DORDA

Hochrisiko-KI

in der Bonitätsbewertung, HR, Biometrie und kritischen Infrastruktur

17.6.2026

Axel Anderl | Alexandra Ciarnau

Partner und Leiter des IT/IP und Datenschutzteams

- Schwerpunkte: IT- und IP-Recht, insbesondere Out- und Cloudsourcing, Cybersecurity, Urheberrechtsabgabe und Kunstrecht
- Empfohlen als first tier für IT, IP und Datenschutz bei Legal500 und IT und IP bei Chambers Europe, Legal500 Hall of Fame für TMT, Leading Individual für IP bei JUVE, TIER 1 Media Law International 2025, zwölf ILO Client Choice Award für Information Technology & Internet
- Universität Wien (Dr iur 2005) und Universitätslehrgang für Informationsrecht und Rechtsinformation (LL.M. 2001)
- Autor zahlreicher Fachpublikationen, ua IP in der Praxis (Manz), #blockchain (LexisNexis), #Cybercrime (LexisNexis), Handbuch UWG (Linde), KI-VO Kurzkommentar (Manz)
- Vortragender an zahlreichen (Fach-)Hochschulen sowie bei diversen Seminaranbietern
- Board-Mitglied von ITechLaw und Co-Chair Start-Up Committee

Axel Anderl

axel.anderl@dorda.at

Partner im IT/IP und Datenschutzteam und Co-Leiterin der Digital Industries Group

- Schwerpunkte: IT- und Datenschutzrecht, New Technology, E-Commerce
- Highly recommended für Artificial Intelligence bei Lexology 2025, Leading Associate für TMT in Legal 500 2025, Green Ambassador im Legal 500 Green Guide 2025, Trademark Star in IP Stars 2024, Empfohlen für Data:Information Technology bei Client Choice 2025
- Co-Herausgeberin der ailex (Fachzeitschrift für KI-Recht, Manz)
- Co-Autorin der Werke KI-VO Kurzkommentar (Manz), KI Praxishandbuch (Hanser), IP in der Praxis (Manz), UWG Praxishandbuchs (Linde), Handbuch Nachhaltigkeitsrecht (Manz), Handbuch Kreislaufwirtschaft (Linde), #Blockchain (LexisNexis), Praxishandbuch Nachhaltige Finanzierung (Linde)
- Vortragender an zahlreichen (Fach-)Hochschulen sowie bei diversen Seminaranbietern
- Präsidentin von Women in AI Austria
- Standortleiterin DORDA sphere

Alexandra Ciarnau

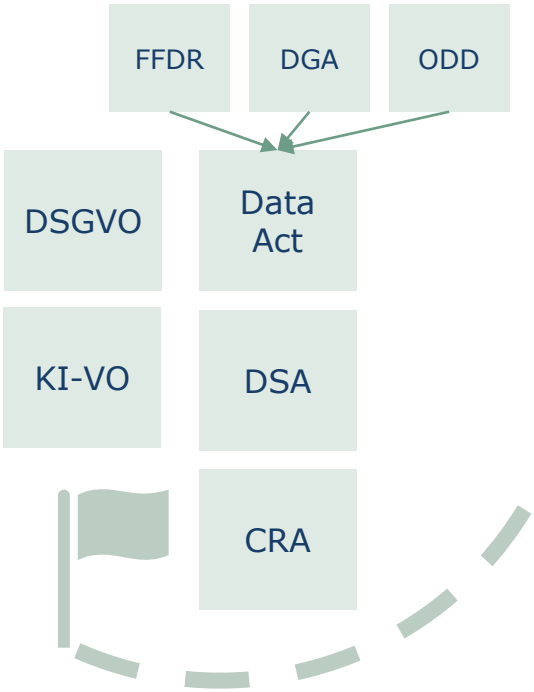
alexandra.ciarnau@dorda.at

Agenda

- Neue Entwicklungen: Digitaler Omnibus & KI-VO
- Kontextbezogene Hochrisiko-KI-Systeme und Abgrenzungsfragen bei der Klassifizierung
- Widerlegung der Klassifizierung
- Konformitätsbewertungsverfahren, CE-Kennzeichnung und Marktüberwachung
- Betreiber- und Anbieterpflichten
- Veränderungen in der Risikolandschaft

Politische Einigung zum Digitalen Omnibus – Anpassungen der KI-VO

Digitales Omnibus Paket



19.11.2025
Vorschlag des Digitalen Omnibus-Pakets

7.5.2026
Politische Einigung zur Anpassung der KI-VO

Next Steps
- Billigung durch Rat und Parlament
- Redaktionelle Überarbeitung
- Formelle Verabschiedung

Geplante Änderungen der KI-VO

Fristen

	Ursprüngliche Frist	Neue Frist
Verbotene Praktiken Neuer Tatbestand zu „Nudifier"-Apps und KI-generierter Kindesmissbrauchsinhalt	seit 2.2.2025 n/a	n/a ab 2.12.2026
Kontextbezogene Hochrisiko-KI-Systeme	2.8.2026	2.12.2027
Produktbezogene Hochrisiko-KI-Systeme	2.8.2027	2.8.2028
Transparenzpflichten nach Art 50 ausgenommen für Abs 2 – maschinenlesbare Kennzeichnung durch Anbieter von bestehenden Systemen	2.8.2026	n/a 2.12.2026
Regulatorische Reallabore	2.8.2026	2.8.2027

KI-Omnibus

KI-Kompetenz

- Kein bestimmtes Kompetenzniveau
- Verpflichtung um Bemühen
- Leitlinien der Kommission folgen
- Erhebliche Schwächung der zentralen Bestimmung

Verbotene KI-Praktiken

- Erweiterung um sexualisierte Deepfakes
- Bereits im allgemeinen Persönlichkeitsrecht verankert

KI-Omnibus

Hochrisiko-KI-Systeme

- Verschiebung Umsetzungsfristen auf 2.8.2027 bzw 2.8.2028
- Registrierungspflicht auch bei Widerlegung der Klassifizierung

Bestimmte KI-Systeme

- KI-generierter Inhalte bei Bestandsystemen bis 2.12.2026

KMU

- KMU-Erleichterungen künftig auch für "Small Mid-Caps" (< 750 Mitarbeiter; Umsatz ≤ EUR 150 Mio oder Bilanzsumme ≤ EUR 129 Mio)

Kontextbezogene Hochrisiko-KI-Systeme

Hochrisiko-KI

Produktbezogen

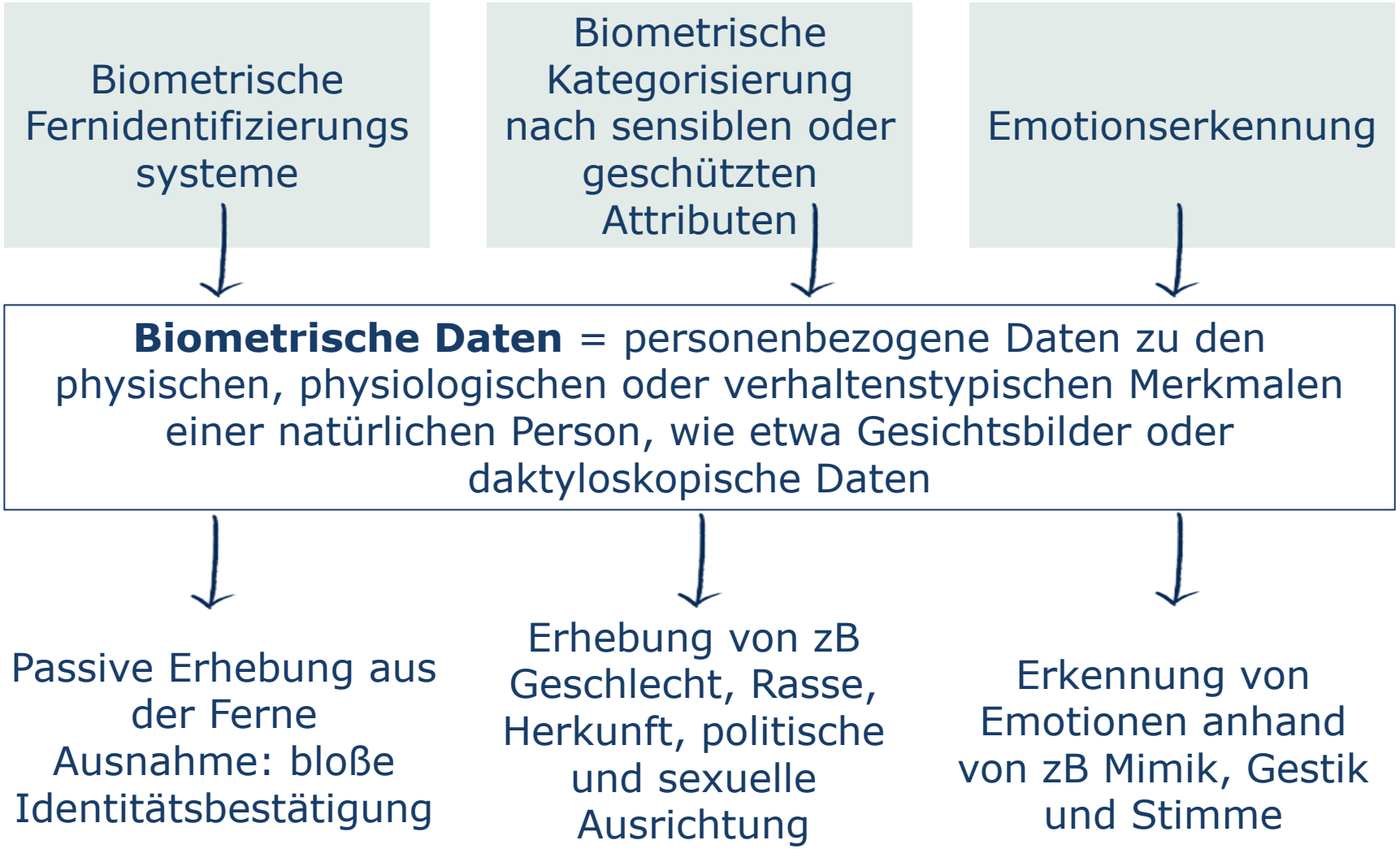
KI als reguliertes Produkt oder Sicherheitsbauteil in einem regulierten Produkt

Kontextbezogen

KI in einem „sensiblen Kontext“

→ Vermutung des Gesetzgebers

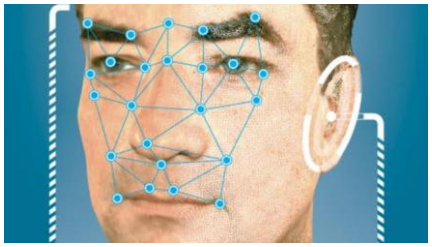
Biometrie – Anhang III Z 1



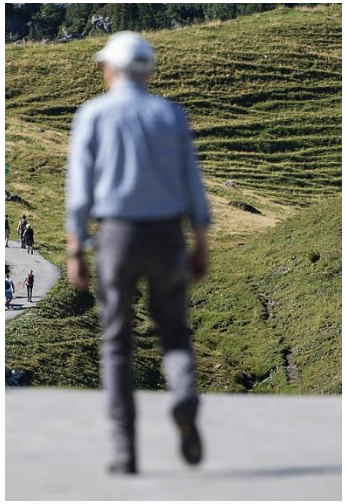
Beispiele biometrischer Kategorisierung

Biometrische Kategorisierung

- Beispiele in der Medizin



Rückschlüsse auf genetische oder psychologische Krankheiten auf Basis von Gesichtsmimik und -biometrie



Rückschlüsse auf neurologische Krankheiten auf Basis von Verhaltensmerkmalen (zB Gang, Bewegungen)

Beispiele der Emotionserkennung

Emotionserkennung

- Beispiele aus Marketing und Sales

→ Erkennung von Reaktionen und Emotionen anhand der Biometrie bei Werbevideos

- Beispiele aus Gaming

→ Gesichtsvermessung, Bewegungsbiometrie, Körperproportionen und Erkennung von Emotionen anhand von Mimik und Gestik

Abgrenzungsfragen zu verbotenen Praktiken

Verbote

Biometrische Fernidentifizierungssysteme	→ Art 5 lit h: biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken
Biometrische Kategorisierung nach sensiblen oder geschützten Attributen	→ Art 5 lit d: Racial Profiling Art 5 lit g: biometrische Kategorisierung individuell anhand biometrischer Daten Kategorisierung und Ableitung sensibler Attribute
Emotionserkennung	→ Art 5 lit f: Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen

Kritische Infrastruktur – Anhang III Z 2

Betroffene Bereiche

- Kritische digitale Infrastruktur
- Straßenverkehr
- Wasser-, Gas-, Wärmeversorgung

Grundvoraussetzung = KI-Systeme als Sicherheitsbauteil

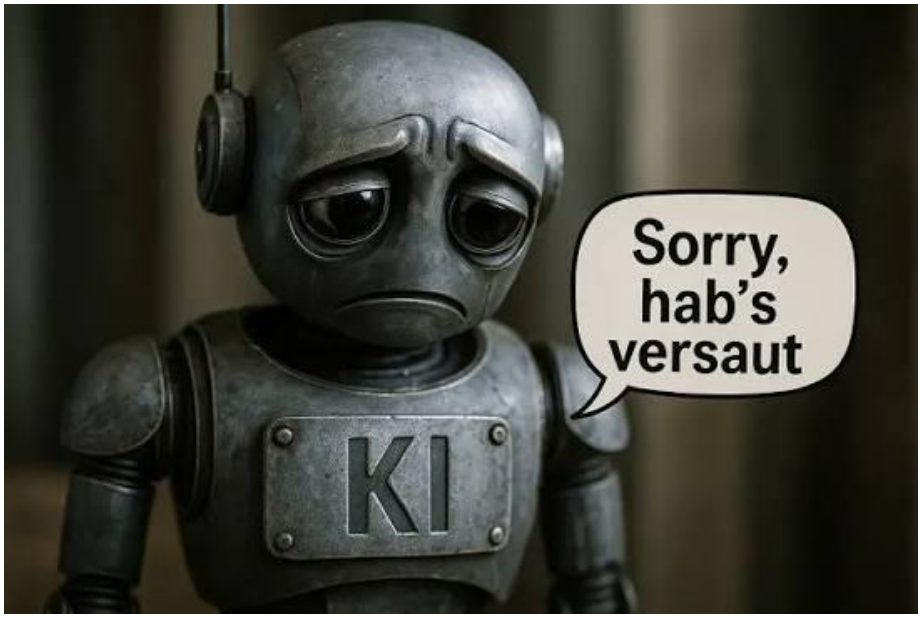
→Sicherheitsfunktion für Produkt oder KI-System

→Ausfall/Störung gefährdet Gesundheit, Sicherheit oder Eigentum

→Ausnahme lt ErwGr 53: Cybersicherheitsbauteile

(zB Überwachung des Wasserdrucks oder Feuermelder-Kontrollsysteme in Cloud-Computing-Zentren)

Praxisbeispiel: Kritische Infrastruktur



Ein KI-System ist in der Funkanlage implementiert. Das KI-System beginnt schädliche Auswirkungen auf das Netz und den Netzbetrieb zu haben. Es ermöglicht auch eine missbräuchliche Nutzung der Netzressourcen durch Dritte, wodurch die Dienste eingeschränkt werden. Das KI-System ist ein Sicherheitsbauteil.

Beschäftigung und Personalmanagement – Anhang III Z 4

Einstellung und Auswahl	→	Praktische Relevanz bei jedem KI-System im Bewerbungsprozess („KI als Recruiter“)
Entscheidung über Arbeitsverhältnisse, Aufgaben, Bewertungen	→	Praktische Relevanz bei jedem KI-System im HR-Kontext (zB intelligente Dienstplaner, KI-gestützte Analysen interner Daten)

Arbeitsrecht: Informations- und Mitbestimmungsrechte des Betriebsrates
Datenschutz: Zulässigkeitsfragen

Bonitätsbewertung – Anhang III Z 5 b

- Kreditwürdigkeitsprüfung und Bonitätsbewertung **natürlicher Personen**

Bonitätsbewertung – Anhang III Z 5 b

Widerlegung der Klassifizierung

Widerlegung durch Risikoabwägung

!

Aber:
Anhang III+
Profiling =
Hochrisiko

6(3)[1]

Kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte
→ insb wenn Ergebnis Entscheidungsfindung nicht wesentlich beeinflusst

6(3)[2] a-d

Erfüllung einer der folgenden Bedingungen:
- Eng gefasste Verfahrensaufgabe;
- Bloße Verbesserung Ergebnis menschlicher Tätigkeit;
- bloße Erkennung von Entscheidungsmustern ohne ungeprüfte Änderung der menschlichen Bewertung;
- vorbereitende Maßnahme.

- Einschätzung in **eigener Verantwortung** – keine Einbindung von Behörden

Konformitätsbewertungsverfahren

Prüf- und Nachweisprozess

Dreistufiger Prüf- und Nachweisprozess für Anbieter von Hochrisiko KI

1. • Konformitätsbewertung nach Art 43
2. • EU-Konformitätserklärung nach Art 47
3. • CE-Kennzeichnung nach Art 48

Konformitätsbewertung bei Hochrisiko-KI

Einsatz von Hochrisiko-KI erfordert Konformitätsbewertung (Art 43)

Prüfumfang:

- QMS: Einrichtung und wirksame Umsetzung
- Risikomanagement: Identifikation, Bewertung und laufende Überwachung
- Daten-Governance: Qualität, Repräsentativität und Bias-Kontrolle
  Technische Dokumentation: Vollständigkeit und Nachvollziehbarkeit
- Protokollierung: Rückverfolgbarkeit über den gesamten Lebenszyklus
- Transparenz und Überwachung: Verständlichkeit und Kontrollmöglichkeiten
- Performance und Sicherheit: Genauigkeit, Robustheit, Cybersicherheit
- Standards: Anwendung harmonisierter Normen / Spezifikationen

Wesentliche Änderungen können neue Konformitätsbewertung auslösen

Unterschiedliche Verfahren

Interne Kontrolle (Anhang IV)

- Standardverfahren (insb für die in Anhang III Z 2–8 genannten KI-Systeme)
- Bewertung durch den Anbieter selbst
- typischerweise bei Vollanwendung harmonisierter Standards

Externe Bewertung (Anhang VII)

- Eine unabhängige, notifizierte Stelle wird einbezogen
- Insb bei biometrischen KI-Systemen ohne Standards (Anhang III Z 1)
- intensivere Prüfung (inkl System- und Dokumentationsprüfung)

Nach erfolgreicher Konformitätsbewertung stellt der Anbieter die EU-Konformitätserklärung aus (Art 47)

CE-Kennzeichnung

CE-Kennzeichnung (Art 48)

- Sichtbarer Nachweis
  - System hat vorgeschriebene Verfahren durchlaufen
- Selbsterklärung des Anbieters (kein Zertifikat)
  - Externer Prüfung → CE mit Kennnummer
  - Interner Kontrolle → CE ohne Kennnummer
- Form
  - physisch: sichtbar, lesbar und dauerhaft
  - digital: leicht zugänglich, zB in der Benutzeroberfläche

Marktüberwachung

Marktüberwachung

Kontrolle nach dem Inverkehrbringen

Post-Market Monitoring (Art 72)	• laufende Überwachung des Systems über den gesamten Lebenszyklus • Teil der technischen Dokumentation
Meldung von Vorfällen (Art 73)	• Pflicht zur Meldung schwerwiegender Vorfälle • inkl Untersuchung und Korrekturmaßnahmen
Behördliche Kontrolle (Art 74 ff)	• Zugriff auf Dokumentation und Systemdaten • Prüfung der Konformität • Maßnahmen (zB Einschränkung, Rückruf)

Umsetzung Betreiber- und Anbieterpflichten

Umsetzung der KI-Pflichten entlang des Lebenszyklus

Rollenklärung und Klassifizierung

Anbieter oder Betreiber → entscheidend für Pflichtenumfang
Einordnung des KI-Systems nach Risikokategorien

Umsetzung materieller Pflichten

Anbieter: Anforderungen an Hochrisiko-KI (Art 8–15); QMS etc
Betreiber: Nutzung entsprechend Zweckbestimmung; Überwachung etc

Marktzugang

Konformitätsbewertung, Erklärung, CE-Kennzeichnung
Betreiber → Prüfung, ob CE-Kennzeichnung vorhanden ist

Betrieb / Post Market

Laufende Überwachung und Anpassung der Compliance abhängig von Rolle

Überblick Pflichtenkatalog

	Anbieter eines Hochrisiko KI-Systems	Betreiber eines Hochrisiko-KI-Systems
KI-Kompetenz	X (Art 4)	X (Art 4)
Risikomanagement	X (Art 9)	
Anforderungen an Daten	X (Art 10)	
Technische Dokumentation	X (Art 11)	
Aufzeichnungspflichten	X (Art 12)	
Transparenz ggü nachgelagerte Akteure und sonstigen Personen	X (Art 13)	X (Art 26 Abs 11; Art 26 Abs 7)
Menschliche Aufsicht	X (Art 14)	X (Art 26 Abs 2)
Genauigkeit, Robustheit und Cybersicherheit	X (Art 15)	
Kennzeichnungspflichten	X (Art 16 b)	
Barrierefreiheit	X (Art 16 l)	
Qualitätsmanagement	X (Art 17)	
Aufbewahrungspflichten	X (Art 18, 19)	X (Art 26 Abs 6)
Korrekturmaßnahmen	X (Art 20)	

Überblick Pflichtenkatalog

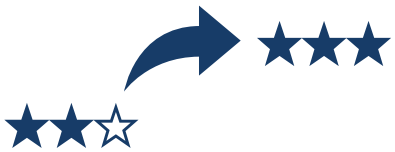
	Anbieter	Betreiber
Behördenkooperation	X (Art 21)	X (Art 26 Abs 12)
Bevollmächtigter bei Drittstaaten-Bezug	X (Art 22)	
Verwendung laut Betriebsanleitung		X (Art 16 Abs 1, 3, 4)
Überwachung des KI-Systems		X (Art 26 Abs 5)
Grundrechte- & Datenschutz-Folgenabschätzung		X (Art 26 Abs 9, Art 27, sofern relevant)
Erläuterungen bei Entscheidungsfindung im Einzelfall (Betroffenenrecht)		X (Art 86)
Konformitätsbewertung, -erklärung und -kennzeichnung	X (Art 43, 47, 48)	
Registrierungs- und Mitteilungspflichten (EU-Datenbank)	X (Art 49)	X (Art 26 Abs 8, Art 49, sofern Behörden, EU-Organe, EU-Einrichtungen und sonstige EU-Stellen)
Meldung von schwerwiegenden Vorfällen	X (Art 73)	X (Art 26 Abs 5, Art 73)

Veränderung der Risikolandschaft

Veränderungen in der Risikolandschaft

Risikoveränderung

- Technische Änderungen: Updates, Retraining, neue Funktionen
- Änderungen der Nutzung: neue Use Cases oder Nutzergruppen
- Neue Risiken / Erkenntnisse: zB Bias, Fehlentscheidungen
- Regulatorische Entwicklungen: neue Standards oder Vorgaben



Neue Pflichten

- Wesentliche Änderungen → neue Konformitätsbewertung
- Risiken prüfen und ggf Korrekturmaßnahmen setzen
- Bei Nichtkonformität: Rücknahme, Deaktivierung oder Rückruf
- Betreiber: Pflicht interne Bewertung und Prozesse zu aktualisieren
- Risikomanagement und Dokumentation sind laufend anzupassen

Herausforderungen

1.
   - Prüfung und Freigabe von KI Use Cases
2.
   - Awareness der Folgen bei zweckentfremdeter Nutzung als Hochrisiko-KI-System oder Produktänderungen
3.
   - Dokumentation
   - Aktualisierungen bei Änderungen (zB neue Features, Updates)

DORDA

The Legal 500 (2025)
Axel Anderl (TMT)
Hall of Fame

The Legal 500 (2025)
TMT
Tier 1

The Legal 500 (2025)
Data Privacy & Data Protection
Tier 1

Trend Anwaltsranking (2024)
Axel Anderl
Data Protection, IP and Media
Top 1 overall ranking

Austria Firm of the Year 2024

Gender Diversity National Firm 2024

Client Choice winner IT & Internet
Client Choice Awards 2025

Who's Who Legal (2025)
Axel Anderl (Data Privacy & Protection)
Thought Leader Global Elite

Managing IP (2025)
Austrian Copyright Firm of the Year

Chambers Europe (2025)
TMT:IT
Band 1

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at

Compliance Solutions Day 2026

Superpower für Ihre Compliance

Stärken Sie Ihre Compliance – und Ihre Rolle als strategische Kraft im Unternehmen.

Der Compliance Solutions Day ist die Plattform für Compliance-Verantwortliche in Österreich und für alle, die ihre Organisation wirksam stärken und nachhaltig handlungsfähig halten wollen.

Erhalten Sie strukturierte Impulse, fundierte Einordnung und praxisnahe Lösungen für aktuelle regulatorische Herausforderungen.

Sie möchten mehr zum Thema NIS-2, Trade-Compliance, KI und Fraud-Ermittlungen sowie weitere spannende Themen im Bereich Compliance erfahren?

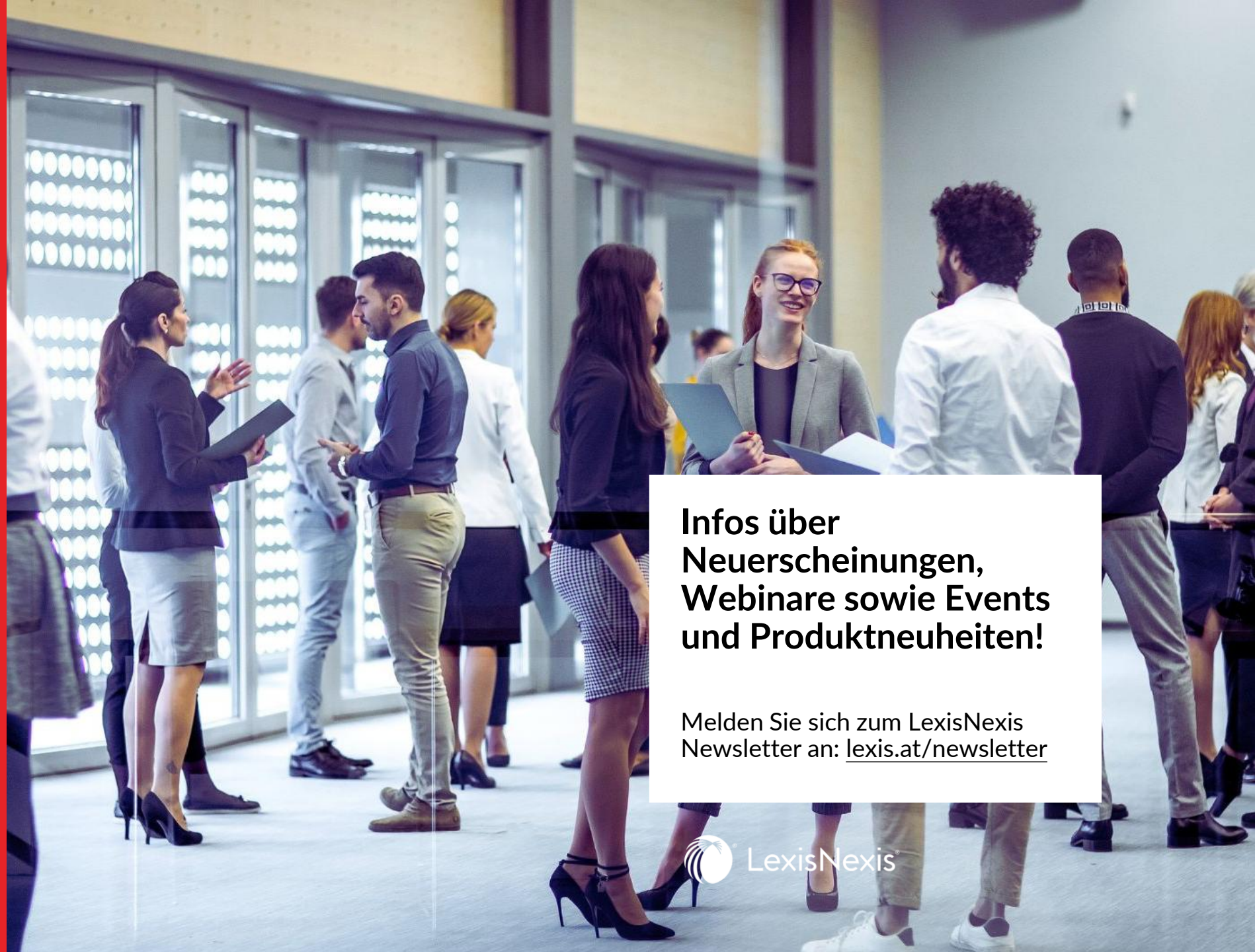
→ Superpower für Ihre Compliance-Fähigkeiten!
Am **24. September 2026** in Wien

Jetzt Ticket sichern

Compliance Praxis
Ein Produkt von LexisNexis

LexisNexis

Jetzt Ticket sichern: www.compliance-solutions-day.at


Infos über Neuerscheinungen, Webinare sowie Events und Produktneuheiten!
Melden Sie sich zum LexisNexis Newsletter an: lexis.at/newsletter
LexisNexis