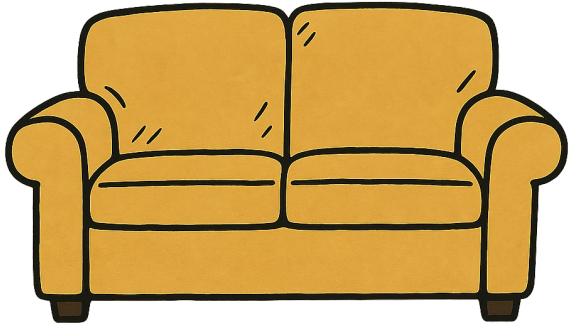




Couch



Cloud

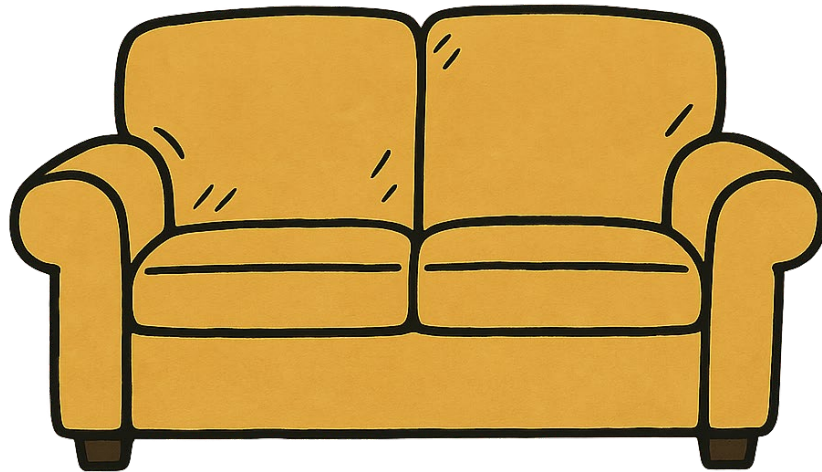


Compliance

Der AI Act zu Hause

Günter Martin
Vorstand SmartHome Deutschland
Düsseldorf, 14.10.2025

Couch: KI im Smart Home



Alltag:

- **Spracherkennung** zur Steuerung von Smart Home-Komponenten
- **Routenplanung** bei Saugrobotern (und Mährobotern)
- **Bilderkennung** (Personen) bei smarterer Sicherheitstechnik
- **Kontrolle**, z.B. Leck-Erkennung anhand Wasserverbrauchskurve
- **Küche**, z.B. künftige smarte Haushaltshilfen beim Kochen/Backen

Pflege:

- **Inhaus**: Assistenzlösungen für Menschen mit Unterstützungsbedarf (Vortrag Enrico Lührke. Smart Home Award 2021)
- **Carechamp**: Entlastung Pflegepersonal (Smart Home Award 2025).
- **SmartHome Deutschland**: Förderanträge bei Behörden stellen mit KI
- **Open Experience**: Bim-4-Care: Planungstool für wohnraumverbessernde Maßnahmen für die Pflege mit Generierung von Förderanträgen und Ausschreibungen

Cloud: KI in der Cloud



Cloud for KI

- Hohe regulatorische Anforderungen (Datenschutz, Datensicherheit)
- Edge-first: Wo möglich On-Device-Verarbeitung

Cloud for Enshitification*

- Software bewusst verschlechtern, um Erlöse zu erhöhen
- Software funktioniert nicht mehr autark, kann „wegen KI“ nur noch sinnvoll in der Cloud ausgeführt werden:
 - Schritt 1: Account-Pflicht: Nutzer muss sich registrieren
 - Schritt 2: Abo-Pflicht: Kostenpflichtiges Abo, Nutzer wird zu Upgrades gedrängt. Nutzer muss seine eigenen Daten zurückmieten
- Vendor-Lock-In Strategie
- Datenschutz: Daten werden monetarisiert, basierend auf freiwillig-gezwungene Nutzer-Zustimmung
- Datensicherheit: Potenzial für Cyber-Angriffe auf Nutzerdaten auf dem Hersteller-Server

Compliance: Anforderungen an SmartHome



DSGVO: Datenschutzgrundverordnung

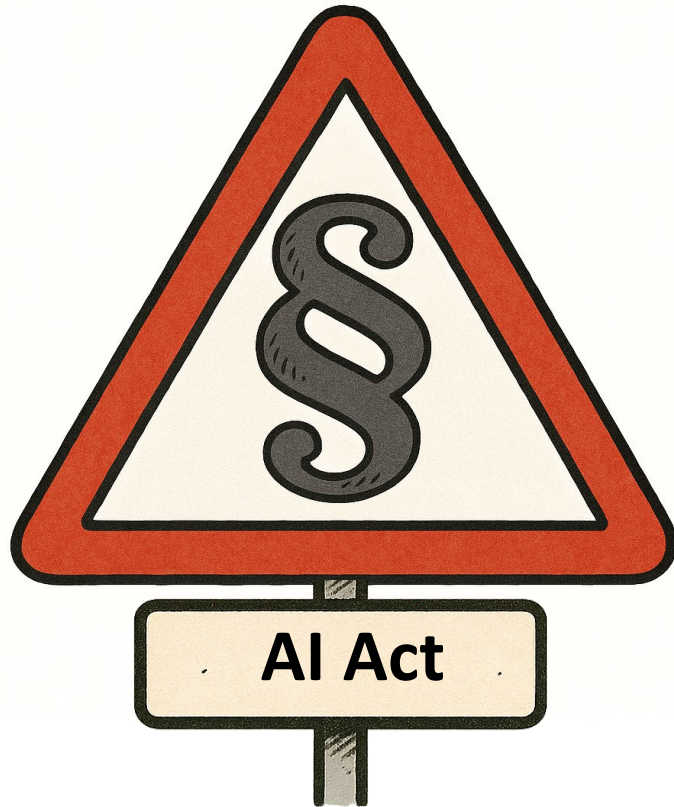
- Inkraft 25.8.2018, 99 Artikel, 88 Seiten
Schutz personenbezogener Daten; Rechte der Betroffenen, Pflichten für Verantwortliche, Aufsichtsbehörden, Datenpannen, Sanktionen
- Viele Öffnungsklauseln „Member States may...“

CRA: Cyber Resilience Act

- Inkraft 10.12.2024, stufenweise bis 11.12.2027, 57 Artikel, 92 Seiten
- Sicherheitsanforderungen, um die Widerstandsfähigkeit von Systemen gegen Cyberangriffe zu stärken.
- Gilt für „Produkte mit digitalen Elementen, die in der Lage sind, mit anderen Produkten zu kommunizieren. Hardware und Software.“
- Anforderungen basieren auf Risikobewertung

RED-Richtlinie 2024: Radio Equipment Directive

- Inkraft 1.8.2025; 45 Seiten
- Funkanlagen: Gesundheit, EMV, effiziente Nutzung des Funkspektrums
- Neu: Anforderungen zum Schutz personenbezogener Daten und der Privatsphäre, zur Netzresilienz und zur Betrugsprävention festzulegen



AI-Act: Artificial Intelligence Act

- Inkraft 1.2.2025 stufenweise bis 1.8.2027, 113 Artikel, 120 Seiten
- Vorgaben für die Entwicklung, Bereitstellung und Nutzung von KI-Systemen.
- Anforderungen basieren auf Risikobewertung.

Breiter Geltungsbereich

- **Anbieter**, die KI-Systeme in der EU in Verkehr bringen oder in Betrieb nehmen.
- **Nutzer** von KI-Systemen, die sich in der EU befinden. Das umfasst auch Behörden und Privatpersonen.
- **Wissenschaft**: Ausnahmeregeln für Forschung, Nutzung von KI-Reallabore ("regulatory sandboxes"). Innovation ermöglichen.

Bei **Verstoß** drohen Strafen von bis zu **30 Millionen Euro** oder sechs Prozent des weltweiten Gewinns

Die vier Risikostufen des AI-Acts



Risiko-Einstufung verpflichtend durch Hersteller/Anbieter

- Kriterien gem. Anhang III des AI-Acts
- Behörden können Einstufung überprüfen und durchsetzen

Verboten (unacceptable risk)

- KI gefährdet Grundrechte oder Sicherheit direkt
- z. B. Social Scoring

Hohes Risiko (high risk)

- KI wird in sicherheits- oder grundrechtsrelevanten Bereichen eingesetzt
- z. B. biometrische Identifizierung, Medizin, Bildung

Begrenztes Risiko (limited risk)

- KI interagiert mit Menschen, aber ohne gravierende Folgen
- z. B. Chatbots, Empfehlungssysteme, Spamfilter

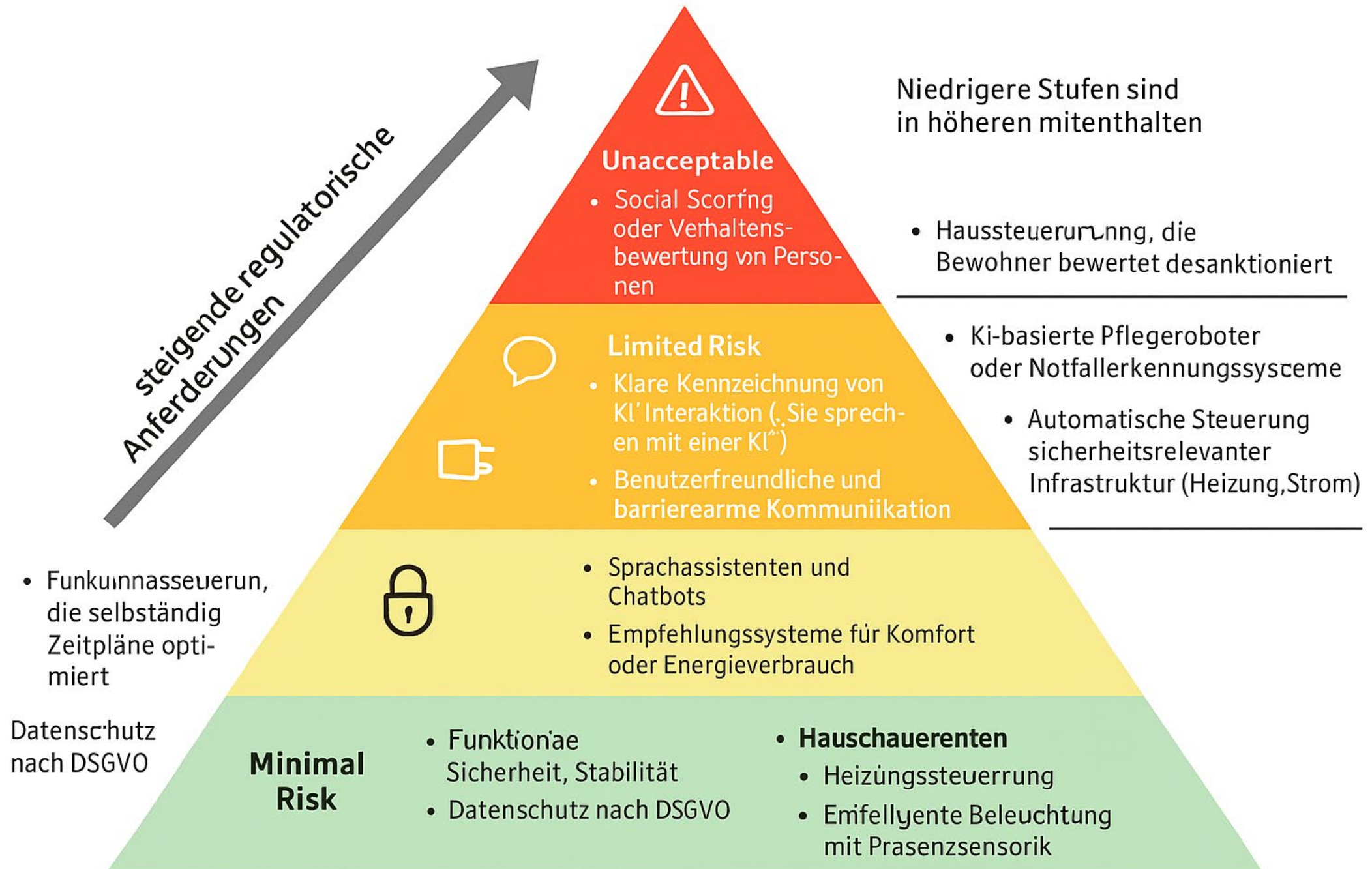
Minimales Risiko (minimal risk)

- rein funktionale KI ohne Relevanz für Grundrechte
- z. B. SmartHome - reine Bedienfunktion, Spiele-KI, Autokorrektur

AI-Act: Anforderungen und Umsetzung

Minimal Risk	Limited Risk	High Risk
Transparenz		
Verbot der Ausnutzung von Vulnerabilitäten		
DSGVO, CRA, RED-Richtlinie		
	Kennzeichnung Deepfakes (manipulierte Inhalte)	
	Hinweis bei biometrischer Kategorisierung und Emotionserkennung	
		Datenqualität und -governance, Bias-Management
		Menschliche Aufsicht und Eingreifbarkeit
		Logging Qualitätsmanagementsystem und Risikomanagement

Umsetzung, z.B./u.a.
Barrierearme, verständliche Anleitungen, SmartHome Deutschland: Technikbotschafter.
Praxis-Tests mit Betroffenen, Prüfen auf Diskriminierungsfreiheit
Datenminimierung, Verschlüsselung, Löschkonzepte, IT-Sicherheitskennzeichen des BSI
Content Content-Credentialing (z. B. C2PA) Integritätsprüfungen
Beschilderung, Pop-Up-Hinweise, kurze Aufbewahrungsfristen
Datenherkunft und -rechte dokumentieren. Regelmäßige Re-Validierung Trainings- und Testdaten.
Rollen und Schwellenwerte konfigurieren, Schulung
Automatische Protokollierung wesentlicher Ereignisse und Entscheidungen Registrierung in der EU-Datenbank und Post-Market-Monitoring samt Vorfallmeldung umsetzen.



Zusammenfassung

