Vertragsanforderungen — Prüfmatrix nach DORA Art. 28 Abs. 7

Version 1.0 | Mai 2026 | Alexander Martens

Ziel dieser Prüfmatrix

DORA Art. 28 Abs. 7 listet 15 vertragliche Mindestinhalte, die jeder IKT-Dienstleistungsvertrag enthalten muss. Diese Prüfmatrix hilft, bestehende Verträge systematisch zu analysieren und Handlungsbedarf zu identifizieren.

Die 15 Mindestanforderungen (Art. 28 Abs. 7 lit. a–o)

Nr	Anforderung	Beschreibung	Status	Nachweis
a	Leistungsbeschreibung	Eindeutige, vollständige Beschreibung aller Funktionen und Dienstleistungen des IKT-Drittdienstleisters		
b	Datenverarbeitungsstandorte	Angabe der Standorte (Regionen/Länder), an denen die Datenverarbeitung erfolgt (inkl. Subunternehmer)		
c	Service-Levels	Verfügbarkeit, Qualität, Performance — einschließlich quantitativer und qualitativer Ziele		
d	Unterstützung bei Vorfällen	Verpflichtung des Dienstleisters zur unverzüglichen Unterstützung bei IKT-Vorfällen — kostenlos oder zu vorab definierten Kosten		
e	Meldefristen	Verbindliche Fristen für die Meldung von		

Nr	Anforderung	Beschreibung	Status	Nachweis
		IKT-Vorfällen durch den Dienstleister		
f	Sicherheitsmaßnahmen	Verpflichtung zur Umsetzung angemessener technischer und organisatorischer Maßnahmen (TOM)		
g	Prüfungsrechte	Uneingeschränkte Zugriffs-, Inspektions- und Prüfungsrechte — durch das Institut oder beauftragte Dritte		
h	Exit-Strategien	Verbindliche Übergangsfristen und Migrationspfade bei Beendigung		
i	Kündigungsrechte	Kündigungsrechte bei wesentlichen Pflichtverletzungen, Leistungsmängeln, Sicherheitsvorfällen — sowie außerordentliches Kündigungsrecht bei aufsichtsrechtlichen Anordnungen		
j	Subunternehmer	Regelungen zur Hinzuziehung von Subunternehmern — einschließlich Genehmigungspflicht und Transparenz über Sub-Dienstleister		
k	SLA-Definitionen	Detaillierte Service Level Agreements mit Messgrößen, Schwellwerten		

Nr	Anforderung	Beschreibung	Status	Nachweis
		und Eskalationsmechanismen		
l	Berichtspflichten	Umfang und Frequenz der Berichterstattung — einschließlich Sicherheitsvorfälle, SLA-Erfüllung und Änderungen		
m	Datenschutz-Compliance	Einhaltung der DSGVO — einschließlich Auftragsverarbeitungsvertrag (AVV), Betroffenenrechte und Meldepflichten		
n	Testpflichten	Teilnahme an Resilienztests — einschließlich TLPT und Sicherheitsaudits		
o	Business Continuity	Notfallvorsorge und Business-Continuity-Pläne — inkl. Testverpflichtung		

Gap-Analyse je Dienstleister

Dienstleister: _____ | Vertrag vom: _____

Anforderung (Art. 28 Abs. 7)	Vertraglich geregelt?	Bewertung (1–5)	Handlungsbedarf	Priorität
a) Leistungsbeschreibung				
b) Standorte				
c) Service-Levels				
d) Vorfall-Unterstützung				
e) Meldefristen				

Anforderung (Art. 28 Abs. 7)	Vertraglich geregelt?	Bewertung (1–5)	Handlungsbedarf	Priorität
f) Sicherheitsmaßnahmen				
g) Prüfungsrechte				
h) Exit-Strategien				
i) Kündigungsrechte				
j) Subunternehmer				
k) SLA-Definitionen				
l) Berichtspflichten				
m) Datenschutz				
n) Testpflichten				
o) Business Continuity				

Handlungsempfehlungen nach Gap-Analyse

Gesamtbewertung	Maßnahme	Frist
> 90 % (13–15 Punkte)	Vertragsanpassung im nächsten regulären Turnus	12 Monate
60–90 % (9–12 Punkte)	Gezielte Nachverhandlung der schwachen Klauseln	6 Monate
< 60 % (< 9 Punkte)	Neuverhandlung oder Ersatz des Dienstleisters prüfen	3 Monate

---

Disclaimer: Diese Prüfmatrix dient der fachlichen Orientierung. Maßgeblich sind der Originaltext der DORA-Verordnung und die jeweils aktuelle BaFin-Auslegung.