von Abhilfemaßnahmen.

V. Verhältnis zur DSGVO

Für europäische Unternehmen mit Singapur-Bezug ist diese Entwicklung besonders relevant. Das PDPA-Regime ist in einigen Bereichen – insbesondere bei Umfang und Detailtiefe der Dokumentationspflichten – weniger strikt als die DSGVO. Die Grundstruktur ist jedoch vergleichbar: Auch in Singapur werden DPO-Pflicht, interne Richtlinien und technisch-organisatorische Schutzmaßnahmen konsequent durchgesetzt. Wer diese Anforderungen vernachlässigt, muss mit regulatorischen Konsequenzen rechnen – unabhängig davon, ob er bereits DSGVO-konform aufgestellt ist. Ein vergleichsweise flexiblerer Rechtsrahmen bedeutet für international tätige Unternehmen damit nicht automatisch geringere Compliance-Anforderungen im operativen Alltag.

VI. Fazit und Ausblick

Unternehmen mit Geschäftsaktivitäten in Singapur sollten ihre Datenschutz-Compliance strukturiert überprüfen – sowohl die rechtlich formalen als auch die technisch-organisatorischen Anforderungen. Es gelten daher besondere Handlungsempfehlungen für die Praxis:

- **Rechtliche Struktur:** Ist ein DPO ernannt und mit ausreichenden Ressourcen und Befugnissen ausgestattet? Bestehen interne Datenschutzrichtlinien, die tatsächlich umgesetzt und an Mitarbeitende kommuniziert werden – und nicht nur eine externe Datenschutzerklärung?

- **Umgang mit besonders sensiblen Daten:** Werden NRIC-Nummern, Reisepassnummern oder FIN-Nummern noch zu Authentifizierungszwecken verwendet? Werden vollständige Bilder von Ausweisdokumenten erhoben und gespeichert, und ist das Schutzniveau dem besonderen Risiko angemessen?

- **Vendor Management:** Sind IT-Dienstleister vertraglich auf klare Sicherheitspflichten verpflichtet, und wird deren Einhaltung aktiv überwacht?

- **Technische Maßnahmen:** Sind Multi-Faktor-Authentifizierungen für administrative Konten, aktuelle Betriebssysteme, regelmäßige Penetrationstests und datenbankbasiertes Monitoring etabliert?

EuGH: Exzessives DSGVO-Hopping kann auch schon bei einem erstem Auskunftsantrag vorliegen

Der EuGH hat in seinem Urteil vom 19.03.2026 (Az. C-526/24) entschieden, dass bereits ein erster Antrag auf Auskunft nach Art. 15 DSGVO „exzessiv“ i. S. v. Art. 12 Abs. 5 DSGVO sein kann, sofern er in missbräuchlicher Absicht erfolgt. Er stellte zudem fest, dass Verstöße gegen das Auskunftsrecht unabhängig von einer unrechtmäßigen Datenverarbeitung einen Schadensersatzanspruch nach Art. 82 DSGVO auslösen können. Außerdem erkennt das Urteil die Unsicherheit darüber, ob personenbezogene Daten verarbeitet wurden, als möglichen immateriellen Schaden an.

Der Sachverhalt

Der Entscheidung des EuGH liegt der Rechtsstreit zwischen dem Optikerunternehmen Brillen Rottler GmbH & Co KG und TC, einer Privatperson, zugrunde. TC hatte sich beim Newsletter von Brillen Rottler angemeldet und kurze Zeit später einen Auskunftsantrag nach Art. 15 DSGVO gestellt. Das Unternehmen wies den Antrag unter Verweis auf Art. 12 Abs. 5 DSGVO zurück, da es ihn für missbräuchliches „DSGVO-Hopping“ hielt. Unter diesem Begriff versteht man das systematische Herbeiführen von Datenverarbeitungen (etwa durch Newsletter-Anmeldungen), um daraufhin Auskunftsanträge zu stellen. Das Ziel des Auskunftsantrags ist dabei nicht die Überprüfung der Datenverarbeitung, sondern die künstliche Schaffung von Voraussetzungen für gewinnbringende Schadensersatzansprüche – etwa wegen verspäteter oder vermeintlich unzureichender Auskunft. TC ist nach öffentlichen Informationen als „DSGVO-Hopper“ bekannt.

Da TC von seinem Antrag nicht absah, erhob Brillen Rottler Klage vor dem AG Arnsberg auf Feststellung, dass kein Schadensersatzanspruch bestehe. Das AG Arnsberg legte dem EuGH daraufhin Fragen zur Vorabentscheidung vor. Zum einen sollte geklärt werden, ob ein erster Auskunftsantrag bereits als „exzessiv“ i.S.v. Art. 12 Abs. 5 DSGVO gewertet werden kann und ob sich Verantwortliche dabei auf öffentliche Informationen über das Verhalten des Antragstellers stützen dürfen. Zum anderen wollte das Gericht wissen, ob die Verletzung des Auskunftsrechts überhaupt einen Schadensersatzanspruch nach Art. 82 DSGVO auslöst und ob der immaterielle Schaden den „Verlust der Kontrolle“ oder die bloße „Ungewissheit“ über die Verarbeitung personenbezogener Daten umfasst.

Die Entscheidung des EuGH

Der EuGH entschied, dass bereits ein erster Auskunftsantrag als „exzessiv“ im Sinne von Art. 12 Abs. 5 DSGVO eingestuft werden kann, wenn er missbräuchlichen Zwecken dient. Da es sich bei Art. 12 Abs. 5 DSGVO um eine Ausnahmeregelung handelt, betont der EuGH, dass der Begriff eng auszulegen ist. Die Beweislast für den exzessiven Charakter trägt der Verantwortliche. Um einen Antrag als exzessiv zu qualifizieren, muss dieser zwei Elemente nachweisen: Erstens, dass trotz formaler Einhaltung der Voraussetzungen der DSGVO das Ziel (sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen) verfehlt wird. Zweitens, dass eine Missbrauchsabsicht vorliegt, also die Voraussetzungen für einen Vorteil aus der DSGVO künstlich geschaffen werden sollen. Bei der Prüfung sind alle Umstände des Einzelfalls zu berücksichtigen; öffentlich zugängliche Informationen können als Indiz herangezogen werden, sofern sie durch weitere Anhaltspunkte gestützt sind. Zudem bejaht der EuGH eindeutig, dass Art. 82 DSGVO auch bei bloßen Verstößen gegen das Auskunftsrecht einen Schadensersatzanspruch gewährt, ohne dass zwingend eine unrechtmäßige Datenverarbeitung vorliegen muss. Dass der Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden auslösen kann, wurde bereits in der früheren Rechtsprechung des EuGH geklärt und wird in dieser Entscheidung erneut bestätigt. In diesem Zusammenhang fasst der EuGH die Voraussetzungen für einen Schadensersatzanspruch nach Art. 82 DSGVO erneut zusammen: Es müssen kumulativ ein Verstoß gegen die DSGVO, ein tatsächlich entstandener Schaden sowie ein Kausalzusammenhang zwischen beiden vorliegen. Der EuGH stellt zudem klar, dass diese Erwägungen auch auf die „Ungewissheit darüber, ob personenbezogene Daten verarbeitet wurden“, übertragbar sind. Ferner weist er erneut darauf hin, dass der Betroffene nachweisen muss, dass ihm durch den Verstoß auch tatsächlich ein Schaden entstanden ist; eine Schadensvermutung ist nicht vorgesehen. Ein Schadensersatzanspruch kommt außerdem nicht in Betracht, wenn der Verstoß und der daraus resultierende Schaden durch missbräuchliches Verhalten der betroffenen Person provoziert wurden, da dies den erforderlichen Kausalzusammenhang unterbricht.

Fazit und Ausblick

Das Urteil des EuGH entfaltet eine starke Signalwirkung gegen missbräuchliche Auskunftsanträge, da es erstmals klarstellt, dass auch der erste Antrag als „exzessiv“ abgelehnt werden kann, wenn ein missbräuchlicher Charakter des Antrags nachgewiesen wird. In der Praxis bleibt jedoch abzuwarten, ob dies dem „DSGVO-Hopping“ tatsächlich Einhalt gebietet, da die Anforderungen an den Nachweis eines solchen rechtsmissbräuchlichen Handelns sehr hoch sind. Gleichzeitig eröffnet das Urteil neue Risiken. Die Bestätigung, dass ein Schadensersatzanspruch nach Art. 82 DSGVO nicht zwingend eine unrechtmäßige Datenverarbeitung voraussetzt, sondern bereits die Verletzung des Auskunftsrechts genügt, und die Anerkennung der „Ungewissheit darüber, ob personenbezogene Daten verarbeitet wurden“ als immaterieller Schaden könnten eine neue Welle an Klagen auslösen.

Digital-Omnibus-Verordnung: Kompromiss nach gescheitertem Trilog

Der EU-Gesetzgeber plante eine größere Anpassung der europäischen Digitalrechtsakte, insbesondere der KI-Verordnung, der DSGVO und des Data Act (**Luther Newsflash Dezember 2025**). Am 29.04.2026 galt das Gesetzgebungsverfahren zu dieser sog. Digital-Omnibus-Verordnung, die Änderungen der KI-Verordnung und weiterer Digitalrechtsakte der EU bringen sollte, zunächst als gescheitert. Nur gut eine Woche später verkündeten das Europäische Parlament und der Rat, eine politische Einigung gefunden zu haben. Die Verordnung bringt voraussichtlich einige Änderungen und räumt Unternehmen insbesondere etwas mehr Zeit ein, die Anforderungen der KI-Verordnung umzusetzen.

Kern der Digital-Omnibus-Verordnung ist die Verschiebung verschiedener Zeitpunkte, zu denen Anforderungen der KI-Verordnung gelten sollen:

- **Kennzeichnungspflichten** für KI-generierte Inhalte und Deepfakes gelten erst ab dem **02.12.2026** und
- Die Geltung der Regelungen für **eigenständige Hochrisiko-KI-Systeme** verschiebt sich auf den **02.12.2027** und für Hochrisiko-KI-Systeme, die als Sicherheitsbauteil eingesetzt werden, auf den **02.08.2028.**

- Für die Mitgliedstaaten verlängert sich die Frist zur Einrichtung von KI-Reallaboren bis zum **02.08.2027**.

Diese Pflichten sollten ursprünglich bereits ab dem 02.08.2026 gelten.

Außerdem wird der Katalog der verbotenen KI-Praktiken um Anwendungen erweitert, die nicht einvernehmliche sexuelle und intime Inhalte oder Darstellungen von sexuellem Missbrauch von Kindern erzeugen. Produkte, die der **Maschinenverordnung** unterfallen, sollen demgegenüber aus dem Anwendungsbereich herausfallen. Weitere Bereiche kann die Kommission künftig aus dem Anwendungsbereich der KI-Verordnung ausnehmen, wenn sektorspezifische Rechtsvorschriften Anforderungen enthalten, die mit der KI-Verordnung vergleichbar sind. Eine Doppelregulierung soll so vermieden werden.

Bislang liegen lediglich Pressemitteilungen von EU-Parlament und Rat vor; das Gesetzgebungsverfahren ist aber noch nicht formal abgeschlossen. Aus den Pressemitteilungen ergibt sich zudem nicht, ob auch die geplanten Aktualisierungen der DSGVO und weiterer Rechtsakte in den Kompromiss eingeflossen sind, von denen sich Unternehmen zusätzliche Erleichterungen erhofft haben. Geplant waren unter anderem:

- Rechtsgrundlagen für die Entwicklung von KI,
- Erleichterungen für KMU,
- Eine einheitliche Meldestelle für Sicherheitsvorfälle und Verschlankung von Meldepflichten,
- Ablehnungsmöglichkeiten von Auskunftsersuchen,
- Vereinfachungen für Consent-Banner und
- Die Stärkung von Geschäftsgeheimnissen.

Ein vollständiger Überblick der geplanten Änderungen findet sich im **Luther Newsflash Dezember 2025**. Wie die Änderungen im Detail ausfallen und wann sie in Kraft treten, bleibt noch abzuwarten.

Cybersecurity als Organpflicht: Warum digitale Resilienz zur Führungsaufgabe wird

Cyberangriffe gehören längst zum unternehmerischen Alltag. Gleichwohl wird Cybersecurity in vielen Unternehmen noch immer primär als operative IT-Aufgabe angesiedelt zwischen Infrastruktur, Datenschutz und Compliance verstanden. Diese Einordnung greift zu kurz. Spätestens mit den verschärften regulatorischen Anforderungen durch NIS2 und DORA ist Cybersecurity endgültig auf Geschäftsleitungsebene angekommen.

Denn im Ernstfall stellt sich nicht allein die Frage, wie es zu einem Sicherheitsvorfall kommen konnte. Im Fokus stehen zunehmend Organisationspflichten, Überwachungsmaßnahmen und Governance-Strukturen der Unternehmensleitung. Maßgeblich ist dabei, ob Vorstand oder Geschäftsführung ihren gesetzlichen Pflichten zur ordnungsgemäßen Unternehmensorganisation nachgekommen sind.

Cybersecurity als Bestandteil ordnungsgemäßer Unternehmensführung

Die Verantwortung der Geschäftsleitung für ein angemessenes Risikomanagement folgt bereits aus allgemeinen gesellschaftsrechtlichen Organisationspflichten: Für Geschäftsführer einer GmbH ergibt sich dies insbesondere aus § 43 Abs. 1 GmbHG. Danach haben Geschäftsführer „in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“. Vergleichbare Pflichten treffen Vorstandsmitglieder einer Aktiengesellschaft nach § 93 Abs. 1 Satz 1 AktG. Die Pflicht zur ordnungsgemäßen Unternehmensorganisation umfasst dabei auch die Einrichtung eines angemessenen Compliance- und Risikomanagementsystems. Dass hierzu auch Cyberrisiken gehören, steht heute außer Frage. Cyberangriffe können erhebliche finanzielle Schäden, Produktionsausfälle, Datenschutzverletzungen sowie Reputationsschäden verursachen. Entsprechend werden sie zunehmend als wesentliche Unternehmensrisiken eingeordnet.

Delegation entbindet nicht von Verantwortung

Zwar können operative Aufgaben im Bereich Informationssicherheit delegiert werden, etwa an einen Informationssicherheitsbeauftragten, eine interne IT-Abteilung oder externe Dienstleister. Die Verantwortung der Geschäftsleitung für Auswahl, Organisation und Überwachung verbleibt jedoch bei ihr. Diese Grundsätze entsprechen allgemeinen gesellschaftsrechtlichen Delegationsmaßstäben: Geschäftsleiter dürfen Aufgaben übertragen, müssen jedoch durch geeignete Kontroll- und Informationsmechanismen sicherstellen, dass Risiken angemessen gesteuert werden. Gerade bei kritischen

IT-Prozessen gewinnt dies erheblich an Bedeutung. Dies gilt insbesondere bei Outsourcing- und Cloud-Strukturen. Unternehmen bleiben auch dann verantwortlich, wenn wesentliche IT-Leistungen durch externe Anbieter erbracht werden. Die Pflicht zur sorgfältigen Auswahl und laufenden Überwachung von Dienstleistern ist gesellschaftsrechtlich anerkannt und wird durch regulatorische Vorgaben zunehmend verschärft.

IT-Sicherheitsregulierung konkretisiert bestehende Organpflichten

Die regulatorischen Entwicklungen der vergangenen Jahre haben die gesellschaftsrechtlichen Organisations- und Überwachungspflichten der Geschäftsleitung im Bereich Cybersecurity erheblich konkretisiert.

Mit der Umsetzung der NIS2-Richtlinie in nationales Recht werden künftig deutlich mehr Unternehmen verpflichtet sein, angemessene technische, operative und organisatorische Maßnahmen zur Cybersicherheit umzusetzen. Erfasst sind dabei nicht nur Betreiber kritischer Infrastrukturen, sondern auch zahlreiche mittelständische Unternehmen aus „wichtigen“ und „besonders wichtigen“ Sektoren. Besondere Bedeutung kommt der ausdrücklichen Einbindung der Leitungsorgane zu. Diese müssen gemäß § 38 BSIG die angemessenen Risikomanagementmaßnahmen im Bereich der Informationssicherheit umsetzen, deren Umsetzung überwachen und regelmäßig an Cybersicherheitsschulungen teilnehmen. Zugleich verschärfen sich die Anforderungen an Risikomanagement, Incident Handling, Business Continuity, Lieferkettensicherheit sowie Melde- und Dokumentationspflichten. Cybersecurity wird damit regulatorisch ausdrücklich als Governance- und Organpflicht verstanden.

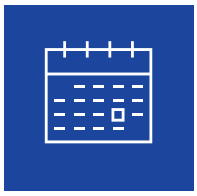
Noch weiter gehen die Vorgaben der DORA-Verordnung für Unternehmen des Finanzsektors. Diese verpflichtet betroffene Unternehmen unter anderem zur Einrichtung eines umfassenden IKT-Risikomanagementrahmens, zur Durchführung regelmäßiger Resilienztests sowie zur strukturierten Steuerung von Drittparteirisiken bei Einbindung von IKT-Dienstleistern. Unternehmen müssen Risiken entlang ihrer Liefer- und Dienstleisterketten identifizieren, überwachen und dokumentieren. Nach Art. 5 DORA trägt das Leitungsorgan hierfür ausdrücklich die letztendliche Verantwortung und hat die Umsetzung entsprechender Strategien aktiv zu überwachen.

Fazit und Handlungsempfehlung

Cybersecurity darf heute nicht mehr isoliert als technisches Spezialthema behandelt werden. Geschäftsleitungen müssen vielmehr sicherstellen, dass Cyberrisiken angemessen in bestehende Governance-, Compliance- und Risikomanagementstrukturen integriert werden. Hierzu gehören insbesondere klare Informations- und Reportingstrukturen, definierte Zuständigkeiten und Eskalationsmechanismen sowie dokumentierte Risiko- und Notfallprozesse. Rechtlich maßgeblich bleibt dabei der Grundsatz der Angemessenheit. Welche Maßnahmen erforderlich sind, richtet sich insbesondere nach Branche, Unternehmensgröße, Schutzbedarf und Risikolage des jeweiligen Unternehmens. Zugleich gewinnt Dokumentation erheblich an Bedeutung: Im Haftungs- oder Aufsichtsverfahren wird regelmäßig entscheidend sein, ob die Geschäftsleitung nachvollziehbar darlegen kann, dass Risiken identifiziert, bewertet und angemessen adressiert wurden.

Unternehmen sollten die aktuellen regulatorischen Entwicklungen daher zum Anlass nehmen, bestehende Governance- und Sicherheitsstrukturen kritisch zu überprüfen. Besondere Aufmerksamkeit verdient dabei die Steuerung von Drittparteirisiken, insbesondere bei Cloud- und Outsourcing-Strukturen. Letztlich ist Cybersecurity heute Teil ordnungsgemäßer Unternehmensführung. Die Fähigkeit, digitale Risiken strukturiert zu steuern und auf Sicherheitsvorfälle resilient zu reagieren, wird zunehmend zum Maßstab verantwortungsvoller Unternehmensleitung.

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

Sutthiphong/Adobe Stock: Seite 3; tippapatt/Adobe Stock: Seite 5; sdecoret/Adobe Stock: Seite 7; BOTAHRY DEX/Adobe Stock: Seite 10; Firn/Adobe Stock: Seite 12; sasun Bughdaryan/Adobe Stock: Seite 15;Getty Images: Seite 17

Luther.

Bangkok, Berlin, Brüssel, Delhi-Gurugram, Düsseldorf, Essen, Frankfurt a. M., Hamburg, Hannover, Ho-Chi-Minh-Stadt, 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

unyer GLOBAL ADVISORS