



# Glossar

## Digitaler Vertragsschluss

# A

## **Attribute-Based Access Control (ABAC)**

Zugriffskontrollmodell, bei dem Entscheidungen über den Zugriff auf Ressourcen anhand von Attributen (Nutzer, Ressource, Kontext, Risiko) getroffen werden.

Für digitale Zustimmungssysteme relevant, um Zugriffsrechte an konkrete Einwilligungsstände zu koppeln.

**Quellen:** Art. 32 DSGVO; NIST AI RMF (Govern, Manage); BSI – Grundprinzip „Least Privilege“

## **Audit Trail / Protokollierung**

Lückenlose, manipulationssichere Dokumentation aller relevanten Schritte eines digitalen Vertragsschlusses oder einer Einwilligung.

Erforderlich zur Erfüllung der Rechenschaftspflicht und zur Nachweisführung.

**Quellen:** Art. 5 Abs. 2 DSGVO; Art. 12 EU AI Act (Protokollierung); NIST AI RMF (Govern-Funktion).

# B

## **Behavioral Nudging**

Gestaltung von Benutzeroberflächen zur subtilen Lenkung von Entscheidungen, ohne sie zu erzwingen.

Abgrenzung zu unzulässigen Dark Patterns ist wesentlich, insbesondere bei Einwilligungen.

**Quellen:** Art. 7 DSGVO (Freiwilligkeit); Art. 25 DSA (Verbot irreführender Gestaltung).

## **Binding / Advanced / Qualified Electronic Signature (BES/AES/QES)**

Drei Stufen elektronischer Signaturen nach der eIDAS-Verordnung.

QES bietet die höchste Beweiskraft und rechtliche Gleichstellung mit einer handschriftlichen Unterschrift.

**Quellen:** Art. 3, 25, 26, 28 eIDAS.

# C

## **Checkbox-Design**

Gestaltung von Auswahlfeldern zur Zustimmung zu Vertragsbedingungen oder Einwilligungen. Erforderlich ist eine aktive Handlung des Nutzers, keine vorausgewählten Optionen.

**Quellen:** Art. 7 DSGVO; Leitlinien WP29 zu Einwilligungen.

## **Clickwrap**

Verfahren, bei dem Nutzer aktiv Bedingungen akzeptieren (z. B. durch Button oder Checkbox). Gilt als rechtssicher, wenn die Bedingungen vorab zugänglich waren.

**Quellen:** BGH-Rechtsprechung zum Vertragsschluss im Online-Bereich; Art. 7 DSGVO (Nachweisbarkeit).

## **Consent Management**

Systeme zur Erhebung, Verwaltung und Dokumentation von Nutzereinigigungen.

**Quellen:** Art. 6, 7, 30 DSGVO; NIST AI RMF (Govern).

## **Consent Receipt**

Standardisierte Bescheinigung einer erteilten Einwilligung, sinnvoll als Nachweis gegenüber Behörden.

**Quellen:** Art. 7 Abs. 1 DSGVO; Art. 5 Abs. 2. DSGVO.

## **Cookies**

Datensätze auf Endgeräten der Nutzer zur Funktionsfähigkeit oder Analyse. Nicht notwendige Cookies erfordern eine vorherige Einwilligung.

**Quellen:** Art. 6 DSGVO; Art. 5 Abs. 3 ePrivacy-Richtlinie.

# **D**

## **Dark Patterns**

Gestaltungsmuster, die Nutzer zu Entscheidungen drängen oder täuschen. Im Kontext von Einwilligungen regelmäßig unzulässig.

**Quellen:** Art. 25 DSA; Art. 7 DSGVO (Freiwilligkeit).

## **Delegierte Zustimmung**

Einwilligungen oder Vertragshandlungen durch berechtigte Dritte (z. B. gesetzliche Vertreter).

**Quellen:** Art. 8 DSGVO (Minderjährige).

## **Digital Services Act (DSA)**

EU-Verordnung für digitale Dienste, u. a. mit Regeln zu Transparenz, Nutzerrechten, Dark Patterns und Inthalteverantwortung.

**Quellen:** DSA; insbesondere Art. 14-25.

## **Digitale-Dienste-Gesetz (DDG)**

Deutsches Umsetzungsgesetz zum DSA. Regelt Aufsicht und Durchsetzung.

Quellen: DDG.

## **Double-Opt-In (DOI)**

Zweistufiges Einwilligungsverfahren: Nutzer gibt Einwilligung ab und bestätigt sie zusätzlich, z. B. per E-Mail.

Wichtig zur Vermeidung missbräuchlicher Anmeldungen.

Quellen: Art. 7 DSGVO (Nachweisbarkeit), BGH "Double-Opt-In".

# **E**

## **E-Mail-Zustimmung**

Vertragsschluss oder Einwilligung per E-Mail.

Erfordert eindeutige Willenserklärung und zweifelsfreie Zuordenbarkeit.

Quellen: §§ 145 ff. BGB; Art. 7 DSGVO.

## **Entwicklung der Vertragsautomatisierung**

Digitalisierung und Automatisierung von Vertragsprozessen durch elektronische Signaturen, Workflows oder KI.

**Quellen:** eIDAS; Art. 50 ff. EU AI Act. (Transparenzpflichten)

# **G**

## **General-Purpose AI (GPAI) – Relevanz für Vertragssysteme**

KI-Modelle, die mehrere Aufgaben erfüllen können und insbesondere bei automatisierten Vertragssystemen eingesetzt werden.

Unterliegen speziellen Transparenz- und Sorgfaltspflichten.

**Quellen:** Art. 53 ff. EU AI Act.

# **I**

## **Identity Verification / KYC**

Identitätsprüfung vor oder während eines digitalen Vertragsschlusses, z. B. zur Erfüllung gesetzlicher Vorgaben oder zur Risikominimierung.

**Quellen:** eIDAS; Art. 32 DSGVO.

## **Indirect Prompt Injection**

Angriffsform, bei der externe Inhalte ein KI-System manipulieren.  
Relevant, wenn KI Vertragshandlungen oder Zustimmungsprozesse beeinflusst.

**Quellen:** BSI: Indirect Prompt Injections.

## **Internationale Regelungsvorschläge (UNCITRAL / ELI)**

Modellregeln und Empfehlungen zur Harmonisierung digitalen Vertragsrechts.

**Quellen:** UNCITRAL Model Law on Electronic Commerce.

# **K**

## **KI und Vertragsschluss**

Einsatz von KI zur Entscheidungsunterstützung, Generierung oder Prüfung von Verträgen.  
Erfordert Transparenz und menschliche Aufsicht.

**Quellen:** Art. 14 EU AI Act (Human Oversight), Art. 50 EU AI Act.

## **Kopplungsverbot**

Einwilligungen dürfen nicht als Voraussetzung für eine Leistung verlangt werden, wenn sie hierfür nicht erforderlich sind.

**Quellen:** Art. 7 Abs. 4 DSGVO.

# **L**

## **Legal Hold**

Prozess zur rechtlichen Sicherung und Aufbewahrung relevanter Daten bei Rechtsstreitigkeiten.

**Quellen:** Art. 5 Abs. 1 lit. e DSGVO (Speicherbegrenzung – Ausnahmen).

# **P**

## **P2B-Verordnung**

Regelt Transparenz und Fairness zwischen Plattformbetreibern und gewerblichen Nutzern.

**Quellen:** P2B-VO (EU) 2019/1150.

## **Praxisbeispiele digitaler Zustimmungssysteme**

Clickwrap, Scrollwrap, elektronische Signaturen, App-Zustimmungssysteme.

**Quellen:** Rechtsprechung zum elektronischen Geschäftsverkehr.

## **Prompt Injection Protection**

Sicherheitsmaßnahmen zur Vermeidung unerlaubter Steuerung von KI in Vertragsprozessen.

**Quellen:** BSI – Prompt Injections; NIST AI RMF (Measure/Manage)

## **Providerhaftung**

Verantwortlichkeit von Plattformen für Nutzerinhalte nach DSA und nationalem Recht.

**Quellen:** Art. 4 ff. DAS.

# **S**

## **Scrollwrap**

Zustimmung nach vorherigem Scrollen durch Bedingungen.  
Juristisch anerkannt, sofern klare Zustimmungshandlung erfolgt.

**Quellen:** BGH zum Online-Vertragsschluss.

## **Secure Execution Environment**

Isolierte Umgebung zur sicheren Verarbeitung von Zustimmungsvorgängen und Vertragsdaten.

**Quellen:** Art. 32 DSGVO; BSI: Sicherheitsgrundlagen.

## **Signaturplattformen**

Systeme, die E-Signaturen bereitstellen, oft mit Identitätsprüfung und Audit Logs.

**Quellen:** eIDAS; Art. 28 DSGVO.

## **Smart Contracts**

Automatisierte Programme, die Vertragsbedingungen technisch durchsetzen.

**Quellen:** EU AI Act Erwägungsgründe zu KI-gestützten Entscheidungsprozessen.

## **Smart Locks**

Digitale Zugangskontrollsysteme, häufig mit automatisierten Zahl- und Vertragsmechanismen.

**Quellen:** Art. 32 DSGVO (Zugangskontrolle).

## **Sprachassistenten**

Digitale Systeme, die auch Willenserklärungen ermöglichen.  
Erfordern klare Zuordnung der Erklärung zu einer Person.

**Quellen:** §§ 116 ff. BGB; Art. 7 DSGVO.

## **T**

### **Transparency Disclosures (KI)**

Pflichtangaben beim Einsatz von KI-Systemen in Vertrags- oder Entscheidungssituationen.

**Quellen:** Art. 50–52 EU AI Act.

## **U**

### **UNCITRAL**

UN-Kommission zu internationalem Handelsrecht; maßgeblich für digitale Vertragsnormen.

**Quellen:** UNCITRAL ML on E-Commerce.

### **User Intent Verification**

Mechanismen zur Absicherung, dass ein Nutzer tatsächlich einen Vertrag abschließen oder eine Einwilligung erteilen möchte. Umfasst zusätzliche Bestätigungsabfragen, Captchas oder biometrische Verifikation. Dient der Vermeidung automatisierter oder unbeabsichtigter Vertragsabschlüsse.

**Quellen:** §§ 116 ff BGB. (Willenserklärung); Art. 7 DSGVO (Freiwilligkeit); Art. 25 DSA.

### **UX (User Experience)**

Gesamtheit der Erfahrungen und Wahrnehmungen eines Nutzers bei der Interaktion mit einem digitalen System, einer Website oder einer Anwendung. Im Kontext digitaler Vertragsschlüsse und Zustimmungssysteme ist die UX-Gestaltung rechtlich relevant: Sie entscheidet darüber, ob Einwilligungen freiwillig, informiert und bewusst erteilt werden – oder ob manipulative Gestaltungsmuster (Dark Patterns) die Entscheidungsfreiheit des Nutzers beeinträchtigen. Eine rechtskonforme UX muss Transparenz, Verständlichkeit und Gleichwertigkeit der Wahlmöglichkeiten (z. B. „Akzeptieren“ und „Ablehnen“ gleich gestaltet) sicherstellen.

**Quellen:** Art. 7 DSGVO (Freiwilligkeit der Einwilligung); Art. 25 DSA (Verbot irreführender Gestaltung); Art. 50 ff. EU AI Act (Transparenzpflichten bei KI-Interfaces); EDSA-Leitlinien zu Dark Patterns.

# W

## **Widerrufsmanagement**

Prozesse zur Ausübung des Widerrufsrechts: technische Umsetzung, Fristen, Bestätigungen.

**Quellen:** Art. 7 Abs. 3 DSGVO; Verbraucherrechte-RL.

# Passende Weiterbildungen finden Sie hier:

## Weiterbildung zum Thema Recht

Finden Sie aus unserem breiten, erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. [Jetzt informieren.](#)

## e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen. [Jetzt testen.](#)

## Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als [Inhouse-Training](#). Jetzt individuelles [Angebot anfordern.](#)