

1. September 2026 | Battke Frühstück Unternehmensrecht & Schutzrechte

Teuer bezahlt, schlecht verhandelt?

Die 10 größten Fehler bei Softwarebeschaffung und -Nutzung

Rechtsanwalt Dr. Daniel Schöneich | Fachanwalt Für Gewerblichen Rechtsschutz



Warum dieses Thema?

70%

aller IT-Projekte verfehlen
Zeit- oder Budgetvorgaben

Standish Group CHAOS Report

Mehrere Mrd.

Schaden durch das
IT-Desaster des Bundes

Bundesrechnungshof

50%

der Streitigkeiten betreffen
Leistungsbeschreibung

Branchenanalyse IT-Recht

IT-Projekte scheitern selten an Technik – meist an vermeidbaren rechtlichen und vertraglichen Fehlern.

Drei Phasen – ein gemeinsames Risiko

Die meisten rechtlichen Fehler entstehen nicht durch bösen Willen, sondern durch Unkenntnis oder Zeitdruck. Die drei kritischen Phasen jedes IT-Projekts:

1

Phase 1: Vertragsschluss

Leistungsbeschreibung,
Vertragstyp, Lizenzmodell, IPR,
Vergabeverfahren

2

Phase 2: Implementierung

Änderungsmanagement, Abnahme,
Termine, Datenschutz

3

Phase 3: Betrieb

SLAs, Exit-Strategie,
Pflegeverträge, Compliance

Jede Phase birgt eigene Fallstricke – und jede kann das gesamte Projekt gefährden.

Fail 1: Unzureichende Leistungsbeschreibung



© Adobe Stock , sebra

Das Problem

- Vage Anforderungen führen zu Rügen oder Streit über den Leistungsumfang.
- **Beispiel:** „Die Software soll alle Prozesse der Buchhaltung abbilden“

Lösung

- Markterkundung nach § 28 VgV vorab
- Lastenheft mit Muss/Soll/Kann-Kriterien und messbaren Akzeptanzkriterien
- Prüfung durch IT-Sachverständige und Rechtsberatung vor Veröffentlichung

Fail 2: Vertragstyp & Lizenzmodelle

Falsche Vertragstyp-Wahl

Agile Projekte im starren Werkvertragsschema.

Individualsoftware als Dienstvertrag → kein Abnahme- und Gewährleistungsanspruch.

Öffentliche Hand: EVB-IT-Muster konsequent nutzen (Erstellung, System, Cloud, Pflege S).

Lizenzmodelle nicht verstanden

Named User in Shared-Umgebungen,

fehlende/nachteilige Audit-Klauseln
→ sechsstellige Nachforderungen möglich.

Erschöpfungsgrundsatz gilt nur bei dauerhafter Überlassung – nicht bei SaaS.

Best Practice: Vorab-Analyse des Lizenzmodells durch IT und Rechtsberatung. Audit-Klauseln verhandeln. Software Asset Management (SAM) etablieren. Nachlizenzierungsbedingungen mit Preisobergrenzen vertraglich regeln.

Fail 3: Open Source & IPR

Open-Source-Risiken

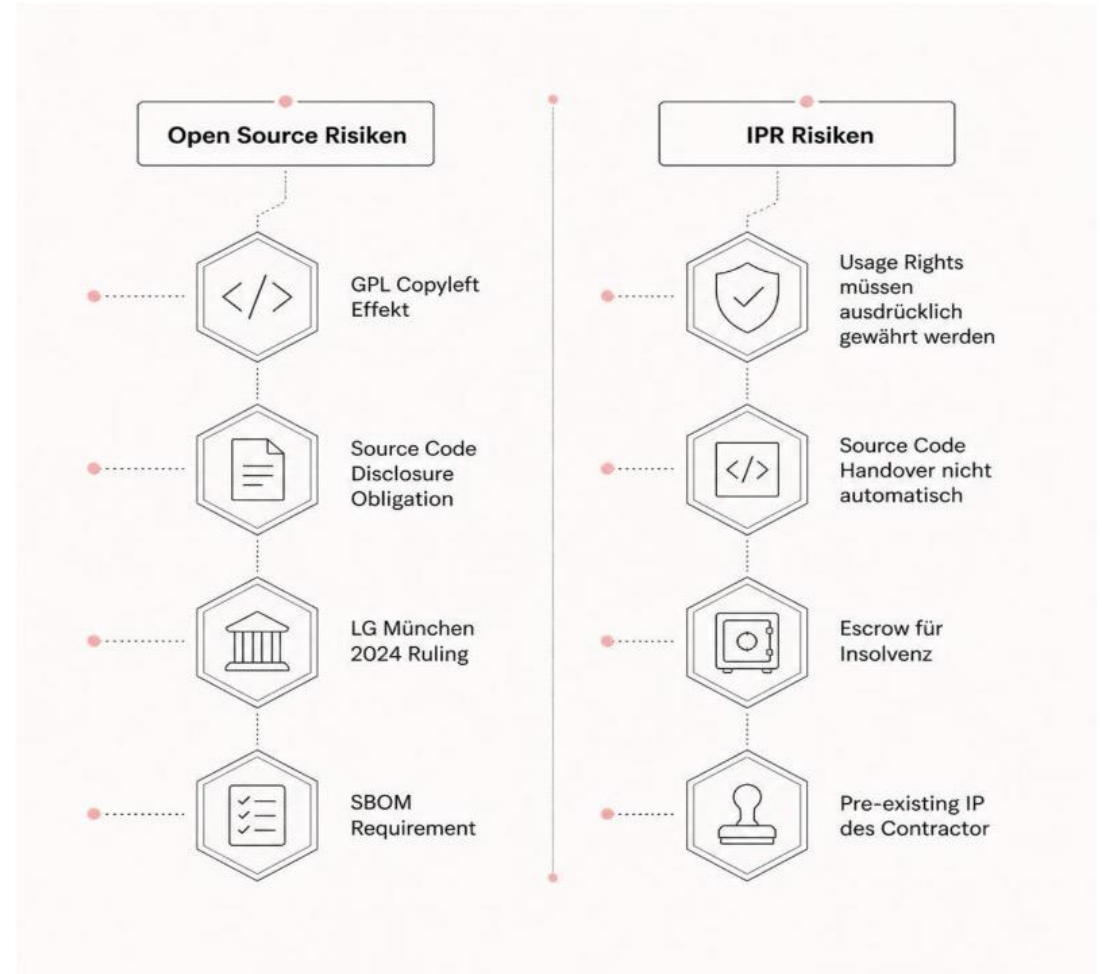
Copyleft-Wirkung der GPL wird unterschätzt: gesamter abgeleiteter Quellcode muss offengelegt werden.

SBOM als Vertragsbestandteil fordern.

IPR bei Individualentwicklung

Nutzungsrechte müssen ausdrücklich eingeräumt werden (§ 31 Abs. 5 UrhG: Zweckübertragungsregel).
Quellcode-Herausgabe kein Automatismus.

Nutzungsrechte mit Drittanbietern



Fail 4: Vergabeverfahren

Verfahrensfehler

De-facto-Vergabe an Bestandsanbieter,

unzulässiges Verhandeln im offenen Verfahren.

Schwellenwert: 216.000 EUR

Vertragsfehler

Leerer EVB-IT-Vertrag an Bieter übergeben,

Vertragsverhandlung nach Zuschlagerteilung.

Best Practice:

Verhandlungsverfahren (§ 17 VgV) für komplexe IT.

Eigenes Vertragsmuster vorlegen, EVB-IT möglichst vollständig ausfüllen. Lückenlose Dokumentation von Beginn an



@ Unsplash, Steven Cordes

Fail 5: Änderungsmanagement & Abnahme



@ Adobe Stock, kasto

Change Requests ohne Struktur

Mündliche Änderungen führen oft zu Streit über Mehrkosten und Leistungsumfang => Beweislastprobleme

Bei öffentlicher Hand: Nachtragsvergabe nach § 132 GWB beachten (Wesentlichkeitsgrenze).

Abnahme nicht oder falsch

Konkludente Abnahme durch Inbetriebnahme löst Verjährung und Zahlungsanspruch aus.
Ohne formales Abnahmeprotokoll: Gefahrübergang und Beweislastumkehr unklar.

Fail 6: Datenschutz & Datenmigration



AVV nach Art. 28 DSGVO

Auftragsverarbeitungsvertrag von Anfang an mitverhandeln – kein optionales Add-on. Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO konkret benennen.



Drittlandtransfer

Standardvertragsklauseln (SCCs), Transfer Impact Assessment (TIA) und EU-US Data Privacy Framework prüfen – insbesondere bei US-Cloud-Anbietern.



Datenmigration

Migrationskonzept als Vertragsanlage: Formate, Verantwortlichkeiten, Zeitplan, Rollback-Szenario. **Exit-Strategie und Datenportabilität** bereits bei Vertragsschluss regeln.

Fail 7: Vendor Lock-in vermeiden – Vertiefung



Exit-Strategie & Datenportabilität

Definition von Prozessen und Formaten für die Datenmigration. Sicherstellen, dass Daten in **offenen, maschinenlesbaren Formaten** exportiert werden können, um eine reibungslose Übernahme durch einen anderen Anbieter zu ermöglichen.



Quellcode-Escrow

Für geschäftskritische Individualentwicklungen: eine **Quellcode-Hinterlegung** bei einem neutralen Treuhänder. Dies gewährleistet den Zugriff auf den Code, sollte der Anbieter seine Leistungen nicht mehr erbringen können (z.B. Insolvenz).



Offene Standards & Transitionssupport

Vertragliche Verpflichtung zur Nutzung **offener Schnittstellen (APIs)** und Standards. Der Anbieter muss aktive Transitionsunterstützung leisten, inklusive Wissenstransfer und Dokumentation für einen reibungslosen Wechsel.



Fail 8: SLAs

Problem: SLAs ohne Konsequenzen

„99,9 % Verfügbarkeit“ – aber Wartungsfenster und Teilausfälle ausgenommen. De facto oft unter 95 %.

Reaktions- und Wiederherstellungszeit → richtige Definition

Service Credits und Sonderkündigungsrecht bei wiederholter SLA-Unterschreitung vertraglich verankern.

Regelmäßiges SLA-Reporting als Anbieterpflicht.

Fail 9: Pflegeverträge & Compliance

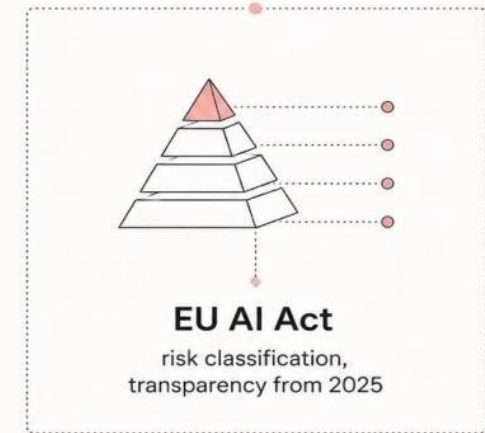
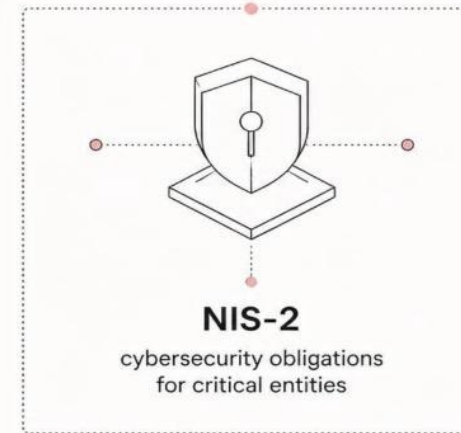
Pflege- und Updateverträge

Keine gesetzliche Pflegepflicht.

Cyber Resilience Act (VO 2024/2847) verpflichtet ab 2027 zur Bereitstellung von Sicherheitsupdates über den gesamten Produktlebenszyklus.

Pflegevertrag parallel zum Hauptvertrag verhandeln – mit Reaktionszeiten, Updates und Preisanpassungsklauseln.

Regulatorische Compliance



Fail 10: Unklare Strategie im Konfliktfall

Vertragsauflösung?

Pro:

- "neuer Wind,,
- Adaptionenmöglichkeit für Leistungsverzeichnis

Contra:

- Zeitverzug
- Ausschreibung?
- Zusatzkosten
- Klageverfahren?

"Ersatzvornahme"?

Pro:

- Zeitgewinn
- Kostenvorschuss

Contra:

- Zugänglichkeit Quellcode → ZBR?
- Ausschreibung?
- Abgrenzung alter / neuer Anbieter

Fortsetzung?

Pro:

- Zeitgewinn im Vergleich zu Alternat.
- kein Klageverfahren

Contra:

- Unzuverlässigkeit?
- Vertrauen (-) bei langem Vertrag