



## Destinations-Netzwerk Austria (dna)

### KI GOVERNANCE FACTSHEET

#### 1. KI-Kompetenz als Grundlage für Chancennutzung & Risikovermeidung

Eine gezielte Förderung der **KI-Kompetenz bei Mitarbeitenden** ist entscheidend, um den sicheren Einsatz von KI-Applikationen zu gewährleisten. Gut geschulte Teams können Chancen effektiv nutzen, Risiken wie inkorrekte Ausgaben, insbesondere Halluzinationen, Verzerrungen (Bias) oder Datenschutzverstöße erkennen und proaktiv vermeiden.

Gemäß EU AI Act müssen alle Organisationen, die KI einsetzen, KI-Kompetenzen aufzubauen. Kompetenz ist dabei in Bezug zur **Rolle der Organisation** (Entwicklung von KI-Systemen [Anbieterseite] vs Nutzung von KI-Systemen, die von Dritten entwickelt wurden [Betreiberseite]) und den **eingesetzten KI-Applikationen** (Hochrisiko KI-Systeme vs KI-Systeme im Bereich mittleres bis geringes Risiko) zu sehen. Unternehmen, welche KI-Applikationen entwickeln, vor allem im Hochrisiko-Bereich, benötigen ein höheres Niveau an KI-Kompetenz, als Unternehmen die (nur) KI-Applikationen im untergeordneten Risikobereich verwenden (z.B. für Erstellen von Bildern, Texten, Podcasts, Videospots, etc).

**Maßnahmen zum Aufbau von KI-Kompetenzen:** interne und externe Schulungen zu KI-Grundlagen (technisch, rechtlich, nutzungsorientiert), Aufbau eines internen KI-Expertenteams oder AI CoE (Center of Excellence), Laufende Weiterbildung zu aktuellen Entwicklungen.

KI-Kompetenz kann durch eine Kombination an Maßnahmen aufgebaut werden. Zu Zwecken des Nachweises wird die Dokumentation des KI-Kompetenzansatzes (z.B. welche Maßnahmen, welche Häufigkeit, Zielgruppen) und der Durchführung (z.B. Teilnahmebestätigungen der Mitarbeitenden) der Organisation empfohlen.

#### 2. KI-Guidelines für die sichere und effiziente Nutzung von KI-Applikationen

**Unternehmensleitlinien**, die klar definieren, welche KI-Applikationen genutzt werden dürfen und wie diese sicher und effizient eingesetzt werden, sind entscheidend, um Mitarbeitende beim KI-Einsatz zu unterstützen. Sie helfen dabei, Chancen gezielt zu nutzen und gleichzeitig Risiken für die Organisation in den Bereichen Schutz von Betriebs- und Geschäftsgeheimnissen, Datenschutz und Urheberrechte zu mindern.

Unternehmensleitlinien für die Nutzung von KI-Applikationen können unterschiedlich ausgestaltet werden, von einer **umfassenden Richtlinie bis hin zu einer einfachen Checkliste** für den KI-Einsatz. Wesentliche Punkte, die behandelt werden sollten, sind unter anderem Verantwortung für generierte Inhalte, Offenlegungen und Datennutzung.

#### 3. Ausgewählte rechtliche Aspekte im Überblick

##### 3.1. Artificial Intelligence Act (EU AI Act)

Der EU AI Act regelt als europäische Verordnung die **Entwicklung und den Betrieb von KI-Systemen** einheitlich für die Europäische Union. Die Regulierung verfolgt einen **risikobasierten Ansatz**. KI-Systeme werden in vier Kategorien eingeteilt:

##### ⊖ Inakzeptables Risiko = 8 Verbotene KI-Praktiken

Sanktion: EUR 35M / 7% weltweiter Jahresumsatz

In Geltung: seit 2. Februar 2025

- KI-Systeme die manipulieren, täuschen oder nachteilig unterschwellig beeinflussen
- KI-Systeme, die Schutzbedürftigkeit oder Vulnerabilität von Personen/Gruppen aufgrund Alter, Behinderung sowie sozialer oder wirtschaftlicher Situation ausnutzen



- KI-Systeme zur Bewertung von Personen aufgrund ihres Sozialverhaltens oder persönlicher Eigenschaften, die zu unverhältnismäßiger Schlechterstellung führt (Social Scoring)
- KI-Systeme zur Bewertung, ob eine Person eine Straftaten begeht basierend auf Profiling
- KI-Systeme zur Emotionsableitung am Arbeitsplatz oder in Bildungseinrichtungen
- Aufbau oder Ausbau von Gesichtsdatenbanken durch ungezieltes Datascraping
- Biometrische Kategorisierung mittels biometrischer Daten, um bestimmte Merkmale abzuleiten (z.B. Rasse, politische Einstellung, Gewerkschaftszugehörigkeit)
- Echtzeit-Fernidentifizierungssysteme zu Strafverfolgungszwecken (mit Ausnahmen)

**Im Bereich Tourismus und Destination Marketing relevante Anknüpfungspunkte:** vor allem im Bereich KI-Marketingpraktiken (z.B. unterschwellige Recommendersysteme, Anreizgestaltung bei KI-Agenten oder Chatbots, App-Gestaltung) ergeben.

**⚠ Hohes Risiko = Hochrisiko KI-Systeme**

Sanktion: EUR 15M / 3% weltweiter Jahresumsatz

In Geltung: geplant 2. August 2026

Verschiebung der Anwendbarkeit nach hinten durch Digitalen Omnibus möglich.

- **Biometrische Systeme und Emotionserkennungssysteme**
- **KI-Systeme für Verwaltung und Betrieb kritischer Infrastrukturen** in den Bereichen Wasser, Gas, Wärme, Strom, Straßenverkehr kritische digitale Infrastruktur.
- **KI-Systeme im Bereich allgemeine und berufliche Bildung**, insbesondere Zugang zu Bildung, Bewertung von Lernergebnissen, Erkennung von verbotenen Prüfungsverhalten
- **KI-Systeme im Personalbereich**, insbesondere gezielte Schaltung von Stellenanzeigen, Filtern und Bewerten von Bewerbenden, Einsatz in Bezug auf Entscheidungen über Bedingungen von Arbeitsverhältnissen (Kündigung, Beförderung, Arbeitszuteilung)
- **KI-Systeme betreffend öffentliche Unterstützungsleistungen**, zur Notfalltriage, zur Risikobewertung und Preisbildung in Bezug auf Lebens- und Gesundheitsversicherungen sowie für Kredit- und Bonitätsscoring von natürlichen Personen.
- Weitere ausgewählte KI-Systeme in den Bereichen Justiz, Demokratie, Strafverfolgung, Asyl, Migration und Grenzkontrolle.

**Folgen für Anbieter (Entwickler):** strenge Anforderungen an das Design des KI-Systems (Risikomanagement, Daten-Governance, technische Dokumentation, Logging, menschliche Aufsicht, Genauigkeit, Robustheit, Cybersicherheit, Qualitätsmanagement).

**Folgen für Betreiber (professionelle Nutzer):** strenge Anforderungen an die Nutzung (KI-Kompetenz, Implementierung menschlicher Aufsicht und Kontrolle, Transparenz, Eingabedaten).

**Im Bereich Tourismus und Destination Marketing relevante Anknüpfungspunkte:** vor allem beim Einsatz von KI-Systemen im Personalbereich oder in Bezug auf Auszubildende (Lehrlinge).

**🔍 Transparenzverpflichtungen**

Sanktion: EUR 15M / 3% weltweiter Jahresumsatz

Anwendbarkeit ab 2. August 2026 (unabhängig vom Digitalen Omnibus).

- Bei KI-Systemen, die für die Interaktion mit natürlichen Personen bestimmt sind, müssen Personen informiert werden, dass sie mit einem KI-System interagieren.



- **KI-generierte oder KI-bearbeitete Audio-, Bild- oder Toninhalte**, die echten Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähneln, und fälschlicherweise als echt oder wahrheitsgemäß erscheinen könnten) müssen sichtbar gekennzeichnet werden.
- **KI-generierte oder KI-bearbeitete Texte** müssen nur dann gekennzeichnet werden, wenn sie für die Öffentlichkeit zur Information über öffentliche Angelegenheiten erstellt werden. Die Kennzeichnungspflicht entfällt bei redaktioneller / menschlicher Kontrolle und redaktioneller Verantwortungsübernahme.

**Im Bereich Tourismus und Destination Marketing relevante Anknüpfungspunkte:** von hoher Relevanz, insbesondere bei der KI-unterstützten Erstellung von diversen Marketingformaten (z.B. Destinationsbilder, Videokampagnen, Podcasts, Pressemitteilungen, Berichte) als auch immersiven Formaten (z.B. digitale Zwillinge, Avatare, Chatbots oder Agents).

### 3.2. Datenschutz (DSGVO)

**Relevanz:** bei Verarbeitung personenbezogener Daten, insbesondere Gästedaten (Namen, Kontaktdaten, Zahlungsinformationen), Profiling (z.B. von Reiseverhalten), Individualisierung und Personalisierung von Angeboten und Kommunikation.

**Leitfragen:**

- Gibt es eine Rechtsgrundlage (Einwilligung, Vertrag, berechtigtes Interesse)?
- Erfolgt Datenübermittlung in Drittstaaten?
- Welche technischen und organisatorischen Maßnahmen sind zu treffen?
- Sind die datenschutzrechtlichen Dokumentationen aktuell?

### 3.3. Schutz von Betriebs- und Geschäftsgeheimnissen

**Relevanz:** Gefahren entstehen durch die Eingabe sensibler Daten (z.B. Preisstrategie, Margenkalkulation, Vertragsdetails, Strategiedokumente) im Besonderen, aber nicht nur in öffentliche KI-Applikationen. Auch nicht-personenbezogene Daten können sensibel sein und Betriebs- und Geschäftsgeheimnisse enthalten.

**Leitfragen:**

- Welche Kritikalität haben die Daten (personenbezogen und nicht-personenbezogen)?
- Wie ist der Umgang mit vertraulichen Informationen geregelt?
- Werden die Daten für KI-Training verwendet?

## 4. Action Items für den rechtssicheren KI-Einsatz

- **KI-Use-Cases identifizieren und klassifizieren:** Bestehende und geplante KI-Anwendungen (z. B. Marketing, Chatbots, Personalisierung) erfassen und nach Risikokategorien sowie regulatorischen Anforderungen bewerten.
- **KI-Verzeichnis aufbauen:** ein zentrales Register aller eingesetzten KI-Systeme erstellen – inklusive Zweck, Anbieter, Datenquellen, Verantwortlichkeiten und Bewertung.
- **Interne KI-Richtlinie entwickeln:** klare Regeln für den Einsatz von KI festlegen (z.B. Umgang mit Daten, Nutzung externer Tools, menschliche Kontrolle, Genehmigungsprozesse).
- **Kennzeichnungs- und Transparenzpflichten umsetzen:** sicherstellen, dass KI-generierte Inhalte (z. B. Texte, Bilde) und Interaktionsformate (z.B. Chatbots) transparent gekennzeichnet und rechtliche Informationspflichten eingehalten werden.
- **KI-Regelungen in Agentur- und Marketingverträge integrieren:** Verträge mit Agenturen und Dienstleistern um Bestimmungen zu KI-Nutzung ergänzen.
- **KI-Kompetenzen ausbauen:** Mitarbeitende regelmäßig schulen, Verantwortlichkeiten definieren und internes Know-how zu rechtlichen und praktischen KI-Fragen stärken.