



White Paper

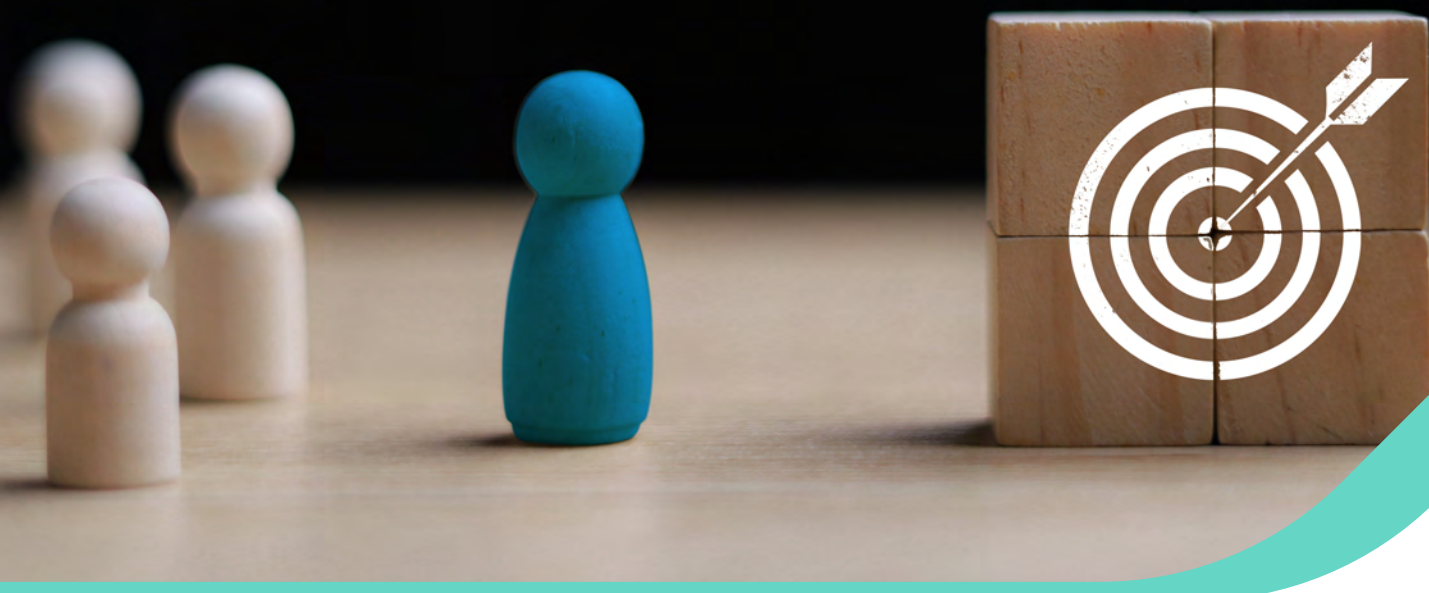
EU AI Act

Checkliste zur Umsetzung für Legal Teams



Die **EU AI Act** steht vor der Tür –

und sie verändert die Spielregeln. Von Risikoklassifizierungen bis hin zu Transparenzpflichten: Rechtsabteilungen werden eine Schlüsselrolle dabei spielen, Unternehmen sicher durch diese neue Regulierung zu führen. Wer jetzt handelt, minimiert Risiken und baut Vertrauen auf – intern wie extern.



Prüfen Sie jetzt hier, was Ihr Team bis wann erledigen muss, um vorbereitet zu sein.

Überblick

Bis August 2025

Transparenzpflichten für General Purpose AI (GPAI)

Bis August 2026

Vollständige Compliance für Hochrisiko-KI

Bis August 2027

Frist für bestehende („Legacy“) KI-Systeme



2025

Bis August 2025: **Transparenzpflichten für** **General Purpose AI (GPAI)**

- KI-generierte Inhalte klar kennzeichnen
- Offenlegung von Trainingsdaten, Risiken und Einschränkungen gewährleisten
- Urheberrechte prüfen und wahren
- Kommunikationsstrategien anpassen (z. B. interne/externe Kommunikation)
- Transparenzhinweise in Tools, Websites und Dokumente integrieren
- Lizenz- und Nutzungsvereinbarungen überprüfen (inkl. SaaS & Drittanbieter)
- Transparenzrichtlinien speziell für GPAI entwickeln
- Legal Review laufender Tools bzgl. Urheberrecht, Daten- und Kennzeichnungspflichten durchführen
- Informationspflichten für Nutzer:innen umsetzen



2026

Bis August 2026: Vollständige Compliance für Hochrisiko-KI

KI-Landschaft erfassen & klassifizieren

- Vollständige Inventur aller eingesetzten KI-Systeme (inkl. SaaS & Drittanbieter).
- Einstufung nach EU AI Act-Risikokategorien: Unvertretbar – Hoch – Begrenzt – Minimal.
- Zentrale Dokumentation aller Systeme, jederzeit auditfähig.

Governance & Verantwortlichkeiten aufbauen

- Multidisziplinäres Team etablieren (Legal, IT, Data, Ethics).
- Einen AI Compliance Officer benennen.
- Verantwortlichkeiten, Freigabe- und Auditprozesse klar definieren.

Risikobewertung & Impact Assessments

- Durchführung von AI Impact Assessments (auch freiwillig bei nicht-hochriskanten Systemen).
- Erfassung juristischer & ethischer Risiken (z. B. Diskriminierung, Haftung, Transparenz).
- Compliance-Prozesse und Kontrollmechanismen für Hochrisiko-KI implementieren.

Verträge anpassen & absichern

- Vendor-Agreements auf AI-Act-Klauseln prüfen und aktualisieren.
- Haftung, Datenschutz, Audit-Rechte, Datenqualität und Support verbindlich absichern.

Awareness & Training

- Juristische und technische Schulungen für Legal, Compliance & Entwickler starten.
- Interne Leitlinien für verantwortungsvollen KI-Einsatz verabschieden.

Technische & organisatorische Anforderungen

- Daten- und Qualitätsmanagement sicherstellen.
- Vollständige technische Dokumentation aller Hochrisiko-Systeme erstellen.
- Menschliche Aufsicht (Human Oversight) und Erklärbarkeit der Systeme gewährleisten.
- Kennzeichnungspflichten für Systeme mit begrenztem Risiko umsetzen.

Registrierung & Auditierbarkeit

- Alle Hochrisiko-KI-Systeme fristgerecht in der EU-Datenbank registrieren.
- Auditierbarkeit sicherstellen: Logging, Dokumentation & systematische Kontrollmechanismen implementieren.



2027

Bis August 2027: Frist für bestehende („Legacy“) KI-Systeme

Vollständige Compliance für Hochrisiko-Systeme

- Anforderungen nachweisen: Daten-Governance, Dokumentation, Logging, Transparenz, Human Oversight, Robustheit & Cybersecurity.
- Nachklassifizierung aller bestehenden Systeme durchführen.
- Fehlende Dokumentationen und Transparenzmaßnahmen ergänzen.

Konformitätsbewertungen & CE-Kennzeichnung

- Hochrisiko-Systeme durch interne Verfahren oder Notified Bodies prüfen lassen.
- CE-Kennzeichnung sicherstellen, wo erforderlich.

Registrierung & Risikoanalysen

- Alle Hochrisiko-KI-Systeme fristgerecht in der EU-Datenbank anmelden.
- Risikoanalysen für bestehende Systeme nachholen.

Audits & Kontrollmechanismen

- Interne Audits durchführen, um Kontrollfähigkeit und Auditierbarkeit nachzuweisen.
- Systematische Kontrollmechanismen für kontinuierliche Überprüfung fest etablieren.

Beschwerde- & Vorfallmanagement

- Interne Meldekanäle für KI-Vorfälle und Beschwerden einrichten.
- Prozesse zur Benachrichtigung von Behörden bei schwerwiegenden Incidents sicherstellen.
- Zusammenarbeit mit Aufsichtsbehörden aktiv vorbereiten.

Monitoring & Update-Prozesse

- Ongoing Monitoring etablieren: regelmäßige Compliance-Überprüfungen (jährlich oder bei relevanten Änderungen).
- Update-Policy für KI-Systeme implementieren, inkl. Dokumentationspflichten.

Strategische Umsetzung

- KI-Inventur und Risikoklassifikation (laufend aktualisieren)
- Interne Richtlinien & Governance anpassen
- Technische und juristische Dokumentation erstellen und pflegen
- Verträge & Lieferantenbeziehungen regelmäßig überprüfen und anpassen
- Schulungsprogramme implementieren und fortlaufend aktualisieren
- Monitoring- und Audit-Mechanismen einrichten und nutzen

Legal Tech Unterstützung

⚠ Herausforderung

- KI-Inventur & Klassifikation

- Vertragsprüfung

- Auditierbarkeit

- Schulung

- Governance & Verantwortung

ℹ Lösung

- Risiko-Mapping Tools

- Automatisierte Vertragsanalyse

- Compliance-Dashboards mit Echtzeitstatus

- Digitale Lernplattform

- Digitale Tools zur Rollenverteilung

Sanktionen bei Nichteinhaltung

- **Verbote von KI-Systemen:**
bis zu 35 Mio. € oder 7 %
des weltweiten Jahresumsatzes
- **Verstöße gegen Hochrisiko-Pflichten:**
bis zu 15 Mio. € oder 3 %
des Jahresumsatzes
- **Falsche oder verweigerte Auskünfte:**
bis zu 7,5 Mio. € oder 1 %
des Jahresumsatzes

Letzter Checkpoint

Erfolg unter dem EU AI Act kommt nicht allein durch Papierarbeit. Die Gewinner sind diejenigen, die Legal Tech nutzen: Workflows automatisieren, Risiken sofort erkennen und Wissen genau dann abrufen, wenn es gebraucht wird. Compliance bedeutet nicht mehr nur, Strafen zu vermeiden – es geht darum, Vertrauen, Effizienz und zukunftsichere Prozesse aufzubauen.

Hier machen die stp.one Lösungen den Unterschied.

Fragen Sie sich

- Verwalten wir alle Workflows, Zeiten, Abrechnungen und Compliance-Dokumente in einem smarten Hub?
- Können wir AI-bezogene Risiken in unseren Verträgen sofort erkennen und verstehen?
- Rufen wir das richtige Compliance-Wissen genau dann ab, wenn wir es brauchen?
- Wenn Sie bei einer dieser Fragen zögern, ist es Zeit zu handeln. Wie? Werfen Sie einen genauen Blick auf unsere **stp.one** Softwarelösungen.

Unsere Experten begleiten Sie auf Ihrem Weg zum Erfolg!.

**Jetzt mit einem Digitalisierungs-
Experten sprechen:**
+49 721 82815-0

Oder schreiben Sie uns:
info@stp.one





STP Informationstechnologie GmbH • Brauerstraße 12 • 76135 Karlsruhe

+ 49 721 828 15 0 | info@stp.one

stp.one

**Behind
every
moment
of life.**