Newsletter 10/2026

FOX Group

Warum aktuelle Geheimhaltungsvereinbarungen scheitern



Die Nutzung künstlicher Intelligenz im Arbeitsalltag kollidiert zunehmend mit bestehenden Geheimhaltungsvereinbarungen (Non-Disclosure Agreements, NDAs). Klassische Verträge untersagen strikt die Weitergabe sensibler Informationen an Dritte. Werden jedoch vertrauliche Mandaten- oder Unternehmensdaten in externe KI-Modelle eingespeist, geschieht genau das:
Die Daten verlassen die eigene Infrastruktur, fließen an den Anbieter und werden im schlimmsten Fall für das Training der Systeme genutzt.

Um schwerwiegende Vertragsbrüche und Haftungsrisiken zu vermeiden, müssen bestehende NDAs dringend angepasst werden. Unternehmen stehen in der Pflicht, klare Definitionen darüber zu integrieren, was im Kontext von KI als „Weitergabe“ gilt. Gleichzeitig sollten Verträge die Nutzung auf lokale, datenschutzkonforme KI-Instanzen beschränken, bei denen eine Datennutzung durch den Anbieter vertraglich ausgeschlossen ist. Nur präzise angepasste NDAs sichern Geschäftsgeheimnisse im KI-Zeitalter rechtlich ab.

Thema 1

Warum aktuelle Geheimhaltungs vereinbarungen scheitern

Thema 2

Erinnerung Praktische Relevanz der KI-Verordnung

Thema 3

KI-Verordnung: Warum Weiterbildung eine rechtliche Pflicht ist

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.

Erinnerung Praktische Relevanz der KI-Verordnung

Seit August läuft die Durchsetzung weiterer Teile der KI-Verordnung (AI-Act). Unter anderem gelten Transparenzanforderungen für bestimmte KI-generierte Inhalte. Gleichzeitig hat die EU durch den Digital Omnibus Teile der Umsetzung verändert. Die Anwendung bestimmter High-Risk-Vorschriften wurde auf den 2. Dezember 2027 beziehungsweise bei in Produkte eingebetteten High-Risk-Systemen auf den 2. August 2028 verschoben. Was bedeutet das konkret?

In Bezug auf den AI-Act und die Transparenzanforderungen bedeutet dies, dass beim Einsatz von KI-Tools, um Bilder, Texte oder Videos bereitzustellen, diese Inhalte für den Nutzer klar und maschinenlesbar als künstlich erzeugt gekennzeichnet sein müssen. Auch Kundenservice-Chatbots müssen sich sofort unmissverständlich als Maschine zu erkennen geben. In diesem Kontext bedeutet „maschinenlesbar“, dass ein KI-Bild bildlich gesprochen zwei „Pässe“ besitzt. Die meisten Anbieter setzen hier auf die vom Gesetz gewünschte „robuste“ Lösung, den offenen Industriestandard C2PA (Content Credentials) oder auf spezielle IPTC-Einträge. Diese für das menschliche Auge unsichtbaren Pixelstrukturen werden einfach in das Bild eingearbeitet.

Der zweite „Pass“ ist der sichtbare Hinweis, dass die Information mit KI erstellt wurde. Wer diese Anforderungen ignoriert, riskiert schon jetzt rechtliche Konsequenzen. Gleichzeitig hat die EU über das Anpassungspaket des Digitalen Omnibus die Reißleine bei den bürokratisch schwersten Auflagen gezogen. Da technische Standards und Prüfstellen noch fehlen, wurden die strengen Auflagen für Hochrisiko-KI zeitlich nach hinten verschoben. Für eigenständige Software – wie KI-gestützte Bewerbungsverfahren – gilt die Pflicht erst ab dem 2. Dezember 2027. Ist die KI fest in Produkte wie Medizingeräte oder Autos eingebettet, greifen die Regeln sogar erst ab dem 2. August 2028. Unternehmen müssen also jetzt sofort transparent kennzeichnen, gewinnen aber wertvolle Jahre, um komplexe Systeme rechtssicher vorzubereiten.

Wer beispielsweise seine Bewerbungen über ein ATS (Applicant Tracking System) steuert, hat Zeit gewonnen, um technische und organisatorische Maßnahmen für menschliche Aufsicht und Diskriminierungsprüfungen zu etablieren. Dies nimmt einige Zeit in Anspruch. Der Gesetzgeber hat diese Atempause zwar gewährt, Unternehmen sollten die gewonnene Zeit jedoch aktiv nutzen, um nicht unvorbereitet in die Fristen zu laufen.

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.

KI-Verordnung: Warum Weiterbildung eine rechtliche Pflicht ist

Künstliche Intelligenz prägt zunehmend den Büroalltag. Für Verantwortliche in Unternehmen muss ein Thema ganz oben auf der Agenda stehen. Die gesetzliche Pflicht, die KI-Kompetenz der Belegschaft systematisch aufzubauen. Was auf Unternehmen wie ein reines Fortbildungsthema wirkt, ist tatsächlich eine strikte rechtliche Vorgabe.

Die Grundlage liefert Artikel 4 des europäischen AI-Acts (KI-Verordnung), der seit Februar 2025 gilt. Er verpflichtet alle Unternehmen, die KI-Systeme einsetzen – ob gewollt oder ungewollt –, eine angemessene KI-Kompetenz bei ihren Mitarbeitenden zu gewährleisten. Beschäftigte müssen Risiken, Datenverarbeitung und rechtliche Grenzen der Werkzeuge realistisch einschätzen können. Wer diese Pflicht vernachlässigt, riskiert bei Folgefehlern wie Datenlecks drakonische Strafen von bis zu 35 Millionen Euro oder sieben Prozent des weltweiten Jahresumsatzes.

Die Bundesnetzagentur als zuständige Marktüberwachungsbehörde hat ihre Erwartungen in einem Hinweispapier konkretisiert. Sie fordert einen strukturierten Vier-Schritte-Prozess: Bedarf ermitteln, Schulungen zielgruppenspezifisch gestalten, diese laufend aktualisieren und die Wirksamkeit überprüfen. Zudem empfiehlt die Behörde dringend eine lückenlose Dokumentation der Maßnahmen, um bei Prüfungen rechtssicher aufgestellt zu sein.

Die Realität in Deutschland hinkt dieser Pflicht jedoch hinterher. Laut aktuellen Bitkom-Zahlen nutzen bereits 57 Prozent der Unternehmen künstliche Intelligenz, doch ein Viertel verzichtet komplett auf KI-Weiterbildung. Dabei entstehen gefährliche Kompetenzinseln, wenn nur IT-Spezialisten geschult werden. Die Unsicherheit ist groß: Für 66 Prozent der Betriebe ist der Datenschutz das größte Hemmnis beim KI-Einsatz. Zudem droht ohne Schulung die unbewusste Einspeisung von Geschäftsgeheimnissen in öffentliche Tools.
Unternehmen müssen nun zeitnah handeln. Die bestehenden KI-Systeme – eine eventuelle Schatten-IT eingeschlossen – müssen analysiert werden, um den Beschäftigten maßgeschneiderte Schulungen zu Datenschutz, Urheberrecht und Informationssicherheit an die Hand zu geben. Flankiert werden sollte dies von klaren internen KI-Nutzungsrichtlinien. Durch diese Verzahnung werden gesetzliche Vorgaben erfüllt, Haftungsrisiken minimiert und unkalkulierbare Sicherheitsrisiken in digitale Wettbewerbsvorteile verwandelt.

Hinweispapier: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/Hinweispapier.pdf?__blob=publicationFile&v=2

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.