DEEP DIVE

TaylorWessing

DIGITAL LEGAL ACADEMY 2025

Ready for AI – vom Hype zum Business

KI-Implementierung in Unternehmen

Dr. Jakob Horn

Dr. Christian Frank

Status quo: KI auf dem Vormarsch

DEEP DIVE DIGITAL LEGAL ACADEMY 2025 by TaylorWessing

Ifo Institut

40,9%

der Unternehmen verwenden KI in Geschäftsprozessen (Vorjahr: 27%)

Ifo Institut (ifo Konjunkturumfrage, 16. Juni 2025) (Quelle: https://www.ifo.de/fakten/2025-06-16/unternehmen-setzen-immer-staerker-auf-kuenstliche-intelligenz)

IW Köln

37%

setzen KI ein (66% bei Großen Unternehmen, 36% bei kleinen Unternehmen)

IW Köln (IW-Report Nr. 33, 4. Juli 2025, Quelle: https://www.iwkoeln.de/studien/barbara-engels-marc-scheufen-edgar-schmitz-kuenstliche-intelligenz-als-wettbewerbsfaktor-fuer-die-deutsche-wirtschaft.html)

Bitkom

42%

der Unternehmen setzen KI in der Produktion ein

8 von 10

gehen davon aus, dass KI entscheidend sein wird für Erfolg der deutschen Wirtschaft

Bitkom (Presseinformation, 27. März 2025, Quelle:https://www.bitkom.org/Presse/Presseinformation/Industrie-4.0-Unternehmen-KI-Produktion)

DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

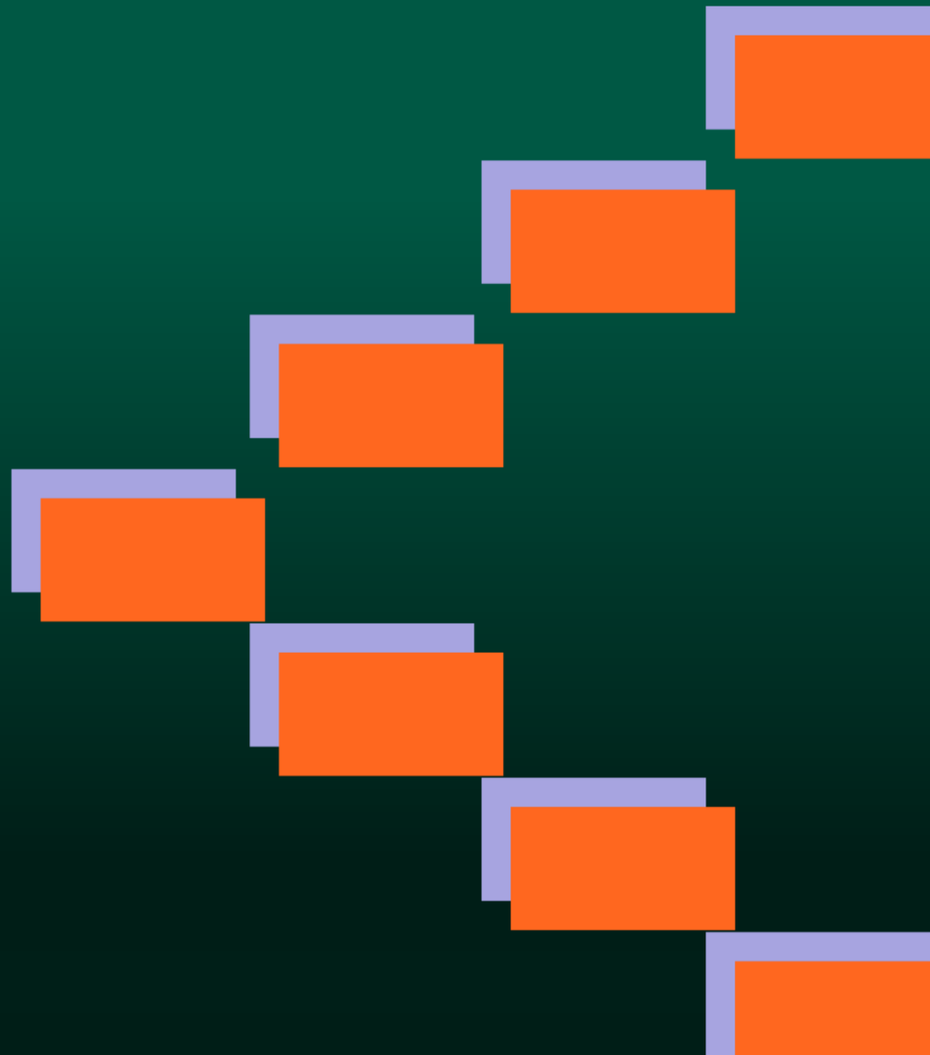
???

Bitte nehmen Sie an der Umfrage teil

Agenda

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

1	**Grundlagen**
	AI Mapping
	Rollen
	Deep Dive: Überschreitung der Akteursgrenzen
2	**Rechtliche Schwerpunktthemen**
	Deep Dive: EU AI Act vs EU Product Liability Directive
	Deep Dive: EU AI Act vs DSGVO
	Deep Dive: AI Agents
3	**Praktische Tipps (Anhang)**
4	**Fragen**



DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

1 Grundlagen

AI Mapping

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Grundlage der AI Governance

⇒ KI-Definition im AI Act sehr weit: KI-Einsatz bleibt ggf. unbemerkt
⇒ Alle Unternehmensteile einbeziehen, um Überblick über KI-Einsatz zu gewinnen
⇒ Synergieeffekt nutzen: nicht nur Compliance fördern, sondern auch Einsatzpotentiale erkennen

Wo wird KI im Unternehmen eingesetzt?

KI eingebettet in Produkten (vgl. Anh. I AI Act)

z.B. als Sicherheitsbauteil in

- Maschinen
- Aufzüge
- Fahrzeuge
- Funkanlagen
- Verbrennungsanlagen
- Medizinprodukte

Standalone-KI-Software (vgl. Anh. III AI Act)

z.B.

- Generative KI (LLMs, Bildgenerierung)
- Biometrische Verifizierungssysteme
- Personalentscheidungssysteme
- IT-Sicherheitssoftware
- Übersetzungsprogramme
- Expertensysteme
- Automatisierte Bilderfassung

AI Act – In-Kraft-Treten

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

AI-Act tritt in Kraft

Entwurf Gesetz zur Durchführung der KI-Verordnung veröffentlicht

Regelungen über Hochrisiko-Systeme, die sicherheitsrelevanter Teil regulierter Produkte sind (Anhang I) + entsprechende Pflichten treten in Kraft – Konformitätszeitpunkt für KI-Systeme, die vor dem 2. August 2025 auf den Markt gebracht wurden

1.8.2024 | 2.2.2025 | 2.8.2025 | 12.9.2025 | **2.8.2026** | 2.8.2027

Regeln zu verbotenen Praktiken treten in Kraft

Bestimmungen für KI-Modelle mit allgemeinem Verwendungszweck („GPAI-Modell“) und Kernpflichten zu Governance, Notifizierung, Strafen sind anwendbar

Genereller Geltungsbeginn (insb. die Regelungen über Hochrisiko-Systeme (Anhang III) + die Transparenzpflichten gemäß Art. 50)

AI Act – Regelungsansätze

DEEP DIVE DIGITAL LEGAL ACADEMY 2025 by TaylorWessing

Risikoeinteilung

Verboten
- Sollte nicht eingesetzt werden
- Jedoch: nur wenige Anwendungsfälle

Hochriskant
- Kernfokus der Regulierung
- Hauptanwendungsfall: Personalangelegenheiten

gering/minimal
- Wenige oder keine Regulierungsvorgaben

Einteilung der Hauptakteure

Anbieter von KI-Modellen („Upstream Provider“)
- Entwickelt oder vertreibt ein KI-Modell auf dem Markt
- Reguliert sind nur bestimmte KI-Modelle (sog. GPAI-Modelle)

Anbieter von KI-Systemen (Software mit KI)
- Entwickelt oder vertreibt ein KI-System auf dem Markt
- Reguliert sind nur bestimmte KI-Systeme, insbesondere die sog. Hochrisiko-KI-Systeme

Betreiber
- Nutzt ein KI-System im eigenen Unternehmen und setzt es für konkrete Zwecke ein

Ziel von AI Governance in diesem Kontext

Feststellen, welche Risikoklasse und welcher Akteur ➡ hilft, die weiteren Weichen zu stellen.

AI Act – Überschreitung der „Akteursgrenzen“

DEEP DIVE DIGITAL LEGAL ACADEMY 2025 by TaylorWessing

Problem:
Bei unzureichenden Maßnahmen kann Betreiber wie ein Anbieter behandelt werden.

Aus Anbietersicht: Kooperationspflichten können Geschäftsgeheimnisse gefährden

Vor allem drei Szenarien:

Szenario 1: White labeling (Art. 25 Abs. 1 lit. a) AI Act)

- Einkauf von Software mit KI und Branding der KI mit eigenem Logo
- Beispiel: Personalwirtschaftssystem oder Recruiting Tool, auf das eigenes Logo angebracht wird.

Szenario 2: Wesentliche Änderung an bereits in Verkehr befindlichen KI-System, sodass es weiterhin Hochrisiko bleibt (Art. 25. Abs. 1 lit. b) AI Act)

- Beispiel: Anbieter kauft Lizenzen eines HR KI-Systems, installiert das System bei Kunden und erweitert es um neue Submodule und erweitert Einsatzzweck enthaltener Module

Szenario 3: Verwendung eines allgemeinen KI-Tools für Hochrisiko-Zweck (Art. 25. Abs. 1 lit. c) AI Act)

- Beispiel: Mitarbeiter lädt Lebensläufe in Chatbot, um sich Ranking für Personalauswahl erstellen zu lassen.
- Problem: Nutzung durch Mitarbeiter kann ungewollt zu Compliance-Verstoß führen

Vorsichtsmaßnahmen:

- Bei Einkauf von KI ausreichende Prüfung der gekauften Software (insb. bei White Labeling)
- Kooperationsregeln und Haftungsklauseln in Verträgen anpassen
- Richtlinien für KI-Einsatz erstellen, Mitarbeiter schulen, ggf. technische Maßnahmen ergreifen.

DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

2 Rechtliche Schwerpunktthemen

EU AI Act vs EU Product Liability Directive

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

8.12.2024: EU-ProduktHaftungsRL 2024/2853 in Kraft, umzusetzen bis 9.12.2026

11.9.2025: Veröffentlichung Referentenentwurf Gesetz zur Modernisierung des Produkthaftungsrechts

- Erweiterter Produktbegriff: „Produkt“ = auch Software, KI-Systeme, Updates, digitale Dienstleistungen, inkl kommerziell eingebundene OS
- Verantwortlichkeit Hersteller für Aufrechterhaltung Sicherheit: Fehlerhafte/unterlassene Updates → Haftungsfall.
- Beweislastumkehr / erleichterte Beweisführung für Geschädigte: Offenlegungspflichten in Art. 9 und Vermutungen in Art. 10 PLD
- Ausweitung des Schadensbegriffs: Auch Datenverluste, Datenschutzverletzungen, Art. 6 I c PLD + Relevanz algorithmischer Fehlentscheidungen (Rec 32) .
- Wichtig: Hier keine Differenzierung nach Hochrisiko

EU AI Act vs EU Product Liability Directive

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Prozesse AI Governance & Produkthaftung konsistent gestalten!

AI Act Dokumentation

- Beispiel: Bias-Prüfung im Trainingsdatensatz
- Beispiel: Incident Reporting und Logging

- Neutraler Sprachstil
- Prozesse statt Fehler
- Separate Dokumentationen
- Konsistenzcheck

Lifecycle Management

- Kontrollgrenzen sauber definieren + dokumentieren
- Keine Selbstverpflichtungsfalle
- Sicherheitsrecht priorisieren
- "Wesentliche Änderungen" als Gate

Verträge Lieferkette anpassen

- Freistellungsklauseln
- Updates, Info zu Sicherheitslücken+ Patches
- Dokumentations- und Informationspflichten
- Compliance Standards, Audits, Kündigungsrechte
- Versicherungsnachweis

EU AI Act vs DSGVO

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Unterschiedliche Zielsetzungen

AI Act:

Sicherheit, Transparenz, Fairness, Risikomanagement von KI-Systemen, aber auch Innovation. Vgl. z.B.

- Art. 10 AI Act: hochwertige Trainingsdaten
- Art. 12 AI Act: Logging und Monitoring

DSGVO:

Schutz personenbezogener Daten und Grundrechte

- Art. 5 I (c) DSGVO: Datenminimierung und Zweckbindung
- Art. 17 DSGVO: Löschung => bei generativem KI-Modell praktisch unmöglich

Darüber hinaus

✓ Unternehmensinteresse am Schutz von Geschäftsgeheimnissen
- Sowohl Geschäftsgeheimnisse, die sich auf Details von KI-Systemen beziehen
- Als auch Schutz bei Verarbeitung von Daten mit Hilfe von KI

EU AI Act vs DSGVO

DEEP DIVE DIGITAL LEGAL ACADEMY 2025 by TaylorWessing

Beispiel 1: KI-Training mit personenbezogen Daten

AI Act:

verlangt z.B. Prüfung auf Diskriminierung (Art. 10 II f) AI Act) → benötigt sensible personenbezogene Daten

DSGVO:

verbietet oder schränkt Verarbeitung sensibler Daten massiv ein. Aber:

- unter engen Voraussetzungen Ausnahme nach Art. 10 V AI Act
- OLG Köln: weitreichende Zulassung von KI-Training mit Nutzerdaten

- Datenschutzkonformes Bias-Management
  - Bei Entwicklung bereits rechtliche Anforderungen im Blick haben
  - Bias-Kontrollen möglichst mit anonymisierten / pseudonymisierten Daten, es sei denn Art. 10 V AI Act ist einschlägig
  - Datenschutz-Folgenabschätzungen (DSFA) eng mit AI-Risikoanalysen verzahnen

- Aus Betreibersicht:
  - Ausreichende Haftungsregelung bei Verletzung vereinbaren (z.B. kann KI-Modell personenbezogene Daten Dritter aufdrängen)

EU AI Act vs DSGVO

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Beispiel 2: Incident Response

AI Act:

schwerwiegender Vorfall → Meldung an Behörden (Art. 73 AI Act)

Betreiber: ggf. Meldung auch bei Verdacht auf Risiko (Art. 26 V AI Act)

DSGVO:

Meldung von Datenschutzverletzungen (Art. 33 DSGVO).

Geheimnisschutz:

Preisgabe internes Wissen über Modellschwächen → möglicher Verlust von Geheimnisschutz.

=> Art. 78 I a) AI Act schützt zwar auch Geschäftsgeheimnisse, aber hier sollte Vorsorge getroffen sein.

- Interne Governance-Verzahnung
  - DSB, Informationssicherheitsbeauftragter und AI-Compliance-Team müssen eng kooperieren
  - Meldeprozesse ggf. aktualisieren, um Meldepflichten nach AI Act und DSGVO im Blick zu haben.
  - Geschäftsgeheimnisse, die bei Meldung offen gelegt werden können im Vorfeld identifizieren und markieren.

EU AI Act vs DSGVO

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Weitere DSGVO Themen

Art. 22 DSGVO

Automatisierte Entscheidung & Profiling

- Gilt auch bei Nicht-Hochrisiko-KI (und selbst ohne KI)
- Beispiel: MatchScores bei Recruiting Tools können zu automatischer Entscheidungsfindung führen

Beachte

- Rollen nach AI Act und DSGVO nicht deckungsgleich
- Anbieter und Betreiber ⇔ Verantwortlicher und Auftragsverarbeiter beliebig kombinierbar

AI Agents

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

- System nimmt selbst Handlungen vor, um bestimmtes Ziel zu erreichen.
  - Keine gesonderte Regelung ► = KI-System, Art. 5ff + 50, 51ff.
- Eigene Rolle klären: Anbieter /Betreiber/Nachgelagerter Anbieter
- Mehrstufiges Vorgehen:

Step 1 Konzeption
- Risikoeinordnung, bei HR insb. Art. 9 + 14
- Integration GPAI: technische Dok (Anhang XI/XIII) vertraglich sichern
- Eigene technische Dok + KI-Kompetenz Schulung

Step 2 Betrieb vorbereiten
- DSGVO:
  - Grundlage Verarbeitung
  - Art. 22
  - DSFA
- § 87 I Nr. 6 BetrVG
- Transparenzpflichten
- Nutzungsrichtlinien intern

Step 3 bei Vermarktung
- Art. 3 Nr. 28
- Vertragl. Pflichten ggü. Kunden
- Produktsicherheit
- Registrierungspflicht checken

AI Agents

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

- Aktivitäten des AI Agents sollen rechtsgeschäftliche Wirkungen erzielen können …
  - Keine ePerson, rechtliche Grundlage Zurechnung umstritten

- Unklare Gesetzeslage durch vertragliche Systeme mit entsprechenden Regelungen ausgleichen

Zurechnung
- Handlungen, Entscheidungen und Ausgaben des KI-Agenten gelten als Handlungen desjenigen, der den KI-Agent für seine Zwecke einsetzt.
- Funktionsbegrenzungen absichern und ggf. offenlegen.
- Ggf. Bestätigungspflichten und Verfahren für bestimmte Bereiche konzipieren

Risikoverteilung
- Anbieter vs Betreiber
- Pflichten zur Bereitstellung technischer Dokumentation Agent und zur Dokumentation des Einsatzes.
- Freistellungspflichten und Haftungsbegrenzungen.
- Aufbewahrungspflichten + Audits

Kontrolle
- Suspendierung und Kill Switch?
- Art. 9 + Art. 25: Verfahren für Informations- und Bewertungspflichten

DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

3 Praktische Tipps

(Anhang)

Verträge prüfen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Grundsätzlich ist der Vertrag zwischen Anbieter und Betreiber ein „normaler“ Softwarenutzungsvertrag

Besonderheiten:

Supplier Screening

- Einstufung als Hochrisiko-KI?
- Entspricht der Anbieter dem AI Act?
- Wird Betriebsanleitung bereitgestellt?
- Sind Vorkehrungen für die menschliche Aufsicht vorgesehen?
- Notwendige Dokumentation vorhanden?

Verträge prüfen

- Rollendefinition klar stellen (z.B. White Labeling kann Risiken nach sich ziehen)
- Erfüllung der Verpflichtungen nach AI Act bei Hochrisiko-KI sicherstellen
- Nutzung von Kundendaten für KI-Training ausschließen
- Verteilung der IP-Rechte an KI-Output

Compliance Fragebögen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

- Verbotene und Hoch-Risiko-KI identifizieren
- Transparenzverpflichtungen identifizieren (sehr begrenzt auch für Betreiber (also Nutzer))
- Eigene Rolle identifizieren
- Prüfen, ob Compliance eingehalten wird (Unternehmen selbst oder Vertragspartner)

AI Governance – Zentrale Fragestellungen

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Zuständigkeiten definieren
- Welche Einrichtungen gibt es schon?
- Braucht es ein eigenes AI Committee oder kann z.B. Legal die Aufgaben übernehmen?
- Wer soll dem Committee angehören?

Risiko-Definition:
- Soll KI eher proaktiv eingesetzt werden, auch zum Experimentieren oder soll es eher vorsichtig voran gehen, um Compliance-Risiken zu minimieren?

Aufgaben definieren
- Risiken identifizieren und Maßnahmen planen (z.B. Schutz eigener Geschäftsgeheimnisse bei Meldung eines Datenschutzverstoßes)
- Welche Aufgaben gibt es?
- Wer übernimmt was?

DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

4 Fragen

DEEP DIVE

DIGITAL LEGAL ACADEMY 2025

by TaylorWessing

???

Bitte nehmen Sie an der Umfrage teil

Ihre Ansprechpartner

DEEP DIVE
DIGITAL LEGAL ACADEMY 2025
by TaylorWessing

Dr. Christian Frank,
Licencié en droit

Partner

Dr. Jakob Horn,
LL.M. (Harvard)

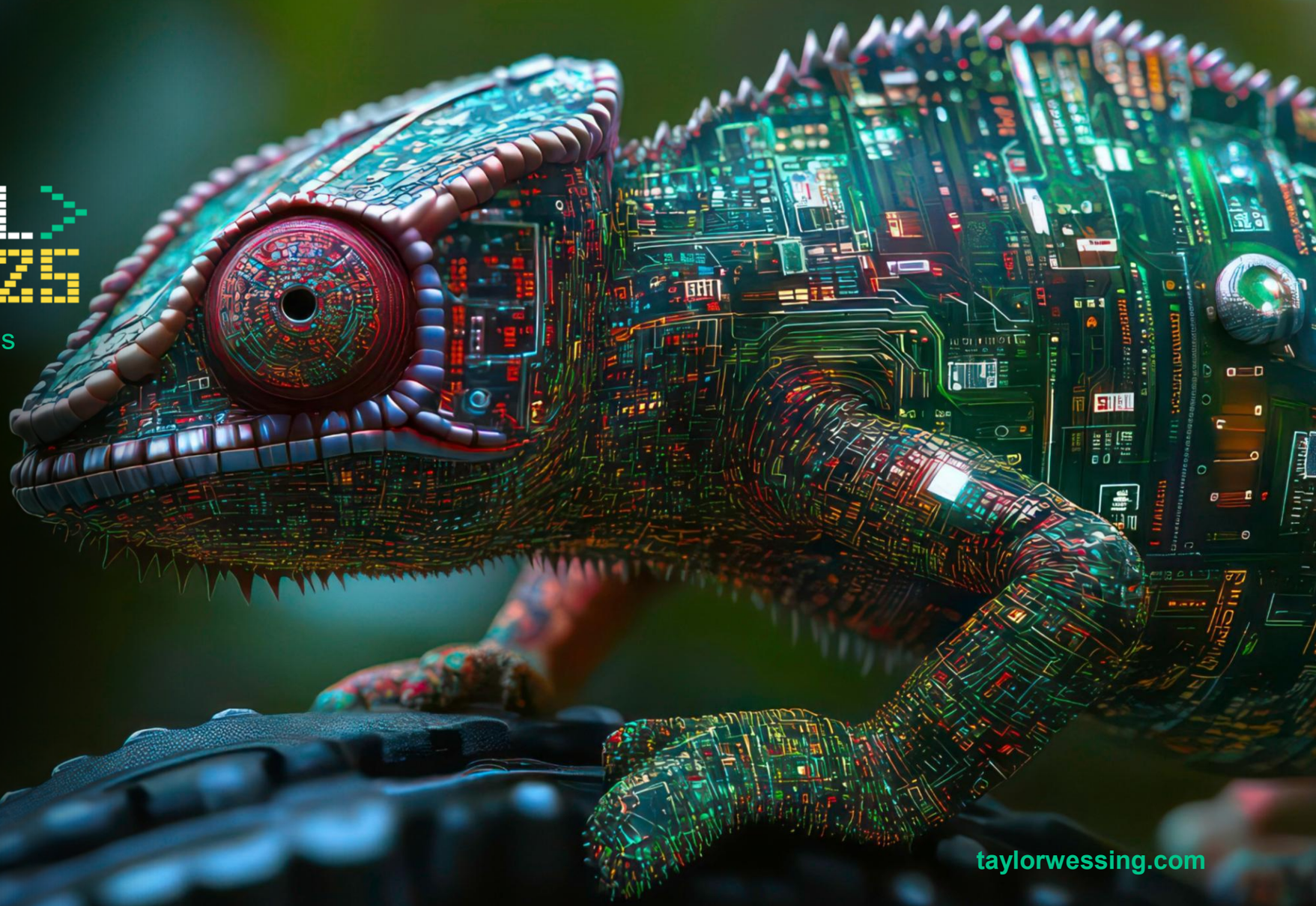
Associate

DEEP DIVE

TaylorWessing

DIGITAL LEGAL ACADEMY 2025

Ready for AI – vom Hype zum Business



taylorwessing.com