COMPLIANCE-BRIEFING 2026

Drei Pflichten. Ein gemeinsamer *Nenner: Dokumentation.*

EU AI Act · DSGVO · CSRD — was Hospitality und menschen-intensive Dienstleister im DACH-Raum ab 2026 kennen sollten. Stand: Mai 2026.

Was Sie in 4 Seiten bekommen: Pro Regelwerk eine Seite — was im Gesetz steht, wen es trifft, wie man strukturiert anfängt. Konservativ formuliert: nur gesetzlich verankerte Daten, keine spekulativen Bußgeld-Bandbreiten.

Wer dahinter steht: Andreas Lerch, 30 Jahre Hospitality, Gründer 3Perspectives.

Wofür gemacht: Eigentümer, Geschäftsführer, HR-Leitung in Hospitality, Klinik, Kanzlei, Handel, Dienstleister.

3Perspectives

STAND MAI 2026 · Q2-EDITION

PFLICHT 1 VON 3

EU AI Act *Art. 4* — KI-Kompetenz

EU-Verordnung 2024/1689, verabschiedet am 13. Juni 2024, schrittweise Anwendung. ***Art. 4 (KI-Kompetenz)*** *ist seit* ***2. Februar 2025 anwendbar*** *und betrifft alle Betreiber von KI-Systemen. Mehrheit der weiteren Pflichten greift ab* ***2. August 2026*** *(Hochrisiko-Systeme nach Annex III).*

Was ein „KI-System" in Ihrem Betrieb ist

Wenn Sie eines der folgenden einsetzen, sind Sie betroffen:

- Dynamic-Pricing-Engines im Channel Manager (SiteMinder, Cloudbeds)
- KI-gestützte PMS-Empfehlungen (Mews, Apaleo) für Pricing oder Belegung
- Voice-Bots oder Chatbots an der Rezeption oder auf der Website
- Sentiment-Analyse von Reviews (ReviewPro, Revinate)
- E-Mail-Triage-Tools mit KI-Klassifizierung
- Automatisierte Personal-Empfehlungs- oder Recruiting-Tools

Was Art. 4 konkret verlangt

1. Mitarbeiter, die diese Tools nutzen oder mit deren Output arbeiten, müssen **„ausreichende KI-Kompetenz"** haben
2. Die Kompetenz muss **proportional zu Rolle und Risiko** sein (Revenue Manager braucht mehr als HSK-MA)
3. Es muss **dokumentierbar** sein — Sie müssen einem Auditor vorlegen können, wer welche Schulung wann erhalten hat

So werden Sie in 4 Wochen Art.-4-konform

- **Woche 1:** Inventur aller KI-Systeme (Liste pro Tool, pro Abteilung)
- **Woche 2:** Schulungs-Curriculum festlegen — pro Tool/Rolle ein Modul (30-90 Min)
- **Woche 3:** Schulung durchführen (live oder über Tool wie das KI-Kompetenz-Modul der 3P Suite)
- **Woche 4:** Dokumentation in Audit-Ordner (Teilnahmebestätigungen, Curriculum, Logbuch)

SANKTIONS-ARCHITEKTUR (ART. 99)

Art. 4 hat keine eigene Sanktions-Norm

Art. 99 Stufe 1 (bis € 35 Mio. / 7 %) gilt nur für Art. 5 (verbotene KI-Praktiken). Stufe 2 (bis € 15 Mio. / 3 %) gilt für sonstige Verstöße. KI-Kompetenz-Lücken wirken in der Praxis vor allem als **verschärfender Faktor** bei anderen Verstößen — und als Reputationsthema im Auditfall.

PFLICHT 2 VON 3

DSGVO & revDSG *— laufend*

*DSGVO (EU-Verordnung 2016/679) gilt seit 25. Mai 2018; revDSG (Schweiz) seit 1. September 2023. Beide laufend wirksam. Bußgeld-Rahmen bis **€ 20 Mio. oder 4 %** des Konzernumsatzes (Art. 83 Abs. 5 DSGVO). Konkrete Bußgeld-Höhe richtet sich nach Schwere, Vorsatz und Kooperation.*

Drei häufige Risiko-Bereiche in 4★+ Hotellerie

- **WhatsApp-Gruppen mit Gastdaten** — „Zimmer 304 erwartet Anruf, Frau Müller", in unverschlüsselter WhatsApp-Gruppe. Berührt Art. 32 DSGVO (technische und organisatorische Maßnahmen): WhatsApp ist kein DSGVO-konformer Auftragsverarbeiter für Gastdaten.
- **Mündliche Schichtübergaben ohne Audit-Trail** — nicht per se ein Verstoß, aber bei Datenschutz-Vorfällen schwer dokumentierbar. Relevant für Art. 5 Abs. 2 (Rechenschaftspflicht).
- **Offene Meldescheine im Backoffice** — gedruckte Meldescheine in unverschlossenen Schubladen / im Empfangsbereich. Berührt Art. 32: Schutz vor unbefugtem Zugriff fehlt.

Was im Audit konkret abgefragt wird

- Verzeichnis der Verarbeitungstätigkeiten (Art. 30) — viele Hotels haben keins
- Auftragsverarbeitungsverträge (Art. 28) mit Channel Managern, PMS, Marketing-Dienstleistern
- Technische und organisatorische Maßnahmen (TOM) — schriftliche Sicherheits-Architektur
- Datenschutz-Folgenabschätzung (Art. 35) — pro KI-System Pflicht, falls Hoch-Risiko
- Meldung von Datenschutzverletzungen innerhalb 72 h (Art. 33)

Quick-Wins für DSGVO-Compliance

1. WhatsApp ersetzen durch DSGVO-konforme Schichtübergabe-Tools
2. Meldescheine digital + verschlüsselt (über PMS, nicht ausgedruckt)
3. Verzeichnis der Verarbeitungstätigkeiten als 1-seitiges Word-Template anlegen (Vorlage frei bei Landesdatenschutzbehörden)

SANKTIONS-RAHMEN DSGVO

Bis € 20 Mio. oder 4 % Konzernumsatz (Art. 83 Abs. 5)

Konkrete Bußgelder DACH-Hotellerie sind nicht systematisch öffentlich. Indirekte Folgekosten (Stornierungen, Reputation, Auditrunden) sind in der Regel höher als das Bußgeld selbst.

PFLICHT 3 VON 3

CSRD — *nach Omnibus stark entschärft*

*Corporate Sustainability Reporting Directive (EU-Richtlinie 2022/2464). Am **16. April 2025** wurde die **Stop-the-Clock-Direktive** (EU 2025/794) im Amtsblatt veröffentlicht. Wave 2 + 3 sind um **2 Jahre verschoben**; geplante neue Schwellen liegen bei **> 1.000 Mitarbeiter und > € 450 Mio. Umsatz** (statt vorher 250 / € 40 Mio.). ESRS-Vereinfachung läuft; erste Anwendung der reduzierten Standards voraussichtlich ab Geschäftsjahr 2027.*

Was das für Hospitality DACH konkret heißt

Die meisten inhabergeführten Hotels und mittelständischen Service-Betriebe DACH werden mit den geplanten neuen Schwellen **nicht direkt CSRD-pflichtig**. Direkt relevant bleibt CSRD vor allem für große Hotelketten und börsennotierte Gruppen.

Indirekt bleibt das Thema präsent: Konzernkunden, Reiseveranstalter, Banken und Versicherer fragen ESG-Daten zunehmend in der Lieferkette ab — auch von Häusern, die selbst nicht berichtspflichtig sind.

Was im Mittelpunkt der ESRS bleibt

- **ESRS E1 (Climate):** Energieverbrauch (Scope 1+2), CO2-Bilanz, Reduktionspfad
- **ESRS E5 (Resources & Circular):** Abfall, Lebensmittel-Verschwendung, Wasser
- **ESRS S1 (Own Workforce):** Mitarbeiter-Demografie, Lohngerechtigkeit, Gesundheit & Sicherheit

Pragmatische Empfehlung: ESG-Basisdaten erfassen — auch ohne Berichtspflicht

1. Energie + Wasser-Tracking systematisch (monatliche Zähler-Erfassung)
2. Lebensmittel-Verschwendung 1×/Quartal erfassen
3. Mitarbeiter-Demografie + Lohngruppen-Übersicht aufstellen
4. ESG-Tool nutzen, das ESRS-kompatibel berichten kann (für B2B-Anfragen)

DIE DREI-PFLICHTEN-SYNTHESE

Alle drei Regelwerke teilen ein Muster: Sie verlangen Dokumentation, Nachweis und Struktur. KI-Kompetenz-Schulung mit Teilnahme-Log. DSGVO-Verarbeitungsverzeichnis. ESG-Datenbasis für B2B-Anfragen.

Häuser, die diese Strukturen jetzt aufbauen, haben einen Prozess-Vorteil — und einen Kommunikations-Vorteil gegenüber Konzern-Kunden, Banken, Versicherern und Auditoren, die diese Belege zunehmend einfordern.

Empfohlener nächster Schritt

→ **QuickCheck machen** (15 Min online, kostenlos) — erste Compliance-Indikation pro Bereich

→ **60-Min-Sparring buchen** (kostenlos, kein Verkaufstermin) — cal.com/andreaslerch/sparring

→ **People Intelligence Bundle 14-Tage-Trial** — gratis ohne Kreditkarten-Gate — 3perspectives.de/pib-pricing

Quellen (alle frei zugänglich):
· EU AI Act: Verordnung (EU) 2024/1689 vom 13.6.2024 (Art. 4 + 99) — artificialintelligenceact.eu
· DSGVO: Verordnung (EU) 2016/679 (Art. 5, 28, 30, 32, 33, 35, 83)
· revDSG Schweiz: Bundesgesetz über den Datenschutz, in Kraft 1.9.2023
· CSRD: Richtlinie (EU) 2022/2464 + Stop-the-Clock-Direktive (EU) 2025/794 vom 16.4.2025
· ESRS-Vereinfachung: Auftrag an EFRAG durch EU-Kommission, Q4 2025

Hinweis: Konkrete Bußgeld-Höhen pro Verstoß sind im EU-Recht *nicht* betragsmäßig festgelegt — nur Maximal-Rahmen. Tatsächliche Sanktionen ergeben sich aus Schwere, Vorsatz, Kooperation und nationaler Aufsichts-Praxis. Dieses Briefing nennt deshalb nur die gesetzlich verankerten *Höchst*-Rahmen, keine spekulativen Bandbreiten.

3Perspectives · Andreas Lerch · Mittermoos 17 · 6391 Fieberbrunn · Österreich · andreas@3perspectives.de · +43 677 624 58439 · 3perspectives.de · Stand: Mai 2026