

MASTERARBEIT | MASTER'S THESIS

Titel | Title

SaaS Beschaffung der öffentlichen Hand: Vergleichbarkeit und Transparenz
Herausforderungen und Lösungen im Rechtsvergleich Österreich/Deutschland

verfasst von | submitted by

Mag.iur. Christina Steininger

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of
Master of Laws (LLM)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 066 997

Studienrichtung lt. Studienblatt | Degree
programme as it appears on the student
record sheet:

Masterstudium Internationale Rechtswissenschaften

Betreut von | Supervisor:

Univ.-Prof. Mag. Dr. Nikolaus Forgó

Danksagung

Mein besonderer Dank gilt meinen Eltern, die meinen Bildungsweg stets unterstützt und gefördert haben. Sie standen mir immer zur Seite, haben mir Vertrauen entgegengebracht und mich in meinen Entscheidungen bestärkt.

Ihre Unterstützung, ihr Rückhalt und ihr Glaube an mich haben wesentlich dazu beigetragen, dass ich meinen Weg gehen konnte. Dafür bin ich ihnen von Herzen dankbar.

KI-Vermerk

Im Rahmen der Erstellung dieser Masterarbeit wurden KI-gestützte Tools (insbesondere Claude und Grammarly) zur sprachlichen Unterstützung, für Grammatikprüfung und stilistische Überarbeitungen, herangezogen.

Die inhaltliche Konzeption, die rechtliche Analyse sowie die Argumentation wurden eigenständig von der Verfasserin erarbeitet. Sämtliche durch KI generierten Vorschläge wurden kritisch geprüft und gegebenenfalls überarbeitet.

Die Verfasserin trägt die alleinige Verantwortung für den Inhalt dieser Arbeit.

Abstract

Diese Masterarbeit untersucht die Beschaffung von Software-as-a-Service-Lösungen durch öffentliche Stellen und stellt dabei die vergaberechtlichen Grundsätze der Transparenz und Vergleichbarkeit in den Mittelpunkt. Ausgangspunkt ist die wachsende Bedeutung cloudbasierter Modelle für den öffentlichen Sektor sowie die damit verbundenen Herausforderungen für die Gestaltung rechtssicherer Vergabeverfahren.

Im Zentrum der Analyse stehen drei Problemfelder, die sich im Zuge der Vorarbeiten besonders klar herauskristallisierten: die eingeschränkte Vergleichbarkeit aufgrund heterogener Preismodelle und dynamischer Leistungsstrukturen, das Risiko eines Vendor-Lock-in sowie datenschutzrechtliche Anforderungen, insbesondere im Zusammenhang mit Drittstaatentransfers nach der *Schrems-II*-Judikatur. Gerade diese Bereiche erwiesen sich als praktisch konfliktanfällig und prägend für die Vergabepaxis.

Methodisch basiert die Arbeit auf einer rechtsdogmatischen Analyse des österreichischen und deutschen Vergaberechts unter Einbeziehung unionsrechtlicher Vorgaben sowie auf einem rechtsvergleichenden Ansatz.

Die Untersuchung zeigt, dass das geltende Vergaberecht grundsätzlich geeignete Instrumente zur Bewältigung der identifizierten Herausforderungen bereitstellt. Auffällig war dabei, dass viele dieser Instrumente – etwa die funktionale Leistungsbeschreibung, die szenariobasierte Lebenszykluskostenrechnung oder ein strukturiertes Exit-Management – bereits *de lege lata* verfügbar sind, in der Praxis jedoch häufig nur zurückhaltend genutzt werden. Auch Service-Level-Agreements erweisen sich als wesentliches Steuerungsinstrument, dessen Potenzial nicht immer ausgeschöpft wird.

Im Rechtsvergleich wird deutlich, dass Deutschland mit standardisierten Vertragswerken wie den EVB-IT Cloud stärker institutionalisierte Lösungen verfolgt, während Österreich überwiegend auf eine flexible, einzelfallbezogene Gestaltung abstellt.

Abschließend entwickelt die Arbeit praxisorientierte Handlungsempfehlungen für Vergabestellen sowie für den Gesetzgeber. Diese leiten sich vor allem aus wiederkehrenden Problemstrukturen ab, die während der Analyse sichtbar wurden. Ziel ist es, eine transparente, vergleichbare und wettbewerbsfördernde Beschaffung von SaaS-Lösungen sicherzustellen und zugleich den besonderen Anforderungen cloudbasierter Modelle angemessen Rechnung zu tragen.

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch (Österreich)
ABl	Amtsblatt der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
Art	Artikel
B2B-Geschäfte	Business-to-Business Geschäfte
BGBI	Bundesgesetzblatt (Österreich bzw Deutschland – aus dem Kontext ersichtlich)
BGB	Bürgerliches Gesetzbuch (Deutschland)
BGH	Bundesgerichtshof (Deutschland)
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVergG 2018	Bundesvergabegesetz 2018 BGBI I 2018/65 idF BGBI. I 2023/148
BVwG	Bundesverwaltungsgericht (Österreich)
BYOK	Bring Your Own Key (Schlüsselhoheit bei der Vergabestelle)
bzw	beziehungsweise
CapEx	Capital Expenditures (einmalige Investitionsaus-/Kapitalausgaben)
CC	Confidential Computing (hardwaregestützte geschützte Ausführungsumgebung)
CR	Computer und Recht (Zeitschrift)
Dako	Datenschutz korrekt
DPF	EU-US Data Privacy Framework (Angemessenheitsbeschluss nach Art 45 DSGVO vom 10.7.2023)
DSGVO	Datenschutz-Grundverordnung
DSFA-V	Datenschutz-Folgenabschätzungs-Verordnung
ECLI	European Case Law Identifier (Europäischer Identifikator für Rechtsprechung)

ecolex	ecolex – Fachzeitschrift für Wirtschaftsrecht
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss (deutsche Übersetzung zum EDPB)
ErläutRV	Erläuterungen zur Regierungsvorlage
ErwGr	Erwägungsgrund
etc	et cetera
EuGH	Gerichtshof der Europäischen Union
EVB-IT Cloud	Ergänzende Vertragsbedingungen für die Beschaffung von Cloudleistungen (Deutschland), BMI-Mustervertrag vom 1.3.2022
f, ff	folgende(r), fortfolgende
GP	Gesetzgebungsperiode
GWB	Gesetz gegen Wettbewerbsbeschränkungen (Deutschland)
Hrsg	Herausgeber:innen
IaaS	Infrastructure as a Service
idF	in der Fassung
insb	insbesondere
ISMS	Informationssicherheits-Managementsystem
ISO/IEC 27001	ISO/IEC 27001:2013, Anforderungen an ein Informationssicherheits-Managementsystem
IT	Informationstechnologie
ITRB	IT-Rechtsberater (Zeitschrift)
iVm	in Verbindung mit
jusIT	Zeitschrift für IT-Recht und Digitalisierung
KG	Kammergericht (Deutschland)
MMR	Multimedia und Recht (ab 2025: Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT) (Zeitschrift)

NIST	National Institute of Standards and Technology (insb NIST SP 800-145)
NZBau	Neue Zeitschrift für Baurecht und Vergaberecht
ÖNORM	Österreichische Norm
OGH	Oberster Gerichtshof (Österreich)
OLG	Oberlandesgericht (Deutschland)
OpEx	Operational Expenditures (laufende Betriebsausgaben)
PaaS	Plattform as a Service
PwC	PricewaterhouseCoopers Austria
RH	Österreichischer Rechnungshof
RL 2014/24/EU	Richtlinie über die öffentliche Auftragsvergabe (Vergaberichtlinie)
RL 2019/770/EU	Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (Digitale-Inhalte-Richtlinie)
Rn	Randnummer
Rsp	Rechtsprechung
Rz	Randzahl
SaaS	Software as a Service
SLA	Service-Level-Agreement
TCO	Total Cost of Ownership, Deutsch: Lebenszykluskosten
TIA	Transfer Impact Assessment (Datentransfer-Folgenabschätzung)
TOM	Technische und organisatorische Maßnahmen
ua	unter anderem
UfAB	Unterlage für Ausschreibung und Bewertung von IT-Leistungen
vgl	vergleiche
Vgv	Vergabeverordnung (Deutschland)

VwGH	Verwaltungsgerichtshof (Österreich)
Z	Ziffer
zB	zum Beispiel
ZIB	Beschaffungsamt des Bundesministeriums des Innern Zentralstelle IT-Beschaffung
ZIIR	Zeitschrift für IT- und Internet-Recht
ZVB	Zeitschrift für Vergabe- und Bauvertragsrecht

Inhaltsverzeichnis

1. Einleitung	1
2. Grundlagen: Was ist SaaS und wie wird es rechtlich eingeordnet?	3
2.1. Technische Grundlagen (Cloud-Computing, SaaS, IaaS, PaaS, Bereitstellungsmodelle)	3
2.2. Abgrenzung: On-Premise-Modelle vs SaaS (CapEx vs OpEx, Verantwortungsteilung)	6
2.3. Zivil- und vergaberechtliche Einordnung von SaaS-Verträgen	6
2.3.1. <i>Zivilrechtliche Einordnung: Der SaaS-Vertrag als Mischvertrag</i>	8
2.3.2. <i>Vergaberechtliche Einordnung: SaaS als Dienstleistungsauftrag</i>	9
2.3.3. <i>Rechtsvergleich: Unterschiedliche Lösungsansätze in Österreich und Deutschland</i>	10
2.4. Vergaberechtliche Grundsätze und ihre Bedeutung für SaaS-Beschaffungen	12
3. Welche Herausforderungen ergeben sich?	16
3.1. Vergleichbarkeitsproblem: Heterogene Preismodelle und dynamische Leistungen	17
3.2. Abhängigkeitsproblem: Vendor-Lock-in durch proprietäre Strukturen	20
3.3. Datenschutzproblem: Drittstaatentransfers und die "Schrems II"-Judikatur	22
3.3.1. <i>Die Schrems II-Problematik als zentrale Herausforderung</i>	23
3.3.2. <i>Technische und organisatorische Maßnahmen als Kompensation</i>	24
3.3.3. <i>Datenschutz-Folgenabschätzung als Pflichtinstrument</i>	24
3.3.4. <i>Konsequenzen für die Vergabepraxis</i>	25
4. Welche Lösungen bietet das Vergaberecht?	27
4.1. Technologieneutralität durch funktionale Leistungsbeschreibung	27
4.1.1. <i>Funktionsbezogene Leistungsbeschreibung als Regelmodell</i>	27
4.1.2. <i>Sachlichkeitsprüfung technologiebezogener Vorgaben</i>	28
4.1.3. <i>Gleichwertigkeitsprinzip und Nachweisführung</i>	29
4.2. Vergleichbarkeit durch szenariobasierte TCO-Bewertung	31
4.2.1. <i>Methodische Grundlagen der TCO-Bewertung</i>	31
4.2.2. <i>Operationalisierung durch Referenzszenarien</i>	32
4.2.3. <i>Rechtsvergleichende Perspektive</i>	33
4.2.4. <i>Praktische Umsetzung in den Vergabeunterlagen</i>	34
4.3. Qualitätssteuerung durch Service-Level-Agreements (SLAs)	35
4.3.1. <i>Die Herausforderung der Vergleichbarkeit von SLA-Parametern</i>	35
4.3.2. <i>Sicherheitsanforderungen und technische Standards</i>	37
4.3.3. <i>Vergaberechtliche Einordnung von SLA-Parametern</i>	37
4.3.4. <i>Rechtsvergleichende Perspektive: Österreich vs. Deutschland</i>	38
4.3.5. <i>Vertragliche Absicherung und Durchsetzbarkeit</i>	39
4.4. Risikominimierung durch vertragliches Exit-Management	40
4.4.1. <i>Exit-Management als vergaberechtliche Notwendigkeit</i>	40

4.4.2.	<i>Technische Anforderungen an die Datenportabilität</i>	40
4.4.3.	<i>Ökonomische Dimension: Exit-Kosten in der TCO-Bewertung</i>	41
4.4.4.	<i>Rechtsvergleichende Perspektive: Unterschiedliche Lösungsansätze</i>	42
4.4.5.	<i>Synthese: Exit-Management als Wettbewerbsvoraussetzung</i>	43
5.	Rechtsvergleich Österreich vs. Deutschland: Standardisierung vs. Flexibilität	44
5.1.	Deutschland: Institutionalisierte Lösung durch EVB-IT Cloud und UfAB	45
5.2.	Österreich: Prozessuale Lösung durch Einzelfallgestaltung	48
5.3.	Vergleichende Bewertung der Ansätze	51
6.	Kritische Analyse der österreichischen Praxis	54
6.1.	Empirischer Befund: Die „On-Premise-only“-Präferenz	55
6.2.	Vergaberechtliche Bewertung: Verstoß gegen Wettbewerb und Technologieneutralität	57
6.3.	Ökonomische Bewertung: Verkürzte Wirtschaftlichkeitsprüfung und Innovationshemmnisse	58
6.4.	Datenschutzrechtliche Bewertung: Schrems II als unzulässige Pauschalbegründung	60
7.	Handlungsempfehlungen für eine innovationsoffene Vergabepaxis	62
7.1.	Für Vergabestellen: Markterkundung, Leistungsbeschreibung und TCO-Modelle	62
7.2.	Für den Gesetzgeber: Standardisierung, Leitfäden und Schulungen	64
8.	Zusammenfassung und Ausblick	65
9.	Schlussbemerkung	69
	Literaturverzeichnis	70
	Judikaturverzeichnis	71
	Verzeichnis der Studien, Leitfäden und Behördendokumente	72
	Internetquellen	74

1. Einleitung

Die digitale Transformation hat die Beschaffungspraxis öffentlicher Vergabestellen grundlegend verändert und vor neue, komplexe Herausforderungen bei der Gestaltung von Vergabeverfahren gestellt.¹ Während in der Vergangenheit vor allem lokal installierte Softwarelösungen und herkömmliche Lizenzmodelle den Markt dominierten, gewinnen cloudbasierte Lösungen – insbesondere „Software as a Service“ (SaaS) – zunehmend an Bedeutung und prägen die IT-Beschaffung im öffentlichen Sektor maßgeblich.²

Ein zentrales Anliegen im öffentlichen Sektor ist jedoch die rechtssichere Gestaltung von Ausschreibungen sowie die objektive Vergleichbarkeit unterschiedlicher Angebote, um die verpflichtend einzuhaltenden Grundsätze der Transparenz, Gleichbehandlung und des fairen Wettbewerbs nach dem Bundesvergabegesetz 2018 (BVergG 2018) zu gewährleisten.³ Diese vergaberechtlichen Grundsätze setzen voraus, dass die ausgeschriebenen Leistungen eindeutig beschrieben sind und eingehende Angebote objektiv miteinander verglichen werden können. Gerade bei der Beschaffung von SaaS-Diensten erweist sich dies jedoch als anspruchsvoll, da sich cloudbasierte Leistungen häufig durch flexible Leistungsumfänge, unterschiedliche Vertrags- und Vergütungsmodelle sowie dynamische Weiterentwicklungen auszeichnen.⁴ Für öffentliche Vergabestellen stellt sich daher die Frage, wie Vergabeverfahren so gestaltet werden können, dass einerseits innovationsoffene Lösungen ermöglicht werden und andererseits die Vergleichbarkeit der Angebote gewahrt bleibt. Diese Spannung führt in der Praxis häufig zu Unsicherheiten, insbesondere im Hinblick darauf, wie Ausschreibungen transparent und nachvollziehbar ausgestaltet werden können, ohne die Innovations- und Gestaltungsfreiheit unterschiedlicher SaaS-Lösungen unnötig einzuschränken.⁵

Neben diesen vergaberechtlichen Herausforderungen wirft die Beschaffung von SaaS-Diensten auch datenschutz- und sicherheitsrechtliche Fragen auf. Insbesondere bei der

¹ vgl. *Claßen/Koch/Müller*, Beschaffung von Cloud-Services durch öffentliche Auftraggeber, MMR 2020, 723 (723).

² vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (724); siehe auch *Strittmatter in Auer-Reinsdorff/Conrad* (Hrsg), Handbuch IT- und Datenschutzrecht³ (2019) § 22 Rn 1.

³ § 20 Bundesvergabegesetz 2018 BGBl I 2018/65 idF BGBl I 2023/148 (BVergG 2018); § 97 Abs 1 Gesetz gegen Wettbewerbsbeschränkungen, dBGBI I 2013, 1750, zuletzt geändert durch Art. 6 des Gesetzes vom 5.12.2024, dBGBI I 2024, 400 (GWB); vgl. EuGH C-496/99 P, *Commission of the European Communities v CAS Succhi di Frutta SpA*, ECLI:EU:C:2004:236, Rn 111; *Gölles in Gölles/Casati* (Hrsg), BVergG 2018 § 137 Rn 1 (Stand 1.10.2020, rdb.at).

⁴ vgl. *Heydn*, Software-as-a-Service – Probleme und Vertragsgestaltung, MMR 2020, 435 (437); siehe auch *Claßen/Koch/Müller*, MMR 2020, 723 (726).

⁵ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (725).

Verarbeitung personenbezogener Daten in Drittstaaten gewinnen diese Aspekte besondere Relevanz.⁶ Öffentliche Vergabestellen sind hier deshalb gefordert, rechtliche, technische und organisatorische Anforderungen so zu koordinieren, dass sie sowohl den Vorgaben des Vergabe- und Datenschutzrechts als auch den praktischen Bedürfnissen des IT-Betriebs gerecht werden.⁷

Diese vielschichtigen Herausforderungen betreffen dabei nicht nur die Phase der Ausschreibung, sondern erstrecken sich über den gesamten Beschaffungsprozess – von der Bedarfsdefinition und Leistungsbeschreibung, über die Angebotswertung bis hin zur vertraglichen Ausgestaltung, Durchführung und Beendigung des Vertrages.⁸

Vor diesem Hintergrund untersucht diese Arbeit die Besonderheiten der Beschaffung von SaaS-Diensten durch öffentliche Vergabestellen mit Blick auf Vergleichbarkeit und Transparenz im Vergabeverfahren. Im Mittelpunkt steht dabei ein rechtsvergleichender Ansatz zwischen Österreich und Deutschland. Obwohl beide Rechtsordnungen durch das europäische Vergaberecht⁹ harmonisiert sind, zeigen sich in der nationalen Umsetzung und vor allem in der Verwaltungspraxis Unterschiede, die sich erheblich auf die Ausgestaltung und Durchführung von SaaS-Beschaffungen auswirken können.¹⁰

Die vorliegende Arbeit verfolgt konkret die folgenden Forschungsfragen: Welche rechtlichen Herausforderungen ergeben sich bei der Beschaffung von SaaS-Diensten für öffentliche Vergabestellen in Österreich und Deutschland im Hinblick auf Vergleichbarkeit und Transparenz? In welchem Umfang bietet das geltende Vergaberecht Lösungsansätze zur Bewältigung dieser Herausforderungen? Und welche praxisorientierten Handlungsempfehlungen lassen sich daraus für eine rechtssichere und wirtschaftlich sinnvolle SaaS-Beschaffung ableiten?

Methodisch stützt sich die Arbeit auf eine rechtsdogmatische Analyse der einschlägigen vergaberechtlichen Regelungen sowie auf einen systematischen Vergleich der

⁶ vgl. EuGH C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems (Schrems II)*, ECLI:EU:C:2020:559; vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (725).

⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727).

⁸ vgl. *Schima*, Zur rechtlichen Einordnung von Software-as-a-Service-Verträgen, *ecolex* 2024, 197 (200).

⁹ RL 2014/24/EU des Europäischen Parlaments und des Rates vom 26.2.2014 über die Vergabe öffentlicher Aufträge, ABI L 2014/94, 65.

¹⁰ In Österreich umgesetzt durch: BVergG 2018 BGBl I 2018/65 idF BGBl I 2023/148; in Deutschland umgesetzt durch: GWB dBGBl I 2013, 1750, zuletzt geändert durch Art. 6 des Gesetzes vom 5.12.2024, dBGBl I 2024, 400 und die Verordnung über die Vergabe öffentlicher Aufträge, dBGBl I 2016, 624, idF dBGBl 2024 I Nr. 39 (VgV); vgl. *Tretzmüller*, Zur rechtlichen Qualifikation von Softwareverträgen, *ZfIR* 2019, 255 (255).

österreichischen und deutschen Beschaffungspraxis. Ziel ist es, einen Beitrag zur rechtlichen Einordnung und praktischen Handhabung der SaaS-Beschaffung zu leisten und Ansatzpunkte für eine verbesserte Vergleichbarkeit und Transparenz in zukünftigen Vergabeverfahren aufzuzeigen.

2. Grundlagen: Was ist SaaS und wie wird es rechtlich eingeordnet?

Die fortschreitende Digitalisierung hat insbesondere im öffentlichen Sektor zu einem Paradigmenwechsel bei der Beschaffung von IT-Dienstleistungen geführt.¹¹ Während in früheren Jahren meist lokal installierte Softwarelösungen (sogenannte „On-Premise“-Lösungen) mit klassischen Lizenz- und Wartungsverträgen im Vordergrund standen, insbesondere weil diesen Lösungen eine höhere Kontrolle über die Datenverarbeitung und die technischen Rahmenbedingungen zugeschrieben wurde, setzen sich heute zunehmend cloudbasierte Modelle durch, unter denen SaaS eine besondere Rolle einnimmt.¹² Das folgende Kapitel gibt eine Einführung in die zentralen Begrifflichkeiten und stellt die technischen und rechtlichen Grundlagen dar, die für die Beschaffung und Nutzung von SaaS-Diensten im öffentlichen Bereich von besonderer Relevanz sind.

2.1. Technische Grundlagen (Cloud-Computing, SaaS, IaaS, PaaS, Bereitstellungsmodelle)

„Cloud-Computing“ bezeichnet nach der weithin rezipierten Definition des US-amerikanischen National Institute of Standards and Technology (NIST) ein Modell, „for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction“,¹³ also ein Modell, das einen ubiquitären, bequemen, bedarfsgerechten Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Rechenressourcen ermöglicht, die schnell und mit minimalem Verwaltungsaufwand bereitgestellt und freigegeben werden können.

Bei diesem Modell handelt es sich nicht um eine eigenständig neue Technologie, sondern um eine Kombination bekannter Konzepte wie Virtualisierung, standardisierte Schnittstellen, netzwerkbasierte Bereitstellung und serviceorientierte Abrechnung. Diese Zusammensetzung wirft jedoch neue rechtliche Bewertungsfragen auf.¹⁴

¹¹ vgl. Claßen/Koch/Müller, MMR 2020, 723 (724).

¹² vgl. Claßen/Koch/Müller, MMR 2020, 723 (725).

¹³ National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, Special Publication (NIST SP) (2011), <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>, 2 (abgerufen am 20. 5.2025).

¹⁴ vgl. Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 1 ff., 10 ff.

Die technische Basis nahezu aller Cloud-Modelle bildet die Virtualisierung. Dabei werden physische Hardware-Ressourcen softwareseitig zu einer logischen Einheit gebündelt und derart segmentiert, dass die Verteilung über verschiedene Server für die Nutzenden vollkommen unsichtbar bleibt. Ein konstitutives Merkmal moderner Cloud-Architekturen – insbesondere im Bereich SaaS – ist dabei die Mehrmandantenfähigkeit („Multi-Tenancy“). Im Gegensatz zu klassischen IT-Modellen erfolgt hier keine Zuweisung einer dedizierten Hardwareinstanz; vielmehr teilen sich mehrere Nutzende eine gemeinsame, hardwareunabhängige Infrastruktur effizient auf.¹⁵

Auf Basis dieser Virtualisierungstechnologie lassen sich drei grundlegende Service-Modelle unterscheiden, die für die vergaberechtliche Einordnung entscheidend sind:¹⁶ „Infrastructure as a Service“ (IaaS) stellt virtualisierte IT-Ressourcen wie Rechenleistung, Speicherplatz oder Netzkapazitäten als Dienstleistung zur Verfügung.¹⁷ Darauf können kundenspezifische Betriebssysteme, Anwendungen und Dienste betrieben werden, wobei Nutzende Verantwortung für deren Konfiguration, Verfügbarkeit und Sicherheit haben.¹⁸

„Platform as a Service“ (PaaS) bietet vordefinierte Plattformen an. Beispiele hierfür sind Entwicklungsumgebungen oder Datenbanken.¹⁹ Anbietende verantworten die Plattform, während Nutzende die darauf entwickelten Applikationen und die Daten verwalten.²⁰

„Software as a Service“ (SaaS) schließlich stellt standardisierte und fertig entwickelte Softwareanwendungen über das Internet bereit, auf die Nutzende über das Internet zugreifen, ohne dass diese lokal bei Nutzenden - also On-Premise - installiert werden müssen.²¹ Die Software läuft in der Regel auf den Servern der Anbietenden, die sowohl für die Wartung als auch für Updates und technische Sicherheit zuständig sind.²² Gegen Zahlung einer meist periodischen Gebühr (zB monatlich oder jährlich) erhalten Nutzende das Recht, die Software im Rahmen des vertraglich vereinbarten Leistungsumfangs zu verwenden - sie erhalten also ein Recht auf Zugriff und Nutzung der Software

¹⁵ vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 5 ff.

¹⁶ Diese Arbeit behandelt ausschließlich die Beschaffung von SaaS Leistungen. Infrastructure as a Service und Platform as a Service werden nur zur Abgrenzung erläutert und im weiteren Verlauf nicht vertieft.

¹⁷ vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 7.

¹⁸ vgl. *Brunner*, Cloud Computing, in *Zankl (Hrsg)*, Rechtshandbuch der Digitalisierung (2021) Rz 4.5.

¹⁹ vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 6.

²⁰ vgl. *Brunner* in *Zankl* Rz 4.7.

²¹ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (724).

²² vgl. *Heydn*, MMR 2020, 435 (436).

über das Internet.²³

Neben der Art des Services ist das Bereitstellungsmodell für die sicherheits- und datenschutzrechtliche Bewertung von zentraler Bedeutung. Man unterscheidet hierbei vier Varianten:

Die „Private-Cloud“ wird für den exklusiven Gebrauch durch eine einzelne Organisation bereitgestellt. In der Private-Cloud beschränkt sich der Kreis der Nutzenden auf ein einziges Unternehmen oder eine einzige Behörde, da die Leistung bzw. die Cloud ausschließlich von diesem Unternehmen oder dieser Behörde genutzt wird.²⁴ Bei einer Private-Cloud handelt es sich also um einen Cloud-Dienst speziell für eine einzige Organisation bzw. ein einziges Unternehmen. Für den Einsatz von Private-Cloud Diensten sprechen vor allem Sicherheitsgründe, da die Kontrolle über die Daten bei den Nutzenden verbleiben. Darüber hinaus lassen sich diese Modelle gezielt an die individuellen Bedürfnisse der Nutzenden anpassen.²⁵ Zwar ermöglicht dieser Ansatz weitreichende Vorgaben hinsichtlich Leistungsort, Sicherheitsniveau und Systemintegrationen, er erweist sich jedoch im Vergleich als deutlich kostenintensiver als andere Bereitstellungsmodelle.

Die „Community-Cloud“ ist auf die exklusive Nutzung durch einen definierten Kreis von Organisationen mit homogenen Anforderungen zugeschnitten. Sie wird gezielt für Akteure bereitgestellt, die gemeinsame Anliegen verfolgen – wie etwa universitäre Netzwerke oder Forschungseinrichtungen – und ermöglicht eine geteilte Infrastruktur unter gleichzeitigem Ausschluss der allgemeinen Öffentlichkeit. Ein wesentlicher Vorteil liegt in der Möglichkeit, gemeinsame Standards – insbesondere bezüglich Sicherheit, Interoperabilität und Portabilität – für alle Teilnehmenden verbindlich zu definieren. Dieser Synergieeffekt setzt jedoch eine enge Abstimmung zwischen den beteiligten Organisationen voraus, um administrative Reibungsverluste zu vermeiden.²⁶

Die „Public-Cloud“ stellt Dienste über eine geteilte, hochstandardisierte und global skalierende Infrastruktur bereit. In der Public-Cloud ist der potenzielle Kreis der Nutzenden nicht begrenzt. Die Services werden am freien Markt angeboten und können deshalb von einer Vielzahl von Nutzenden gleichzeitig genutzt werden.²⁷ Public-Cloud-Lösungen zeichnen sich durch hohe Flexibilität aus, die insbesondere aus der dynamischen

²³ vgl. Schima, *ecolex* 2024, 197 (198).

²⁴ vgl. Claßen/Koch/Müller, *MMR* 2020, 723 (725).

²⁵ vgl. Claßen/Koch/Müller, *MMR* 2020, 723 (726).

²⁶ vgl. Brunner in Zankl *Rz* 4.11.

²⁷ vgl. Claßen/Koch/Müller, *MMR* 2020, 723 (726).

Skalierbarkeit von Services, Rechenleistung und Speicherkapazitäten resultiert. Zudem gewährleisten sie eine gesteigerte Verfügbarkeit bei gleichzeitig optimierter Kostenstruktur, was primär auf Skaleneffekten der Anbietenden beruht.²⁸ Der Einsatz von Public-Cloud-Modellen setzt jedoch präzise vertragliche Vereinbarungen voraus. Um die angestrebten Datenschutz-, Sicherheits- und Souveränitätsziele zu wahren, sind insbesondere klare Festlegungen zur Datenlokation, zu dezidierten Zugriffsregimen sowie zu Audit- und Reporting-Rechten erforderlich.²⁹

Die „Hybrid-Cloud“ kombiniert verschiedene Bereitstellungsmodelle miteinander. Dieser Ansatz ist besonders für differenzierte Schutzbedürfnisse prädestiniert: Während hochsensible Datenbestände On-Premise oder in einer EU-Private-Cloud verarbeitet werden, deren Standort sowie die rechtliche Verantwortung des bereitstellenden Unternehmens innerhalb der Europäischen Union liegen, lassen sich weniger kritische Workloads kosteneffizient in die Public-Cloud auslagern.³⁰

2.2. Abgrenzung: On-Premise-Modelle vs SaaS (CapEx vs OpEx, Verantwortungsteilung)

Aufbauend auf den in Kapitel 2.1 erläuterten technischen Grundlagen von SaaS, werden in diesem Kapitel die fundamentalen Unterschiede zum traditionellen On-Premise-Modell herausgearbeitet. Diese Abgrenzung ist für die Beantwortung der Forschungsfragen von zentraler Bedeutung, da die unterschiedliche Verantwortungsverteilung und Kostenstruktur die Kernursache für die Herausforderungen bei der Vergleichbarkeit und Transparenz im Vergabeverfahren sind.

Die Gegenüberstellung beider Modelle offenbart grundlegende Divergenzen, die sich maßgeblich auf die Gestaltung von Vergabeverfahren auswirken. Der wohl fundamentalste Unterschied manifestiert sich in der Verlagerung von Verantwortung und Risiko.³¹ Während bei klassischen On-Premise-Lösungen Nutzende bzw. auftraggebende Stellen die volle Kontrolle über die technische Infrastruktur behalten und damit auch die vollständige Verantwortung für deren Betrieb tragen, verlagert sich, abhängig vom gewählten Bereitstellungsmodell von SaaS diese Verantwortung mehr oder weniger auf die Anbietenden, was folglich zu einer signifikanten Verschiebung des Risikoprofils führt.³² Diese strukturelle Risikoverlagerung muss sich zwingend in der vertraglichen

²⁸ vgl. Brunner, in Zankl Rz 4.12.

²⁹ Heydn, MMR 2020, 435 (442); Hunzinger, Die neuen EVB-IT Cloud aus Anbietersicht: Ein Jahr Praxis, CR 2023, 349 (349 ff).

³⁰ vgl. Brunner, in Zankl Rz 4.13.

³¹ vgl. Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 5.

³² vgl. Heydn, MMR 2020, 435 (436).

Ausgestaltung, insbesondere in detaillierten „Service-Level-Agreements“ (SLAs), widerspiegeln, ein Aspekt, der in Kapitel 4.3 vertieft wird.³³

Eng damit verknüpft ist der Wandel der Kostenstruktur: Beim klassischen On-Premise-Modell erwerben Nutzende sämtliche notwendige Lizenzen häufig in einem Zug – etwa durch ein einmalig zu entrichtendes Entgelt, häufig in Form eines Kaufvertrags. Im Gegensatz dazu steht beim SaaS-Modell das kontinuierliche Nutzungsrecht in Form von virtuellen Zutrittsrechten in die Cloud im Vordergrund. Ökonomisch verschiebt sich beim SaaS-Modell daher der Schwerpunkt von „Capital Expenditures“ (CapEx), also einmaligen Investitions-/Kapitalkosten bei On-Premise-Lösungen, zu „Operational Expenditures“ (OpEx), also laufenden Betriebskosten, was eine reine Gegenüberstellung von Anschaffungspreisen im Vergabeverfahren unzulänglich macht.³⁴

Ein weiterer kritischer Differenzierungspunkt liegt in der physischen Standortfrage: Bei On-Premise-Lösungen kann die auftraggebende Stelle exakt bestimmen, wo die Daten gespeichert werden – beispielsweise in eigenen oder behördlich kontrollierten Rechenzentren. Im Gegensatz dazu erfolgt die Datenhaltung beim SaaS-Modell in der Regel durch die bereitstellenden Unternehmen oder in deren Cloud-Infrastruktur, die sich teilweise auch in Drittländern befinden kann. Insbesondere für öffentliche Stellen resultieren daraus komplexe Anforderungen an die Einhaltung der DSGVO-Vorgaben sowie nationaler Sicherheitsgesetze, vor allem hinsichtlich der Rechtmäßigkeit von Drittlandtransfers, die in Kapitel 3.3 als zentrale datenschutzrechtliche Herausforderung analysiert werden.³⁵

Schließlich führt die technische Architektur von Cloud-Lösungen zu einem Spannungsfeld zwischen Standardisierung und Individualisierung. Dem Multi-Tenancy-Prinzip folgend, basieren SaaS-Angebote auf einer tiefgreifenden technischen Standardisierung, die individuelle Anpassungen stark einschränkt. Dies kollidiert mit der gängigen Praxis öffentlicher Stellen, im Vergabeverfahren die Vertragsbedingungen einseitig festzulegen. Ohne eine sorgfältige Reflexion der eigenen Anforderungen und einen Abgleich mit den realisierbaren Standards der Branche besteht die Gefahr, dass die Marktgängigkeit der Ausschreibung beeinträchtigt wird und das Verfahren mangels geeigneter Angebote scheitert.³⁶

³³ vgl. *Möglich*, 80.2 Vertragsbedingungen der öffentlichen Hand EVB-IT, in *Taeger/Pohle* (Hrsg.), *Computerrechts-Handbuch* (40. EL März 2025) Rz 188 ff.

³⁴ vgl. *Heydn*, MMR 2020, 435 (435 ff).

³⁵ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726); vgl. auch *Schulz*, *Cloud Computing in der öffentlichen Verwaltung – Chancen – Risiken – Modelle*, MMR 2010, 75 (78).

³⁶ vgl. *Möglich* in *Taeger/Pohle* Rz 194 ff; siehe auch *Baier*, *Software-as-a-Service (SaaS) Verträge*:

2.3. Zivil- und vergaberechtliche Einordnung von SaaS-Verträgen

Die in Kapitel 2.1 und 0 dargestellten technischen und ökonomischen Besonderheiten von SaaS-Modellen werfen die Frage auf, wie diese Verträge rechtlich einzuordnen sind. Diese Einordnung ist für die Beantwortung der Forschungsfragen von zentraler Bedeutung, da sie bestimmt, welche gesetzlichen Regelungen anwendbar sind und welche Anforderungen an die Vertragsgestaltung im Vergabeverfahren zu stellen sind.³⁷ Während die zivilrechtliche Qualifikation die Rechte und Pflichten der Vertragsparteien definiert, determiniert die vergaberechtliche Einordnung die anzuwendenden Verfahrensregeln. Der Rechtsvergleich zwischen Österreich und Deutschland offenbart dabei unterschiedliche Lösungsansätze zur Bewältigung der SaaS-spezifischen Herausforderungen.

2.3.1. Zivilrechtliche Einordnung: Der SaaS-Vertrag als Mischvertrag

Bei der zivilrechtlichen Einordnung von SaaS-Verträgen lassen sich grundlegend zwei zentrale Aspekte identifizieren. Zum einen weist SaaS mietrechtliche Komponenten auf, da Nutzende für einen bestimmten Zeitraum die Möglichkeit erhalten, über das Internet auf eine Software zuzugreifen. Diese mietrechtliche Komponente ergibt sich aus der entgeltlichen Gebrauchsüberlassung der Software auf Zeit, geregelt in §§ 1090 ff Allgemeines Bürgerliches Gesetzbuch (ABGB) bzw §§ 535 ff Bürgerliches Gesetzbuch (BGB).³⁸

Zum anderen hat SaaS einen starken Dienstleistungscharakter, da die Anbietenden fortlaufend Leistungen wie Betrieb, Wartung und regelmäßige Updates erbringen. Für diese Leistungen sind die §§ 1151 ff ABGB bzw §§ 611 ff BGB einschlägig.³⁹

Werden darüber hinaus individuelle Anpassungen der Software geschuldet, können zudem werkvertragliche Elemente nach §§ 1165 ff ABGB bzw. §§ 631 ff BGB hinzutreten.⁴⁰

Nach überwiegender Ansicht in der Literatur handelt es sich um einen atypischen Mischvertrag mit überwiegend mietrechtlichen Elementen, da die

Einordnung und Möglichkeiten, SRD-Rechtsanwälte Blog, 09.04.2025, <https://www.srd-rechtsanwaelte.de/blog/saas-vertraege-einordnung-moeglichkeiten> (abgerufen am 27. 12. 2025).

³⁷ vgl. Tretzmüller, ZIIR 2019, 255 (255).

³⁸ vgl. Schima, ecolex 2024, 197 (198)

³⁹ vgl. Tretzmüller, Handbuch Softwarerecht¹ (2023) Rz 1053; siehe auch Tretzmüller, Wie sind SaaS-Verträge rechtlich einzuordnen? digital-recht.at (Blog Kanzlei Dr Tretzmüller) (2023), <https://www.digital-recht.at/blog/wie-sind-saas-vertraege-rechtlich-einzuordnen> (abgerufen am 27. 12. 2025).

⁴⁰ vgl. Heydn, MMR 2020, 435 (436); Müller, Zur vergaberechtlichen Einordnung von ASP-/Cloud-Leistungen, ZIIR 2014, 372 (374).

Gebrauchsüberlassung den Vertrag prägt.⁴¹ Dies hat zur Folge, dass Anbietende eine verschuldensunabhängige Haftung für Mängel trifft, wie sie in § 1096 ABGB bzw § 536a BGB normiert ist.⁴² Während das Mietrecht eine Instandhaltungspflicht vorsieht, schulden Anbietende nach Dienstvertragsrecht nur ein sorgfältiges Bemühen, jedoch keinen konkreten Erfolg.⁴³

2.3.2. Vergaberechtliche Einordnung: SaaS als Dienstleistungsauftrag

SaaS-Verträge sind vergaberechtlich als Dienstleistungsaufträge im Sinne der RL 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe⁴⁴ einzuordnen. Vergaberechtlich ausschlaggebend ist, dass nicht die Überlassung, also die Übergabe, einer Softwarekopie, sondern der Betrieb, die Bereitstellung sowie die kontinuierliche Wartung der digitalen Infrastruktur die spezifische Charakteristik des Vertragsverhältnisses prägen. Diese Unterscheidung ist nicht bloß akademischer Natur, sondern hat unmittelbare Auswirkungen auf die anzuwendenden Verfahrensregeln.⁴⁵

Während On-Premise-Beschaffungen typischerweise als Lieferauftrag (Softwarelizenz) gegebenenfalls in Kombination mit einem Dienstleistungsauftrag (Pflege, Wartung) zu qualifizieren sind, handelt es sich bei SaaS um einen reinen Dienstleistungsauftrag.⁴⁶ Es gelten daher die Verfahrensregeln für Dienstleistungsaufträge nach §§ 78 ff BVergG 2018 bzw §§ 121 ff GWB.⁴⁷ Dies hat insbesondere Auswirkungen auf die Leistungsbeschreibung, die Eignungsprüfung und die Zuschlagskriterien. Die funktionale statt konstruktiver Beschreibung wird zum Regelfall⁴⁸, ein Aspekt, der in Kapitel 4.3 vertieft wird, die technische Leistungsfähigkeit wird primär über Referenzen und Zertifizierungen nachgewiesen, und qualitative Aspekte wie SLAs, Sicherheit und Portabilität gewinnen gegenüber reinen Preisvergleichen an Bedeutung.⁴⁹

⁴¹ vgl Schima, *ecolex* 2024, 197 (198 f); aA etwa Tretzmüller, *ZfIR* 2019, 255 (256), der für eine differenziertere Anwendung der Kombinationstheorie plädiert.

⁴² vgl Heydn, *MMR* 2020, 435 (438); siehe auch Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 33.

⁴³ vgl Claßen/Müller/Koch, *MMR* 2020, 723 (728), Härtel, Software-as-a-Service-Vertrag, *ITMediaLaw Wissensbank*, 11. April 2025, <https://itmedialaw.com/wissensdatenbank/software-as-a-service-vertrag-saas-vertrag/> (abgerufen am 27. 12. 2026).

⁴⁴ Vergaberichtlinie 2014/24 ABI. L 2014/094, 65; RL (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (Digitale-Inhalte-Richtlinie), ABI L 2019/136, 1.

⁴⁵ vgl Heydn, *MMR* 2020, 435 (436).

⁴⁶ vgl Claßen/Koch/Müller, *MMR* 2020, 723 (723 ff); Heydn, *MMR* 2020, 435 (436).

⁴⁷ § 2 Z 2 Nr 7 BVergG 2018; § 2 Nr 3 GWB; vgl Bischof, *ITRB* 2023, 165 (166).

⁴⁸ Art 42 RL 2014/24/EU; § 104 Abs 2 BVergG 2018; § 31 VgV.

⁴⁹ Art 67 Abs 2 RL 2014/24/EU § 81 BVergG 2018; § 121 GWB; vgl Hunzinger, *CR* 2023, 349 (352); vgl Claßen/Koch/Müller, *MMR* 2020, 723 (727 f).

2.3.3. *Rechtsvergleich: Unterschiedliche Lösungsansätze in Österreich und Deutschland*

Obwohl die materiellen Beschaffungsgrundsätze durch harmonisierte EU-Vorgaben weitgehend identisch sind, weichen die praktischen Rahmenbedingungen für die SaaS-Vertragsgestaltung erheblich ab.⁵⁰ Deutschland verfügt seit dem 1. März 2022 über die „Ergänzenden Vertragsbedingungen für die Beschaffung von Cloudleistungen“ (EVB-IT Cloud)⁵¹, veröffentlicht durch das Bundesministerium des Innern. Dieses Vertragsmuster adressiert systematisch die zentralen Kernthemen: Leistungsgegenstand und Leistungsort, Datenschutz und IT-Sicherheit, Verfügbarkeit und Störungsmanagement, Migration, Portabilität und Exit-Management, Nutzungsrechte, sowie Vergütung, Mängelrechte und Haftung.⁵²

Eine Besonderheit ist die kontrollierte Öffnung für Allgemeine Geschäftsbedingungen (AGB) der Anbietenden über Anhang I bzw. Nr. 1.2.4. Diese bewusste Abweichung vom traditionellen Ausschluss von Anbietenden-AGB stellt einen Paradigmenwechsel dar, dessen Hintergründe und Konsequenzen für die Beschaffungspraxis in Kapitel 5.1 eingehend analysiert werden.

Diese Öffnung darf jedoch nicht als Blankoscheck verstanden werden, sondern wirft komplexe Abgrenzungs-, Prioritäts- und AGB-Kontrollfragen auf. In der Beschaffungspraxis wird die Vergleichbarkeit durch ein mehrstufiges System sichergestellt: Eine strikte Hierarchie der Vertragsdokumente sichert den Vorrang der Vorgaben der ausschreibenden Stelle. Klare Mindestanforderungen müssen definiert werden, deren Nichteinhaltung zum zwingenden Angebotsausschluss führt. Objektive Zuschlagskriterien werden vorab bekannt gemacht, wobei die AGB als Nachweis für die Erfüllung dieser Kriterien dienen können.⁵³

In Österreich fehlt ein mit den EVB-IT Cloud vergleichbares Standardvertragswerk für IT-Beschaffungen. Die existierenden ÖNORMEN⁵⁴ sind auf das klassische Bauwesen

⁵⁰ Art 10 Vergaberichtlinie; BVergG 2018 § 20; GWB § 97; Beschaffungsamt des Bundesministeriums des Innern Zentralstelle IT-Beschaffung (ZIB), Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-ufab-node.html>, 184 ff (abgerufen am 1. 1. 2026); vgl. Hunzinger, CR 2023 (349 ff); Heydn, MMR 2020 (435).

⁵¹ Ministerium für Digitales und Staatsmodernisierung, EVB-IT Cloud – Vertrag, https://www.digitale-verwaltung.de/SharedDocs/downloads/Webs/DV/DE/digitale-loesungen/it-einkauf/evb-it-bvb/basisvertraege/cloud/it-cloud-vertrag.docx?__blob=publicationFile&v=2 (abgerufen am 2. 1. 2026); vgl. Möglich, in Taeger/Pohle Rz 19; BTL Rechtsanwälte, RA Dr. Tobias Beltle, Blogbeitrag, 11. 7. 2022, <https://www.btl-recht.de/blog/evb-it-cloud-vertrag/> (abgerufen am 7. 3. 2026).

⁵² vgl. Möglich, in Taeger/Pohle Rz 161 ff.

⁵³ vgl. OLG Düsseldorf 1.6.2016, VII-Verg 6/16, Rn 122 f; vgl. Möglich, in Taeger/Pohle Rz 160.

⁵⁴ ÖNORMEN sind österreichische Normen („Österreichische Normen“), standardisiert vom Austrian Standards Institute (ASI); gegliedert in Bereiche wie Bauwesen, Maschinenbau, Dienstleistungen,

zugeschnitten und für die komplexen Anforderungen digitaler Dienstleistungen weitgehend ungeeignet.⁵⁵ Die daraus resultierenden Herausforderungen für die Vergabepraxis werden in Kapitel 5.2 näher analysiert.

Die Lösung für Österreich bietet jedoch das BVergG 2018 selbst durch das Instrument der funktionalen Leistungsbeschreibung nach § 104 Abs 2.⁵⁶ Eine funktionale Beschreibung muss die Leistung nicht in jedem technischen Detail vollständig spezifizieren; vielmehr ist sie so zu fassen, dass die Anforderungen als hinreichend genaue, zu lösende Aufgabenstellung definiert werden. Dies ermöglicht es den öffentlich auftraggebenden Stellen, den Fokus weg von starren technischen Vorgaben hin zu den angestrebten Leistungs- und Funktionszielen zu verschieben, was insbesondere der technologischen Dynamik von SaaS-Lösungen gerecht wird.⁵⁷

Im Ergebnis offenbart der Rechtsvergleich zwei fundamental unterschiedliche Lösungsstrategien, um die technologische Dynamik von SaaS-Leistungen in der Leistungsbeschreibung vergaberechtlich zu bewältigen.⁵⁸ Deutschland verfolgt mit den EVB-IT Cloud einen institutionalisierten, vertraglichen Lösungsansatz. Hierbei wird die Dynamik der Leistungserbringung bewusst in ein standardisiertes, hochkomplexes Vertragswerk verlagert. Dieses steuert notwendige Leistungsänderungen sowie technische Weiterentwicklungen durch eine kontrollierte Einbeziehung der AGB der anbietenden Unternehmen. Damit wird die Rechtssicherheit durch eine vorab definierte Vertragshierarchie gewährleistet, die den Spielraum für technologische Anpassungen innerhalb klarer Leitplanken zulässt.⁵⁹ Österreich hingegen begegnet dieser Herausforderung primär auf der Ebene der verfahrensrechtlichen Gestaltung. In Ermangelung eines vergleichbaren Standardwerks rückt die funktionale Leistungsbeschreibung in das Zentrum der Beschaffungsstrategie.⁶⁰ Dies verlagert die Verantwortung für die technologische Lösungsspezifikation stärker in den Wettbewerb und fordert von den ausschreibenden Stellen eine hohe Kompetenz bei der Definition präziser, aber technologieneutraler Funktionsziele.⁶¹

<https://www.usp.gv.at/themen/betrieb-und-umwelt/laufender-betrieb/weitere-informationen-laufender-betrieb/normen-und-standards.html> (abgerufen am 7. 3. 2026).

⁵⁵ vgl. Claßen/Koch/Müller, MMR 2020, 723 (725).

⁵⁶ § 104 Abs 2 BVergG 2018; vgl. Göllles in Göllles/Casati, BVergG 2018 § 104 Rz 32 ff.

⁵⁷ vgl. Göllles in Göllles/Casati, BVergG 2018 § 104 Rz 35; Diem in Göllles/Casati, BVergG 2018 § 106 Rz 38.

⁵⁸ vgl. Bischof/Intveen, Die neuen EVB-IT Cloud aus Anwendersicht, ITRB 2022, 157 (161 f); Hunzinger, CR 2023, 349 (351).

⁵⁹ vgl. Hunzinger, CR 2023, 349 (351); Möglich in Taeger/Pohle Rz 160.

⁶⁰ § 104 Abs 2 BVergG 2018; vgl. Göllles in Göllles/Casati, BVergG 2018 § 104 Rz 32 ff.

⁶¹ Diem in Göllles/Casati, BVergG 2018 § 106 Rz 29 ff.; Casati in Göllles/Casati, BVergG 2018 § 20 Rz 25

Beide Ansätze sollen eine nachvollziehbare und überprüfbare Grundlage für die Zuschlagsentscheidung gewährleisten, sodass der Zuschlag auf das tatsächlich wirtschaftlichste Angebot und nicht auf jenes mit der undurchsichtigsten Preisstruktur erfolgt.⁶²

2.4. Vergaberechtliche Grundsätze und ihre Bedeutung für SaaS-Beschaffungen

Aufbauend auf der zivil- und vergaberechtlichen Einordnung von SaaS-Verträgen in Kapitel 0 ist nun der normative Rahmen zu beleuchten, dem jede öffentliche Beschaffung unterliegt. Die in § 20 Abs 1 BVergG 2018 verankerten Grundsätze – Transparenz, Gleichbehandlung und Wettbewerb – gelten für alle Vergaben und entfalten bei der Beschaffung von SaaS-Leistungen eine besondere Sprengkraft. Sie bilden die Grundlage für die in Kapitel 3 zu analysierenden Herausforderungen und die in Kapitel 4 zu entwickelnden Lösungsansätze.

Der Transparenzgrundsatz verpflichtet die auftraggebende Stelle, sämtliche Etappen des Verfahrens für teilnehmende Unternehmen vorhersehbar zu gestalten. Dies manifestiert sich vor allem in einer strengen Dokumentations- und Begründungspflicht, um die Einhaltung der übrigen Grundsätze jederzeit objektiv überprüfen zu können.⁶³ Ein wesentlicher Aspekt der Transparenz ist zudem die Selbstbindung der auftraggebenden Stelle an die von ihr selbst aufgestellten Bedingungen der Vergabeunterlagen. Nachträgliche Änderungen der Ausschreibungsbedingungen oder die Stützung der Vergabeentscheidung auf Kriterien, die vorab nicht bekanntgemacht wurden, sind unzulässig.⁶⁴ Damit einher geht eine gewisse Formenstrenge, ohne die das Transparenzgebot nicht umsetzbar wäre.⁶⁵ Die Vergabeunterlagen müssen daher so formuliert sein, dass alle gebührend informierten und mit üblicher Sorgfalt handelnden Bietenden die genaue Bedeutung der Bedingungen sowie Modalitäten verstehen und in gleicher Weise auslegen können.⁶⁶ Andernfalls liegt ein Verstoß gegen das Transparenzgebot

f.

⁶² Art 91 Abs 1 BVergG 2018; § 127 Abs 1 GWB; vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad*, § 22 Rn 10 ff.

⁶³ § 20 Abs 1 BVergG 2018; § 31 Abs 6 VgV; ErwGr 84 der RL 2014/24/EU ABI L 2014/94, 65; vgl. OLG Düsseldorf 27. 6. 2012, VII-Verg 7/12, Rn 25.

⁶⁴ §§ 53, 96 ff BVergG 2018; EuGH C-278/14, *Enterprise Focused Solutions*, ECLI:EU:C:2015:228, Rn 27; BGH 18. 1. 2000, X ZR 101/97; OLG Brandenburg 28. 3. 2017, 6 Verg 5/16.

⁶⁵ OLG München 6. 7. 2000, U (K) 5047/99; OLG Düsseldorf 8. 5. 2000, Verg 6/00; vgl. *Schneevogl* in *Summa/Schneevogl* (Hrsg), juris PraxisKommentar Vergaberecht⁷ § 97 GWB Rz 52 (Stand 21.05.2025, juris.de).

⁶⁶ VwGH 1. 2. 2017, Ro 2016/04/0054; VwGH 1. 7. 2010, 2006/04/0139; BGH 10. 6. 2008, X ZR 78/07, Rn 17; OLG Celle 12. 10. 2021, 13 Verg 7/21, Rn 68; OLG Düsseldorf 13. 12. 2017, VII-Verg 19/17, Rn 69.

vor, wobei Unklarheiten in den Vergabeunterlagen stets zulasten der auftraggebenden Stelle gehen.⁶⁷

Eng damit verknüpft ist der Gleichbehandlungsgrundsatz, der besagt, dass alle Anbietenden die gleichen Chancen haben müssen, sich um einen öffentlichen Auftrag zu bemühen. Während der Transparenzgrundsatz die Vorhersehbarkeit sichert, garantiert die Gleichbehandlung die objektive Neutralität der auftraggebenden Stelle. Dies umfasst sowohl die formale Ebene – etwa durch einen identischen Informationsstand für alle – als auch die materielle Ebene, die eine vorweggenommene Einschränkung auf spezifische Unternehmen oder Technologien untersagt.⁶⁸ In der praktischen Umsetzung bedeutet dies, dass die einmal aufgestellten Kriterien während des gesamten Verfahrens vollkommen diskriminierungsfrei angewendet werden müssen.⁶⁹

Das Wettbewerbsprinzip zielt wiederum darauf ab, durch eine effektive Konkurrenz auf der Seite der Anbietenden die Effizienz öffentlicher Beschaffungsvorgänge sicherzustellen.⁷⁰ Die öffentliche Hand hat in einem offenen Wettbewerb jenes Angebot zu ermitteln, das das beste Preis-Leistungs-Verhältnis aufweist.⁷¹ Ob und inwieweit im Einzelfall spezifische Systeme oder Produktvorgaben gefordert werden dürfen, unterliegt einer strengen Prüfung. Derartige Festlegungen müssen unter einer wirtschaftlichen Betrachtungsweise der tatsächlichen Umstände sachlich gerechtfertigt, umfassend dokumentiert und im Streitfall nachgewiesen werden.⁷²

Als prozedurales Herzstück zur Umsetzung dieser Grundsätze fungiert die Leistungsbeschreibung. Gemäß § 103 BVergG 2018 verbleibt der auftraggebenden Stelle die Wahl zwischen einer konstruktiven Leistungsbeschreibung mittels technischer Spezifikationen und einer funktionalen Beschreibung über Leistungs- und Funktionsziele.⁷³ Insbesondere bei dynamischen IT-Leistungen wie SaaS-Modellen legt diese Systematik einen Schwerpunkt auf funktionale Leistungsbeschreibungen nahe. Die materiellen Anforderungen ergeben sich aus § 104 BVergG 2018: Die Leistung muss so eindeutig

⁶⁷ EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rz 87; VwGH 1. 2. 2017, Ro 2016/04/005; OLG Düsseldorf 8.3.2017, VII-Verg 39/16 Rn 74; KG Berlin 4. 6. 2019, Verg 8/18.

⁶⁸ EuGH C-496/99 P, *Kommission/CAS Succhi di Frutta*, ECLI:EU:C:2004:236, Rz 108; EuGH C-45/87, *Kommission/Irland*, ECLI:EU:C:1988:435, Rn 16 ff Rz 37; § 97 Abs 3 BVergG 2018; vgl *Gölles/Casati*, BVergG 2018 § 97 Rz 15 ff; vgl auch *Claßen/Koch/Müller*, MMR 2020, 723 (728).

⁶⁹ OLG Düsseldorf Verg 8. 5. 2000, 6/00.

⁷⁰ § 20 BVergG 2018; § 97 Abs 1 GWB.

⁷¹ vgl *Moick/Gföhler*, BVergG 2018^{1.01} § 91 E146/1 ff (Stand 1.3.2021, rdb.at).

⁷² vgl *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 43; vgl auch ErläutRV 69 BlgNR 26. GP 52 f.

⁷³ vgl *Gölles* in *Gölles/Casati*, BVergG 2018 § 105 Rz 13 ff; *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 1, 45.

und erschöpfend definiert sein, dass sämtliche Anbietende die Vorgaben einheitlich interpretieren können und infolgedessen die Vergleichbarkeit der Angebote gewährleistet ist.⁷⁴ Dieses weite Ermessen findet seine Grenze jedoch im Gebot der Produktneutralität in § 106 BVergG 2018. Eine Einengung des Wettbewerbs auf spezifische Erzeugnisse ist demnach nur in eng geführten, sachlich begründeten Ausnahmefällen zulässig und muss zwingend durch den Zusatz „oder gleichwertig“ für den Wettbewerb geöffnet werden.⁷⁵

Schließlich markiert die Prüfung der Eignung der Teilnehmenden ein entscheidendes Stadium, in dem die auftraggebende Stelle verifiziert, ob das anbietende Unternehmen über die notwendige Fachkunde, Leistungsfähigkeit sowie Zuverlässigkeit verfügt.⁷⁶ Im spezifischen Kontext von SaaS-Lösungen gewinnen insbesondere drei Aspekte an Relevanz: Erstens die berufliche Zuverlässigkeit, bei der die Integrität hinsichtlich des Datenschutzrechts von eminenter Bedeutung ist.⁷⁷ Zweitens die technische Leistungsfähigkeit, die regelmäßig durch Referenzprojekte oder anerkannte Zertifizierungen beispielsweise zur Informationssicherheit (zB ISO/IEC 27001) nachgewiesen wird.⁷⁸ Drittens die wirtschaftliche und finanzielle Leistungsfähigkeit, um die kontinuierliche Bereitstellung des Dienstes über die gesamte Vertragslaufzeit abzusichern.⁷⁹ Sämtliche Eignungskriterien müssen bereits im Vorfeld klar, präzise und diskriminierungsfrei in den Vergabeunterlagen bekanntgemacht werden, um den Grundsätzen der Transparenz und Gleichbehandlung vollumfänglich zu entsprechen.⁸⁰

Abschließend verdeutlicht eine tabellarische Gegenüberstellung der wesentlichen Unterschiede den Paradigmenwechsel von On-Premise zu SaaS und unterstreicht die vergaberechtlichen Implikationen für Transparenz und Vergleichbarkeit:

⁷⁴ vgl. Göllles in Göllles/Casati, BVergG 2018 § 105 Rz 13, 21; auch Schrotz/Zdanowiecki, CR 2015, 485 (486 f.).

⁷⁵ vgl. EuGH C-413/17, *Roche Lietuva*, ECLI:EU:C:2018:865, Rz 35 ff; und § 106 Abs 6 BVergG 2018; § 31 Abs 6 VgV; vgl. OLG Düsseldorf 27. 6. 2012, VII-Verg 7/12, Rz 25; vgl. auch Casati in Göllles/Casati, BVergG 2018 § 106 Rz 6 ff; EuGH C-496/99 P, *Kommission/CAS Succhi di Frutta*, ECLI:EU:C:2004:236, Rz 111; EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rz 61, 109.

⁷⁶ §§ 122 ff. GWB; §§ 42 ff. VgV; §§ 78 ff. BVergG 2018.

⁷⁷ § 83 Abs 1 BVergG 2018; § 124 Abs 1 Z 3 GWB.

⁷⁸ § 82 ff. BVergG 2018; § 46 Abs 3 VgV; vgl. *Bischof/Intveen*, ITRB 2022, 157 (159 f.).

⁷⁹ Für Österreich: § 84 BVergG 2018; für Deutschland: § 122 Abs 2 Satz 2 Nr 2 GWB.

⁸⁰ § 20 BVergG 2018; § 97 GWB; vgl. EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rz 43.

Kriterium	On-Premise-Modell	Software as a Service (SaaS)
Beschaffungsgegenstand	Erwerb einer Lizenz (dauerhaft oder befristet) zur Installation und Nutzung einer Softwarekopie. ⁸¹	Bezug einer Dienstleistung, die das Recht zum Zugriff und zur Nutzung der remote betriebenen Softwarefunktionalität auf Zeit umfasst. ⁸²
Betrieb & Verantwortung	Kunde ist für Infrastruktur, Installation, Wartung, Updates und Sicherheit verantwortlich. Volle Kontrolle, aber auch volle Verantwortung. ⁸³	Anbieter:in ist für den gesamten technischen Betrieb, Wartung, Updates und Sicherheit der Anwendung verantwortlich. Verantwortung und Risiko werden verlagert. ⁸⁴
Kostenstruktur	Hohe Anfangsinvestitionen für Lizenzen und Hardware (CapEx). ⁸⁵	Laufende, periodische Gebühren (OpEx). Geringere Anfangsinvestitionen. ⁸⁶
Physischer Standort	Datenhaltung in eigenen oder kontrollierten Rechenzentren. Der Standort ist klar bestimmbar. ⁸⁷	Datenhaltung in der Cloud-Infrastruktur des:der Anbieter:in, die global verteilt sein kann. Der Ort der Verarbeitung ist für die Nutzerin oder den Nutzer oft nicht

⁸¹ vgl. Förster, IT-Vertragsrecht: Teil 4 – Miete und Kauf von Standardsoftware, MMR 2024, 760 (762).

⁸² vgl. Müller, ZIIR 2014, 373 (373).

⁸³ vgl. Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 13.

⁸⁴ vgl. Heydn, MMR 2020, 435 (436).

⁸⁵ vgl. Claßen/Koch/Müller, MMR 2020, 723 (727).

⁸⁶ vgl. Claßen/Koch/Müller, MMR 2020, 723 (727).

⁸⁷ vgl. Schulz, MMR 2010, 75 (76).

		lokalisierbar. ⁸⁸
Vergaberechtliche Einordnung	Typischerweise Lieferauftrag (Softwarelizenz), ggf. in Kombination mit einem Dienstleistungsauftrag (Pflege). ⁸⁹	Typischerweise reiner Dienstleistungsauftrag. ⁹⁰

Abb 1: Wesensmerkmale SaaS vs. On-Premise – tabellarische Gegenüberstellung

Diese Gegenüberstellung verdeutlicht, dass der Paradigmenwechsel vom Besitz der Software im On-Premise-Modell zur Nutzung der Software als SaaS-Modell eine grundlegend andere vertragliche - und somit auch vergaberechtliche - Behandlung erfordert.⁹¹

3. Welche Herausforderungen ergeben sich?

Die in Kapitel 2 dargelegten Grundlagen haben gezeigt, dass SaaS-Verträge sowohl zivilrechtlich als auch vergaberechtlich einer besonderen Einordnung erfordern und dass die vergaberechtlichen Grundsätze der Transparenz, Gleichbehandlung und des Wettbewerbs den normativen Rahmen für jede öffentliche Beschaffung bilden. Aufbauend auf diesen Grundlagen widmet sich das folgende Kapitel den spezifischen Herausforderungen bei der Beschaffung von SaaS-Diensten für öffentliche Vergabestellen im Hinblick auf Vergleichbarkeit und Transparenz.

Die Beschaffung von SaaS-Leistungen stellt die öffentliche Hand vor drei zentrale Herausforderungen, die sich unmittelbar aus den in Kapitel 0 dargestellten strukturellen Unterschieden zu On-Premise-Modellen ergeben: Erstens erschwert die Heterogenität der Preismodelle die objektive Vergleichbarkeit der Angebote (siehe dazu Kapitel 3.1). Zweitens birgt die technische Architektur von Cloud-Lösungen das Risiko eines „Vendor-Lock-in“, also die technologische und wirtschaftliche Abhängigkeit von der einmal gewählten Vertragspartei, der die langfristige Handlungsfähigkeit der öffentlichen Hand gefährdet (siehe Kapitel 3.2). Drittens werfen Drittlandtransfers personenbezogener Daten komplexe datenschutzrechtliche Fragen auf, die sich unmittelbar auf die

⁸⁸ vgl. Claßen/Koch/Müller, MMR 2020, 723 (727).

⁸⁹ vgl. Claßen/Koch/Müller, MMR 2020, 723 (725).

⁹⁰ OLG Düsseldorf 1. 8. 2012, VII-Verg 10/12.

⁹¹ vgl. Schima, ecolex 2024, 197 (198).

Zulässigkeit bestimmter SaaS-Angebote auswirken (siehe Kapitel 3.3).

3.1. Vergleichbarkeitsproblem: Heterogene Preismodelle und dynamische Leistungen

Die Abkehr vom einmaligen Lizenzkauf hin zu Abonnement-Modellen hat eine erhebliche Varianz an Vergütungsstrukturen hervorgebracht. Diese Heterogenität stellt die öffentlich auftraggebenden Stellen bei der Ermittlung des geschätzten Auftragswerts und der Vergleichbarkeit der Angebote vor komplexe juristische und kalkulatorische Herausforderungen.⁹² Dogmatisch lassen sich drei Hauptkategorien unterscheiden:

Nutzerzentrierte Vergütung weist die stärkste strukturelle Nähe traditionellen Softwarelizenzierungsmetriken auf, da sie die Vergütung an die Anzahl der berechtigten Personen knüpft.⁹³ Die Vergütung bemisst sich entweder nach der Anzahl personalisierter Zugänge oder der maximalen Anzahl simultan aktiver Zugriffe. Während dies eine hohe Planungssicherheit bietet und vergaberechtlich aufgrund der eindeutigen Fixierbarkeit im Leistungsverzeichnis unproblematisch ist⁹⁴, besteht haushaltsrechtlich das Risiko für ungenutzte Kapazitäten bezahlen zu müssen, was dem Gebot der Wirtschaftlichkeit widersprechen kann.⁹⁵

Funktionszentrierte Vergütung erfolgt anhand der Freischaltung spezifischer Module oder Funktionspakete, die häufig in Form von Editionen angeboten werden.⁹⁶ Dieses Modell verlagert das wirtschaftliche Risiko maßgeblich in die Phase der Leistungsbeschreibung: Ermangelt es an einer exakten Differenzierung zwischen zwingenden Mindestanforderungen und bloßen optionalen Zusatzfunktionalitäten, besteht die Gefahr, dass im Wettbewerb funktional reduzierte Basis-Versionen offeriert werden, um einen künstlich niedrigen Angebotspreis zu erzielen. Notwendige Erweiterungen müssten in der Folge kostenpflichtig nachlizenziiert werden, was nicht nur das Nachtragsmanagement belastet, sondern auch die Integrität des ursprünglichen Wettbewerbsergebnisses gefährdet.⁹⁷

⁹² vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10.

⁹³ vgl. *García-Fernández/Parejo/Ruiz-Cortés*, *Pricing4SaaS*, arXiv:2404.00311v1 (2024), 6; *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rz 5 ff, 32 ff.

⁹⁴ Zur Bestimmtheit der Mengenangaben im Leistungsverzeichnis vgl. § 105 Abs 2 BVergG 2018; vgl. auch *Gölles* in *Gölles/Casati*, BVergG 2018 § 105 Rz 57 ff.

⁹⁵ vgl. *Möglich* in *Taeger/Pohle* Rn 7 f; ergänzend *Strittmatter*, in *Auer-Reinsdorff/Conrad* § 22 Rn 72 ff.

⁹⁶ vgl. *García-Fernández/Parejo/Ruiz-Cortés*, *Pricing4SaaS*, arXiv:2404.00311v1 (2024), 6; vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10.

⁹⁷ Zur Problematik nachträglicher Vertragsänderungen vgl. EuGH C-454/06, *Presstext*, ECLI:EU:C:2008:351; OLG Düsseldorf 28. 7. 2011, VII-Verg 20/11, Rn 110 ff; 104 Abs 2 BVergG 2018; *Gölles* in *Gölles/Casati*, BVergG 2018 § 104 Rz 32 ff.

Volumenzentrierte Vergütung ermittelt die Kosten dynamisch anhand technischer Verbrauchsparameter – etwa der Anzahl an Transaktionen, dem belegten Speicherplatz, der beanspruchten Rechenleistung oder dem Datendurchsatz. Während dieses Modell eine hohe Allokationseffizienz verspricht, erweist es sich vergaberechtlich als am anspruchsvollsten. Es kollidiert potenziell mit dem Gebot der Bestimmtheit der Leistung, wenn die verbrauchsrelevanten Parameter und Nutzungsszenarien nicht hinreichend konkret festgelegt werden, weil der exakte Endpreis dann bei Vertragsschluss nicht einmal prognostisch zuverlässig eingegrenzt werden kann.⁹⁸ Für die Budgetierung stellt dies ein erhebliches Risiko dar.⁹⁹ Zudem erschwert es die Prüfung ungewöhnlich niedriger Angebote, da niedrige Einheitspreise bei hohem Volumen zu exorbitanten Gesamtkosten führen können.¹⁰⁰

Die zuvor analysierten Vergütungsstrukturen münden allesamt in wiederkehrende Abonnement-Modelle. Diese führen zwangsläufig dazu, dass sich die Gesamtkosten eines Angebots erst über die Vertragslaufzeit zuverlässig bestimmen lassen. Unterschiede in der Ausgestaltung von Preisstaffelungen und Rabattmechanismen können bei identischer Nutzung zu erheblichen Abweichungen in den Lebenszykluskosten führen. Ohne eine einheitliche, von der öffentlich auftraggebenden Stelle vorgegebene Kalkulationsgrundlage wird die vergaberechtlich gebotene Vergleichbarkeit der Angebote verunmöglicht.¹⁰¹

In der Beschaffungspraxis agieren Cloud-Leistungen oft als hochgradig standardisierte Produkte. Neben der funktionalen Leistungsbeschreibung bildet das Bezahlmodell die zentrale Stellschraube des Vertragswerks.¹⁰² Die oft undurchsichtige Struktur von Skalierungs- und Volumenrabatten in Preislisten oder AGB unterstreicht die Heterogenität der anbietenden Unternehmen. Dies begründet die Notwendigkeit, sämtliche

⁹⁸ Zur Bestimmtheit der Leistung bei funktionaler Leistungsbeschreibung vgl § 104 Abs 2 BVergG 2018; *Gölles* in *Gölles/Casati*, BVergG 2018 § 104 Rz 32 ff.

⁹⁹ vgl CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/web-site_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Hand-book-v2-FEB-2022_de.pdf, Abschnitt 3.2 (abgerufen am 21. 1. 2026).

¹⁰⁰ Zur Prüfung ungewöhnlich niedriger Angebote vgl § 137 BVergG 2018; § 60 VgV; BGH 31. 1. 2017, X ZB 10/16.

¹⁰¹ vgl Art 67 Abs 2 lit b, Art 68 RL 2014/24/EU; § 92 Abs 1 i.V.m. § 2 Z 23 BVergG 2018; vgl auch *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff (Standardisierung von Cloud-Geschäftsmodellen, „kopflastige“ Vertragsstruktur, Bezahlmodell als zentraler Vertragsbestandteil); *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f) zur Heterogenität der Anbieterbedingungen und zur Notwendigkeit vorab festgelegter Bewertungsmaßstäbe zur Sicherung der Vergleichbarkeit; *Claßen/Koch/Müller*, MMR 2020, 723 (724 f) zur Einordnung von Cloud-Leistungen als Dauerschuldverhältnisse und zu den Risiken heterogener Vertrags- und Preismodelle.

¹⁰² *Strittmatter* in *Auer-Reinsdorff/Conrad*, § 22 Rn 10–15, 12 f. (Standardisierung von Cloud-Vertragsbedingungen, „kopflastige“ Struktur und Fokussierung auf Leistungsbeschreibung und Bezahlmodell).

Kostenkomponenten im Rahmen einer szenariobasierten Lebenszykluskostenbetrachtung transparent zu machen.¹⁰³

Vergaberechtlich wird dadurch untermauert, dass eine bloße Abfrage von Basispreisen unzureichend ist, sondern eine Überführung in vergleichbare Nutzungsszenarien zwingend geboten ist. Ohne eine vorab normierte Erfassung aller relevanten Faktoren in den Preisblättern wäre das Transparenz- und Gleichbehandlungsgebot gefährdet.¹⁰⁴ Die Koexistenz diverser Modelle in einem einzigen Vergabeverfahren führt andernfalls zu einer faktischen Unvergleichbarkeit der Angebote: Während ein Unternehmen ein günstiges Basis-Abonnement mit hohen variablen Transaktionskosten offeriert, könnten andere Wettbewerbsteilnehmende Pauschalen anbieten, die sämtliche Volumina inkludieren.¹⁰⁵ Um eine Wettbewerbsverzerrung zu vermeiden, muss die gewählte Umrechnungsformel gewährleisten, dass der relative Preisabstand zwischen den Angeboten angemessen abgebildet wird.¹⁰⁶

Neben der Heterogenität der Preismodelle erschwert auch die dynamische Natur von SaaS-Leistungen die Vergleichbarkeit. Anders als bei klassischen IT-Beschaffungen, bei denen der Leistungsgegenstand nach Vertragsschluss weitgehend statisch bleibt, unterliegen Cloud-Dienste einem kontinuierlichen Wandel: Funktionserweiterungen, Sicherheitsupdates, Änderungen der Benutzeroberfläche oder Anpassungen an neue regulatorische Anforderungen erfolgen laufend. Diese Dynamik wirft die Frage auf, wie die öffentlich auftraggebende Stelle sicherstellen kann, dass die bei Vertragsschluss zugesicherten Leistungsmerkmale über die gesamte Vertragslaufzeit erhalten bleiben, ohne dass die technologische Weiterentwicklung des Dienstes behindert wird.¹⁰⁷

Vergaberechtlich manifestiert sich diese Problematik in der Spannung zwischen der Selbstbindung der auftraggebenden Stelle an die Vergabeunterlagen und der Notwendigkeit, Anpassungen an veränderte technische oder rechtliche Rahmenbedingungen

¹⁰³ Claßen/Koch/Müller, MMR 2020, 723 (724 f); Schrotz/Zdanowiecki, CR 2015, 485 (486 f).

¹⁰⁴ vgl Art 67 Abs 2 lit. b RL 2014/24/EU; § 92 i.V.m. § 2 Z 23 BVergG 2018; zur Erforderlichkeit vorher bekannt gemachter Bewertungsmaßstäbe und zur Vergleichbarkeit der Angebote Schrotz/Zdanowiecki, CR 2015, 485 (486 f); CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 376 ff (abgerufen am 21. 1. 2026).

¹⁰⁵ zur Notwendigkeit der TCO-Betrachtung zur Herstellung von Vergleichbarkeit vgl CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 39 (abgerufen am 21. 1. 2026).

¹⁰⁶ vgl Hunzinger, CR 2023, 349 (351 f).

¹⁰⁷ vgl Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 10 ff.

zu ermöglichen.¹⁰⁸ Während nachträgliche Änderungen der Spielregeln grundsätzlich unzulässig sind, muss die Leistungsbeschreibung gleichzeitig so flexibel gestaltet sein, dass sie die kontinuierliche Weiterentwicklung des SaaS-Dienstes nicht ausschließt.¹⁰⁹ Dieser Zielkonflikt lässt sich nur durch eine präzise Abgrenzung zwischen zwingenden Mindestanforderungen und optionalen Zusatzfunktionen sowie durch klare Regelungen zu Updates und Upgrades auflösen.¹¹⁰

3.2. Abhängigkeitsproblem: Vendor-Lock-in durch proprietäre Strukturen

Neben der Vergleichbarkeit der Preismodelle stellt die strukturelle Abhängigkeit von einem einmal gewählten SaaS-Anbietenden eine zentrale Herausforderung für öffentliche Vergabestellen dar.¹¹¹ Da Cloud-Verträge dogmatisch als Dauerschuldverhältnisse zu qualifizieren sind, entsteht durch die Speicherung und Verarbeitung von Daten in der Sphäre der anbietenden Unternehmen eine strukturelle Abhängigkeit, die sich am Vertragsende als faktischer Vendor-Lock-in manifestieren kann.¹¹²

Diese Abhängigkeit wird kritisch, wenn technische Hürden oder sehr hohe Migrationskosten einen Wechsel der anbietenden Seite wirtschaftlich unzumutbar machen oder faktisch verunmöglichen.¹¹³ Die Ursachen für einen solchen Lock-in sind vielfältig: Proprietäre Datenformate, die nur mit der ursprünglich eingesetzten Software lesbar sind, führen zu erheblichem Migrationsaufwand.¹¹⁴ Fehlende oder unzureichend dokumentierte Schnittstellen erschweren die Integration in Folgesysteme. Vertragliche Restriktionen können die Datenherausgabe an enorm hohe Kosten oder langwierige Prozesse knüpfen. Schließlich können auch faktische Abhängigkeiten entstehen, wenn die öffentliche Stelle über die Vertragslaufzeit hinweg Prozesse und Arbeitsabläufe so stark an die spezifische Lösung angepasst hat, dass ein Wechsel organisatorisch kaum mehr bewältigbar erscheint.¹¹⁵

Vergaberechtlich ist diese Problematik von besonderer Brisanz, da sie die Integrität

¹⁰⁸ BGH 18. 1. 2000, X ZR 101/97; OLG Brandenburg 28. 3. 2017 6 Verg 5/16.

¹⁰⁹ vgl. *Strittmatter in Auer-Reinsdorff/Conrad* § 22 Rn 10 ff.

¹¹⁰ Zur Problematik nachträglicher Vertragsänderungen vgl. EuGH C-454/06, *Presstext*, ECLI:EU:C:2008:351; OLG Düsseldorf 28. 7. 2011, VII-Verg 20/11, Rn 110 ff.; 104 Abs 2 BVergG 2018; *Gölles in Gölles/Casati*, BVergG 2018 § 104 Rz 32 ff.

¹¹¹ vgl. *Tretzmüller*, ZIIR 2019, 255 (256 f.); vgl. *Schima*, *ecolex* 2024, 197 (199 f.).

¹¹² vgl. *Möglich in Taeger/Pohle* Rz 194.

¹¹³ vgl. *Tretzmüller*, ZIIR 2019, 255 (256 f.); vgl. *Hunzinger*, CR 2023, 349 (351).

¹¹⁴ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (724); *Strittmatter in Auer-Reinsdorff/Conrad* § 22 Rn 10 ff.; *Schrotz/Zdanowiecki*, CR 2015, 485 (486 ff.); *Möglich in Taeger/Pohle* Rz 194 ff.

¹¹⁵ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726).

künftiger Vergabeverfahren gefährdet.¹¹⁶ Wenn die öffentlich auftraggebende Stelle aufgrund technischer oder wirtschaftlicher Zwänge faktisch gezwungen ist, den bestehenden Vertrag mit demselben Unternehmen zu verlängern, wird der Wettbewerb bei der Neuausschreibung zur *Farce*.¹¹⁷ Die in Kapitel 2.4 dargelegten Grundsätze der Gleichbehandlung und des Wettbewerbs laufen ins Leere, wenn andere Anbietende zwar formal teilnehmen können, aber aufgrund der bestehenden Abhängigkeiten keine realistische Chance auf den Zuschlag haben.¹¹⁸

Anknüpfend an diese operativen Anforderungen wird deutlich, dass die ökonomische Vergleichbarkeit von SaaS-Angeboten maßgeblich durch die Spezifikation von Vertragslaufzeiten, Kündigungsmodalitäten und den damit verbundenen Exit-Kosten determiniert wird. Werden diese Parameter in den Vergabeunterlagen nicht eindeutig vorgegeben, eröffnet dies dem Kreis der Teilnehmenden die Möglichkeit zu strategischen Mischkalkulationen: Angebote mit niedrigen laufenden Entgelten, aber prohibitiv hohen, versteckten Exit-Kosten erscheinen im reinen Preisvergleich günstig, unterlaufen jedoch das Wirtschaftlichkeitsgebot über den gesamten Lebenszyklus.¹¹⁹

Aus dieser ökonomischen Problematik resultiert vergaberechtlich die zwingende Pflicht zu einer lebenszyklusorientierten Bewertungsmethodik. Der unionsrechtliche Transparenzmaßstab verlangt zwingend, dass aus den Vergabeunterlagen klar hervorgeht, welche Kostenbestandteile in die Wertung einfließen und wie diese gewichtet werden.¹²⁰ Unklare Bewertungslogiken, die keine verlässliche Prognose der Gesamtkosten erlauben, sind unzulässig und angreifbar.

Die Vermeidung von Vendor-Lock-in erweist sich damit als zwingende Prämisse für die Rechtmäßigkeit des gesamten Vergabeverfahrens.¹²¹ Welche konkreten Anforderungen an Reversibilität und Portabilität zu stellen sind und wie diese in die Wirtschaftlichkeitsbewertung einzubeziehen sind, wird in Kapitel 4.4 im Detail entwickelt.

¹¹⁶ vgl. *Tretzmüller*, ZIIR 2019, 255 (256 f.).

¹¹⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726); *Heydn*, MMR 2020, 435 (438); *Hoeren/Pinelli*, IT-Vertragsrecht (2024) Rn 376 ff.

¹¹⁸ § 20 Abs 1, § 106 Abs 1 BVergG 2018; EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 62, 109; *Gölles* in *Gölles/Casati*, BVergG 2018 § 104 Rz 35.

¹¹⁹ vgl. *Hunzinger*, CR 2023, 349 (350); *Bischof/Intveen*, ITRB 2022, 157 (160).

¹²⁰ EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 87 f.

¹²¹ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (wonach es der öffentlichen Vergabestelle bei rechtswidriger Datenverarbeitung an der Rechtsgrundlage fehlt); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 903.

3.3. Datenschutzproblem: Drittstaatentransfers und die "Schrems II"-Judikatur

Neben den Herausforderungen der Vergleichbarkeit und des Vendor-Lock-in stellt die datenschutzrechtliche Zulässigkeit von SaaS-Beschaffungen eine weitere zentrale Hürde dar. Während die beiden zuvor analysierten Problemfelder primär vergaberechtlicher Natur sind, handelt es sich hierbei um eine materielle Rechtmäßigkeitsvoraussetzung: Eine SaaS-Lösung, die gegen zwingende datenschutzrechtliche Vorgaben verstößt, kann nicht Gegenstand eines rechtmäßigen Zuschlags sein.¹²²

Die Einhaltung des Datenschutzrechts stellt für öffentlich auftraggebende Stellen keine bloße Option, sondern eine zwingende Rechtmäßigkeitsvoraussetzung des gesamten Beschaffungsvorgangs dar.¹²³ Gemäß den vergaberechtlichen Grundsätzen sind Verfahren unter strikter Beachtung der unionsrechtlichen Vorgaben durchzuführen, wozu im digitalen Raum untrennbar die Prinzipien der Datenschutz-Grundverordnung¹²⁴ (DSGVO) zählen.¹²⁵ Insbesondere die in Art 5 Abs 1 lit f DSGVO normierten Grundsätze der Integrität und Vertraulichkeit bilden eine materielle Schranke für die vergaberechtliche Beschaffungsfreiheit. Unabhängig von der Wahl zwischen einem On-Premise-Modell und einer Cloud-Lösung muss die Leistungsbeschreibung so gestaltet sein, dass der Schutz personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen über den gesamten Lebenszyklus der Verarbeitung sichergestellt bleibt.¹²⁶ Angebote, die diese zwingenden Vorgaben verfehlen, leiden an einem unbehebbar inhaltlichen Mangel.¹²⁷ Da ein rechtskonformer Zuschlag auf eine rechtswidrige Leistung rechtlich unmöglich ist, sind solche Angebote zwingend auszuscheiden.¹²⁸

¹²² vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726).

¹²³ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726); zur Abgrenzung zw Verantwortlicher und Auftragsverarbeiter vgl. auch *Tretzmüller*, Wann muss ein Auftragsverarbeitervertrag nach Art 28 DSGVO abgeschlossen werden? *Dako* 2019/1, 7.

¹²⁴ VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, *ABl L* 2016/119, 1 (Datenschutz-Grundverordnung, DSGVO).

¹²⁵ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726 f); siehe auch Art 28 Abs 3 DSGVO.

¹²⁶ vgl. Art 5 Abs 1 lit f und Art 32 Abs 1 DSGVO; zur Notwendigkeit der Implementierung von Sicherheitsstandards (wie ISO 27001) zur Gewährleistung der Integrität und Vertraulichkeit vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (728); zu den Anforderungen an die technischen und organisatorischen Maßnahmen vgl. *Pollirer in Knyrim* (Hrsg), *Der DatKomm*, Art 32 DSGVO Rz 27 f (Stand 1. 5. 2022, rdb.at).

¹²⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (wonach für eine Übermittlung zu anderen als den beauftragten Zwecken die Rechtsgrundlage fehlt); zur Unmöglichkeit des Zuschlags auf rechtswidrige Angebote vgl. auch *Tretzmüller*, *Handbuch Softwarerecht*¹ Rz 903.

¹²⁸ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727); siehe auch EDPB, European Data Protection Board, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems

3.3.1. Die Schrems II-Problematik als zentrale Herausforderung

Eine der komplexesten Herausforderungen bei der Beschaffung moderner SaaS-Dienstleistungen ist die potenzielle Übermittlung personenbezogener Daten in Drittstaaten. Dies betrifft in der Praxis primär die Einbindung von Cloud-Modellen marktdominanter US-Dienstleistungsunternehmen. Seit dem wegweisenden Urteil des EuGH in der Rechtssache *Schrems II*¹²⁹ und dem damit einhergehenden Wegfall des „EU-US Privacy-Shield“, das bislang einen Datentransfer in die USA legitimierte, setzt ein rechtmäßiger Datentransfer voraus, dass im Empfängerland ein Schutzniveau gewährleistet ist, das dem unionsrechtlichen Standard sachlich gleichwertig ist.¹³⁰

Für die USA wurde diese Rechtslage durch den Angemessenheitsbeschluss der Europäischen Kommission zum „EU-US Data Privacy Framework“ (DPF) vom 10. Juli 2023¹³¹ neu bewertet. Diese Entscheidung erleichtert den Datentransfer erheblich, sofern das anbietende Unternehmen unter dem Framework zertifiziert ist und in der offiziellen Liste des US-Handelsministeriums geführt wird. Für zertifizierte Organisationen entfällt die Notwendigkeit, zusätzliche Garantien wie Standardvertragsklauseln („Standard Contractual Clauses“ (SCC))¹³² oder ergänzende technische Maßnahmen vorzusehen.¹³³

Sofern jedoch keine Zertifizierung vorliegt oder der Transfer in ein Drittland ohne Angemessenheitsbeschluss erfolgt, verbleibt es bei den strengen Anforderungen der *Schrems II*-Judikatur. In diesen Fällen sind geeignete Garantien zu vereinbaren, vorrangig durch die von der EU-Kommission herausgegebenen SCC. Die bloße vertragliche Einbindung dieser Klauseln ist jedoch nicht ausreichend. Vielmehr obliegt es der öffentlichen Stelle in ihrer Funktion als Verantwortliche, die Rechtsordnung des Drittlandes im Rahmen einer Einzelfallprüfung zu verifizieren. In diesem als „Transfer Impact Assessment“ (TIA) bezeichneten Verfahren ist zu prüfen, ob die Wirksamkeit der

(23.07.2020), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_de.pdf, (abgerufen am 16. 1. 2026).

¹²⁹ EuGH C-311/18, *Schrems II*, ECLI:EU:C:2020:559.

¹³⁰ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 903.

¹³¹ Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. 7. 2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, ABI L 2023/231, 118.

¹³² vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 901.

¹³³ siehe zu ergänzenden Maßnahmen auch EDPB, European Data Protection Board, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems (23.07.2020) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_de.pdf (abgerufen am 16. 1. 2026).

Standardvertragsklauseln durch lokale Gesetze faktisch untergraben wird.¹³⁴

3.3.2. Technische und organisatorische Maßnahmen als Kompensation

Ein zentrales Element der datenschutzrechtlichen Compliance bildet die Verpflichtung zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art 32 DSGVO. Sowohl die verantwortliche Stelle als auch das auftragsverarbeitende Unternehmen sind normativ angehalten, geeignete technische und organisatorische Maßnahmen (TOM) zu implementieren, um ein dem Risiko angemessenes Schutzniveau zu garantieren.¹³⁵ Dieser risikobasierte Ansatz erfordert eine Abwägung zwischen dem Stand der Technik, den Implementierungskosten sowie der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung einerseits und der unterschiedlichen Eintrittswahrscheinlichkeit sowie Schwere potenzieller Grundrechtsbeeinträchtigungen andererseits.¹³⁶

Für die Vergabep Praxis impliziert dies, den unbestimmten Rechtsbegriff des "Standes der Technik" bereits in der Leistungsbeschreibung zu konkretisieren. In der Praxis orientieren sich auftraggebende Stellen zur Bestimmung des erforderlichen Sicherheitsniveaus häufig an etablierten Zertifizierungen und Standards. Einschlägige Normen wie die ISO/IEC 27001 fungieren dabei als Indikator für ein funktionierendes Informationssicherheits-Managementsystem und werden häufig als Teilnahmeanforderung vorgegeben.¹³⁷ Es ist jedoch hervorzuheben, dass Zertifikate allein die individuelle Prüfungspflicht der verantwortlichen Stelle nicht vollständig ersetzen, sondern lediglich als Indiz für die Eignung eines anbietenden Unternehmens herangezogen werden können.¹³⁸

3.3.3. Datenschutz-Folgenabschätzung als Pflichtinstrument

Maßgebliche Orientierungshilfen zur Identifizierung eines hohen Risikos nach Art 35 Abs 1 DSGVO bieten auf europäischer Ebene die Leitlinien der Art-29-Datenschutzgruppe.¹³⁹ Diese definieren spezifische Kriterien, die für SaaS-Modelle im öffentlichen Sektor von entscheidender Relevanz sind: Neben der Datenverarbeitung im großen Umfang wird insbesondere die innovative Nutzung technologischer oder

¹³⁴ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (unter Verweis auf die FAQ des EDSA); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 901 (zur Prüfpflicht des Datenexporteurs).

¹³⁵ vgl. *Pollirer* in *Knyrim*, Der Datkomm Art 32 DSGVO Rz 27 f.

¹³⁶ vgl. *Pollirer* in *Knyrim*, Der Datkomm Art 32 DSGVO Rz 28; vgl. auch Art 32 Abs 1 DSGVO.

¹³⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (728); vgl. auch *Tretzmüller*, Handbuch Softwarerecht¹ Rz 898.

¹³⁸ vgl. *Pollirer*, in *Knyrim*, Der Datkomm Art 32 DSGVO Rn 27 f.

¹³⁹ vgl. Art.-29-Datenschutzgruppe, WP 248, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), 9, https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf (abgerufen am 8.2.2026).

organisatorischer Lösungen als Indikator für die verpflichtende Vornahme einer Datenschutz-Folgenabschätzung (DSFA) genannt.¹⁴⁰ Eine solche Neuerung liegt bei SaaS-Modellen regelmäßig vor, da die Auslagerung von Anwendungen in externe Infrastrukturen die technische Kontrolle und Einsehbarkeit der Prozesse für die öffentliche Hand systembedingt reduziert und somit eine strukturelle Intransparenz schafft.

Im österreichischen Rechtsrahmen wird dieser Zusammenhang durch die Datenschutz-Folgenabschätzungs-Verordnung (DSFA-V)¹⁴¹ weiter konkretisiert. Gemäß § 2 Abs 2 Z 4 DSFA-V ist eine solche Folgenabschätzung zwingend durchzuführen, wenn neuartige organisatorische Lösungen zum Einsatz kommen, welche die Abschätzung der Auswirkungen auf die betroffenen Personen erschweren.¹⁴² In den Erläuterungen zur DSFA-V wird klargestellt, dass die Verordnung jene Verarbeitungsvorgänge typisiert, bei denen jedenfalls von einem hohen Risiko auszugehen ist, ohne dass damit der Anwendungsbereich des Art 35 Abs 1 DSGVO insgesamt abschließend determiniert würde.¹⁴³ Für SaaS-Beschaffungen kommt der DSFA-V vor allem insoweit Bedeutung zu, als sie eine nicht abschließende Liste hochrisikobehafteter Verarbeitungen enthält. Verantwortliche öffentlich auftraggebende Stellen haben daher auch bei nicht ausdrücklich erfassten SaaS-Konstellationen anhand der allgemeinen Kriterien des Art 35 Abs 1 DSGVO zu prüfen, ob die geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt.¹⁴⁴

3.3.4. Konsequenzen für die Vergabepaxis

Gelangt das TIA zu dem Ergebnis, dass im Empfängerland Defizite im Datenschutzniveau bestehen, die auch durch zusätzliche technische Maßnahmen nicht kompensiert werden können, scheidet ein vollumfänglicher Datentransfer in dieses Land und somit eine reine Public-Cloud-Lösung für Datenkategorien mit hohem Risiko aus. In diesem Spannungsfeld erweisen sich hybride Infrastrukturmodelle als sachlich gerechtfertigte und oft notwendige Option. Dabei verbleiben sensible oder besonders schutzwürdige

¹⁴⁰ vgl Art.-29-Datenschutzgruppe, WP 248, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), 9, https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf, 10 f (Kriterien 3 und 7) (abgerufen am 8.2. 2026).

¹⁴¹ Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist BGBl II 2018/278 (DSFA-V).

¹⁴² § 2 Abs 2 Z 4 DSFA-V BGBl II 2018/278; vgl *Trieb* in *Knyrim*, Der Datkomm Art 35 DSGVO Rz 41.

¹⁴³ Datenschutzbehörde, Erläuterungen zur DSFA-V, Allgemeiner Teil 1, https://dsb.gv.at/sites/site0344/media/downloads/erlaeuterungen_zur_dsfa-v.pdf, (abgerufen am 8. 2. 2026).

¹⁴⁴ vgl *Trieb* in *Knyrim*, Der Datkomm Art 35 DSGVO Rz 41; vgl Erläut DSFA-V, Besonderer Teil zu § 2 Abs 2 Z 4, 3, wonach die Nutzung organisatorischer Lösungen, welche die Abschätzung der Auswirkungen erschweren, die DSFA-Pflicht auslöst.

Datenbestände in einer lokalen On-Premise-Umgebung oder einer kontrollierten Private Cloud, während weniger kritische Daten in die Public Cloud ausgelagert werden.¹⁴⁵ Durch diese Datentrennung kann die öffentliche Auftraggeberschaft Skalierungsvorteile nutzen, ohne die Hoheit über sensible personenbezogene Daten zu verlieren.

Für die österreichische Vergabep Praxis ergeben sich aus dieser Problemstellung spezifische Anforderungen an die Eignungsprüfung sowie die Angebotsbewertung. Die datenschutzrechtliche Zuverlässigkeit der Anbietenden ist als wesentliches Element der technischen Leistungsfähigkeit in die Prüfung und Wertung einzubeziehen.¹⁴⁶ Konkret bedeutet dies, dass bei der Einbindung von US-Dienstleistungsunternehmen entweder der Nachweis einer Zertifizierung unter dem Data Privacy Framework oder – bei Rückgriff auf Standardvertragsklauseln – die Vorlage eines schlüssigen TIA-Konzepts einschließlich wirksamer technischer Zusatzmaßnahmen zu fordern ist. Kann das anbietende Unternehmen diesen Nachweis nicht erbringen, ist eine datenschutzkonforme Leistungserbringung faktisch ausgeschlossen. Ein Angebot, das auf einer solchen rechtswidrigen Datenübermittlung basiert, muss zwingend ausgeschieden werden, da die öffentlich auftraggebende Stelle keinen Zuschlag auf eine Leistung erteilen darf, deren Ausführung gegen zwingendes Unionsrecht verstoßen würde.¹⁴⁷

Die Einhaltung der datenschutzrechtlichen Vorgaben ist somit keine nachgelagerte Vertragsmodalität, sondern eine zwingende Prämisse für die Rechtmäßigkeit des gesamten Vergabeverfahrens. Die vorausschauende Risikobewertung verpflichtet die beschaffenden Stellen zu einer strengen Prüfung der datenschutzrechtlichen Eignung auf der Seite der anbietenden Unternehmen. Kann die unionsrechtlich gebotene Sicherheit der Verarbeitung nicht garantiert werden, führt dies mangels Zuschlagsfähigkeit zwingend zum Ausschluss des Angebots.¹⁴⁸ Datenschutzrechtliche Compliance avanciert somit zu einem wichtigen Eignungskriterium in der modernen IT-Vergabe.

¹⁴⁵ Zur Notwendigkeit der örtlichen Beschränkung der Verarbeitung (zB auf die EU/EWR) bei sensiblen Daten vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726); vgl. auch *Hunzinger*, CR 2023, 349 (357), wonach die Nutzung von Cloud-Services für kritische Infrastrukturen oft eingeschränkt ist.

¹⁴⁶ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (zur Auswahlverantwortung nach Art 28 Abs 1 DSGVO).

¹⁴⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (wonach es dem öffentlichen Auftraggeber an der Rechtsgrundlage fehlt); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 903.

¹⁴⁸ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (wonach es der öffentlichen Vergabestelle bei rechtswidriger Datenverarbeitung an der Rechtsgrundlage fehlt); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 903.

4. Welche Lösungen bietet das Vergaberecht?

Die in Kapitel 3 analysierten Herausforderungen – die Vergleichbarkeit heterogener Preismodelle, das Risiko eines Vendor-Lock-in sowie die datenschutzrechtliche Zulässigkeit von Drittstaatentransfers – werfen die Frage auf, welche Instrumente das geltende Vergaberecht zur Bewältigung dieser Problemlagen bereithält. Während Kapitel 3 die strukturellen Defizite offengelegt hat, widmet sich das folgende Kapitel der Frage, in welchem Umfang das geltende Vergaberecht Lösungsansätze zur Bewältigung dieser Herausforderungen bietet.

Die Antwort findet sich in einer konsequenten Anwendung der in Kapitel 2.4 dargelegten vergaberechtlichen Grundsätze auf die Spezifika von SaaS-Beschaffungen. Das zentrale Instrument bildet dabei die funktionale Leistungsbeschreibung, die es ermöglicht, Anforderungen technologieneutral zu formulieren und damit den Wettbewerb offenzuhalten, siehe Kapitel 0. Ergänzend hierzu bedarf es einer szenariobasierten Kostenabfrage, um die Heterogenität der Preismodelle in ein vergleichbares Bewertungsraster zu überführen, siehe Kapitel 4.2. Die qualitative Leistungssteuerung erfolgt über präzise definierte SLAs, siehe Kapitel 4.3, während klare Exit-Regelungen den Vendor-Lock-in verhindern, siehe Kapitel 4.4.

4.1. Technologieneutralität durch funktionale Leistungsbeschreibung

Die praktische Umsetzung der Technologieneutralität entscheidet sich bei SaaS-Beschaffungen an der Schnittstelle zwischen dem Bedarfsermessen der Vergabestelle und der rechtlichen Form der Leistungsbeschreibung.¹⁴⁹ Die §§ 103 und 106 BVergG 2018 bilden hierfür das zentrale Instrumentarium: Sie lenken die Beschreibung des Beschaffungsgegenstands auf funktions- und leistungsbezogene Vorgaben und beschränken technologiebezogene Festlegungen auf objektiv erforderliche, auftragsbezogene und verhältnismäßige Ausnahmefälle.¹⁵⁰ Über das Gleichwertigkeitsprinzip des § 106 Abs 6 BVergG 2018 wird zugleich die Teilnahme technisch andersartiger, aber gleich leistungsfähiger Cloud-Lösungen eröffnet.¹⁵¹

4.1.1. Funktionsbezogene Leistungsbeschreibung als Regelmodell

Wie in Kapitel 2.4 dargelegt, lässt § 103 BVergG 2018 sowohl eine konstruktive als auch eine funktionale Leistungsbeschreibung zu. Erfahrungsgemäß ist in IT-Vergaben

¹⁴⁹ § 103 BVergG 2018.

¹⁵⁰ § 106 Abs 1 BVergG 2018; LVwG NÖ 7. 6. 2018, LVwG-VG-3/002-2018.

¹⁵¹ § 106 Abs 6 BVergG 2018.

die funktions- bzw leistungsbezogene Beschreibung die sachgerechtere Option, weil sie den Bedarf über Funktionen, Qualitätsniveaus und Schutzziele definiert und die Frage der konkreten technischen Umsetzung den Anbietenden überlässt.¹⁵² Die Materialien zum BVerG 2018 knüpfen daran ausdrücklich die Erwartung, dass funktionale Beschreibungen den Wettbewerb stärken und technische Innovationen begünstigen.¹⁵³ Gerade im Cloud-Bereich, der von Virtualisierung, Mehrmandanten-Architekturen und standardisierten Schnittstellen geprägt ist, spricht vieles dafür, Anforderungen funktional zu formulieren. Damit bleiben sowohl On-Premise- als auch SaaS-Lösungen grundsätzlich zugelassen, ohne eine bestimmte Architektur vorzugeben.¹⁵⁴

Demgegenüber verengen konstruktive Vorgaben, die architektonische Details oder einen bestimmten Bereitstellungsmodus festschreiben – etwa durch Vorgaben wie "Installation im lokalen Subnetz auf kundeneigener Hardware" oder "Betrieb ausschließlich im Rechenzentrum der Vergabestelle" – den Wettbewerb typischerweise faktisch auf On-Premise-Szenarien. In einem Markt, in dem Cloud-typische Leistungen in hohem Maße standardisiert sind, kann bereits eine aus Sicht der öffentlich auftraggebenden Stelle untergeordnete konstruktive Spezifikation einzelne anbietende Unternehmen *de facto* ausschließen.¹⁵⁵

Methodisch geboten ist daher eine technologieoffene Beschreibung über Funktionen, Schutzziele und Qualitätsniveaus, flankiert durch klare Mess- und Nachweiskonzepte.¹⁵⁶ Praktisch bedeutet dies, dass Anforderungen an Verfügbarkeiten des Systems, Informationssicherheit, Interoperabilität und Datenportabilität so zu formulieren sind, dass verschiedene Bereitstellungsmodelle prinzipiell teilnahmefähig bleiben. Das Bereitstellungsmodell wird dadurch für die Zulässigkeit des Angebots nachrangig, solange die geforderten Ergebnisse nachprüfbar erreicht werden.¹⁵⁷

4.1.2. Sachlichkeitsprüfung technologiebezogener Vorgaben

Setzt die Vergabestelle dennoch an einem bestimmten Bereitstellungsmodell an, etwa

¹⁵² vgl *Diem* in *Gölles/Casati*, BVerG 2018, §106 Rz 18 ff.

¹⁵³ vgl ErläutRV 69 BlgNR 26. GP 133 f; vgl *Diem* in *Gölles/Casati*, BVerG 2018, §106 Rz 18 ff.

¹⁵⁴ VwGH 17. 11. 2004, 2002/04/0078, unter Verweis auf EuGH C-448/01, *EVN AG und Wienstrom GmbH*, ECLI:EU:C:2003:65, Rz 57 und EuGH, C-19/00, *SIAC Construction*, ECLI:EU:C:2001:553, Rn 41; EuGH C-278/14; *Enterprise Focused Solutions*, ECLI:EU:C:2015:228, Rn 27 ff, siehe auch *Diem*, in *Gölles/Casati*, BVerG 2018 § 106 Rz 5 f.

¹⁵⁵ vgl *Diem* in *Gölles/Casati*, BVerG 2018, §106 Rz 22.

¹⁵⁶ vgl *Schrotz/Zdanowiecki*, CR 2015, 485 (486 ff).

¹⁵⁷ vgl *Claßen/Koch/Müller*, MMR 2020, 723 (724 f).

On-Premise, handelte es sich um eine technologiebezogene Festlegung.¹⁵⁸ Diese ist nur zulässig, wenn sie durch den Auftragsgegenstand objektiv erforderlich ist und weniger eingriffsintensive, technologieoffene Spezifikationen das Beschaffungsziel nicht ebenso gut erreichen könnten.¹⁵⁹ In der Praxis kommen als sachliche Gründe insbesondere nachweisliche Offline-Erfordernisse, etwa für einen autarken Krisen- oder Ausfallbetrieb, besonders hohe Geheimschutzbedarfe oder zwingende Integritäts- und Kompatibilitätsanforderungen bei Erweiterungsvorhaben in Betracht.¹⁶⁰

Liegt keine sachliche Rechtfertigung für eine bestimmte Betriebsform vor, müssen die Anforderungen an Datensicherheit und Systembetrieb über messbare Standards definiert werden. Statt eine Technologie vorzuschreiben, sind klare Kriterien für Verfügbarkeit, Datentransfer und Interoperabilität mit anderen Systemen festzulegen, sodass On-Premise- und Cloud-Lösungen gleichermaßen teilnehmen können.¹⁶¹ Die wettbewerblichen Auswirkungen potenziell verengender Vorgaben sind vorab zu prüfen und – einschließlich geprüfter Alternativen – im Vergabevermerk nachvollziehbar zu dokumentieren.¹⁶²

Um die Wahl einer bestimmten Betriebsform objektiv zu rechtfertigen, empfiehlt sich im Vorfeld die Durchführung einer Markterkundung gemäß § 24 BVergG 2018. Mit diesem Instrument lässt sich klären, welche Lösungen am Markt verfügbar sind und ob Cloud-Angebote die gestellten Anforderungen, insbesondere an Sicherheit und Souveränität, ebenso erfüllen können.¹⁶³ Das Bundesverwaltungsgericht (BVwG) hat außerdem anerkannt, dass die Vergabestellen durch eine im Vergabeakt dokumentierte Markterkundung nachweisen können, nicht gegen das Diskriminierungsverbot verstoßen zu haben.¹⁶⁴

4.1.3. Gleichwertigkeitsprinzip und Nachweisführung

Bezieht sich die technische Spezifikation ausnahmsweise auf bestimmte Normen, Marken, Herkunftse oder besondere Verfahren im Sinne des § 106 Abs 5 BVergG 2018, ordnet § 106 Abs 6 BVergG 2018 zwingend den Zusatz "oder gleichwertig" an.¹⁶⁵ Nach

¹⁵⁸ § 106 Abs 1 BVergG 2018.

¹⁵⁹ § 106 Abs 2 Z 2/3 BVergG 2018.

¹⁶⁰ ErlRV BGBl I Nr 65/2018 S 44.

¹⁶¹ vgl § 106 BVergG 2018; *Diem* in *Gölles/Casati*, BVergG 2018, § 106 Rz 12.

¹⁶² vgl *Schrotz/Zdanowiecki*, CR 2015, 485 (489 f).

¹⁶³ VwGH 1. 3. 2022, Ra 2019/04/0139, Rn 1.

¹⁶⁴ §§ 24, 196 BVergG; BVwG 12. 9. 2018, W138 2203735-2; vgl auch *Diem* in *Gölles/Casati*, BVergG 2018, § 106 Rz 19.

¹⁶⁵ § 106 Abs 5 und 6 BVergG 2018, Art 42 der Vergaberichtlinie; vgl *Diem* in *Gölles/Casati*, BVergG

österreichischer Lehre dürfen Vergabestellen zwar an Referenzprodukte oder -normen anknüpfen, müssen über die Gleichwertigkeitsöffnung aber Raum für technisch andersartige Lösungen lassen, die die geforderten Funktionen und Schutzziele in gleichwertiger Weise erreichen.¹⁶⁶

Der entsprechende Nachweis ist aus Gründen der Gleichbehandlung und Transparenz grundsätzlich bereits mit der Angebotsabgabe zu erbringen. Für SaaS-Angebote bedeutet Gleichwertigkeit vergaberechtlich nicht Identität der System- oder Infrastrukturarchitektur, sondern die Gleichwertigkeit der funktionalen und qualitativen Ausführung der Leistung. Entscheidend ist das erreichte Ergebnis und nicht das zugrunde liegende Bereitstellungsmodell oder die spezifische technische Umsetzung.¹⁶⁷

Geeignete, technologieagnostische Kriterien – die in den Unterlagen klar zu definieren und mit entsprechenden Nachweisformen zu hinterlegen sind – umfassen insbesondere ein nachweisbares Informationssicherheitsniveau, wie etwa durch ein zertifiziertes Informationssicherheits-Managementsystem, sowie die durchgängige Verschlüsselung der Daten und ein geregeltes Schwachstellen- und Störungsmanagement. Darüber hinaus sind Anforderungen an die Verfügbarkeit und Betriebskontinuität sowie die Datenportabilität und Reversibilität von zentraler Bedeutung. Letztere ist vor allem durch die Möglichkeit vollständiger Datenexporte in standardisierten, maschinenlesbaren Formaten sowie durch klar dokumentierte Exit-Prozesse sicherzustellen. Schließlich bildet die Interoperabilität über standardisierte Schnittstellen ein wesentliches Kriterium, um die Zusammenarbeit mit anderen Systemen herstellerunabhängig zu gewährleisten.¹⁶⁸

Derartige Kriterien verlagern die Prüfung weg vom zugrundeliegenden Betriebsmodell hin zur Erreichung der Schutzziele in den Bereichen Sicherheit, Verfügbarkeit, Portabilität und Interoperabilität. Die §§ 108 und 109 BVergG 2018 stellen hierfür das notwendige Instrumentarium bereit, um Spezifikationen über Gütezeichen, Testberichte oder Zertifizierungen zu operationalisieren. Dabei muss die öffentlich auftraggebende Stelle jedoch stets die nach § 106 Abs 3 und 4 gebotene Offenheit für gleichwertige Nachweise sicherstellen, um den Wettbewerb nicht unzulässig auf Anbietende bestimmter

2018, §106 Rz 14; vgl auch EuGH C-59/00, *Bent Moustén Vestergaard*, ECLI:EU:C:2001:652, Rn 14 f.

¹⁶⁶ vgl *Diem* in *Gölles/Casati*, BVergG 2018, §106 Rz 3 ff, 39 ff; *Kurz* in *Heid/Deutschmann/Hofbauer/Reisner* (Hrsg), BVergG 2018 (2019) § 106 BVergG 2018, Rz 3 f, 9 ff; *Schrotz/Zdanowiecki*, CR 2015, 485 (486, 489 f).

¹⁶⁷ vgl *Diem* in *Gölles/Casati*, BVergG 2018, §106 Rz 6 f, 16, 40 f; *Kurz* in *Heid et al*, BVergG 2018, § 106 BVergG 2018, Rz 3 f, 9 ff; *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f).

¹⁶⁸ vgl *Tretzmüller*, Handbuch Softwarerecht¹ Rz 1063, 1065–1066, 2086 ff.

Zertifizierungen zu verengen.¹⁶⁹

Daraus ergibt sich konsequenterweise, dass ein Angebot nicht allein deshalb ausgeschlossen werden darf, weil es cloudbasiert ist. Maßgeblich ist, ob die in der Ausschreibung rechtmäßig und sachlich gerechtfertigt geforderten Anforderungen erfüllt werden bzw – bei abweichender Architektur – der Gleichwertigkeitsnachweis ordnungsgemäß geführt wurde. Die Produkt- und Technologieneutralität nach § 106 BVergG 2018 und die vom EuGH entwickelte Linie zur künstlichen Einengung des Wettbewerbs verbieten es, Cloud-Angebote allein wegen ihrer Bereitstellungsform auszuschließen, sofern sie die geforderten Schutzziele und Leistungsparameter nachprüfbar erreichen.¹⁷⁰

4.2. Vergleichbarkeit durch szenariobasierte TCO-Bewertung

Die in Kapitel 3.1 analysierte Heterogenität der SaaS-Preismodelle – von nutzerabhängigen Entgelten über volumenbasierte Zuschläge bis zu optionalen Zusatzmodulen – erfordert ein methodisches Instrument, um variable Entgeltbestandteile in ein objektivierbares Bewertungsraster zu überführen.¹⁷¹ Die bloße Abfrage von Basispreisen genügt dem vergaberechtlichen Transparenz- und Gleichbehandlungsgebot nicht, da sie die tatsächlichen Kosten über den gesamten Lebenszyklus nicht abbildet.¹⁷² Die Lösung bietet die szenariobasierte Lebenszykluskostenrechnung, auch als „Total Cost of Ownership“ (TCO)-Bewertung bezeichnet.¹⁷³

4.2.1. Methodische Grundlagen der TCO-Bewertung

Die TCO-Betrachtung umfasst die Summe aller Kosten, die während der gesamten Lebensdauer eines Produkts oder einer Dienstleistung anfallen.¹⁷⁴ Dazu gehören neben den direkten Anschaffungskosten auch indirekte Kosten wie Wartung, Instandhaltung,

¹⁶⁹ § 106 Abs 3 und 4, §§ 108, 109 BVergG 2018; vgl *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 5.

¹⁷⁰ EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 61 f; EuGH C-413/17, *Roche Lietuva*, ECLI:EU:C:2018:865, Rn 35 f, 38; BVwG 26. 6. 2018, W139 2162939-2; vgl *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 6 f, 16, 39 f.

¹⁷¹ vgl *Claßen/Koch/Müller*, MMR 2020, 723 (725); zur Vielfalt der Vergütungsmodelle (Pay-as-you-go vs Pauschale) siehe auch *Möglich* in *Taeger/Pohle* Rz 203.

¹⁷² vgl Art 67 Abs 2 lit. b RL 2014/24/EU; § 92 i.V.m. § 2 Z 23 BVergG 2018; zur Erforderlichkeit vorher bekannt gemachter Bewertungsmaßstäbe und zur Vergleichbarkeit der Angebote *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f); CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 38 f (abgerufen am 21. 1. 2026).

¹⁷³ Total Cost of Ownership (TCO): So behält der Einkauf die Gesamtkosten im Blick, Beschaffung aktuell, 29.7.2024, [Total Cost of Ownership \(TCO\): So behält der Einkauf die Gesamtkosten im Blick](#) (abgerufen am 30. 12. 2025).

¹⁷⁴ Total Cost of Ownership (TCO): So behält der Einkauf die Gesamtkosten im Blick, Beschaffung aktuell, 29.7.2024, [Total Cost of Ownership \(TCO\): So behält der Einkauf die Gesamtkosten im Blick](#) (abgerufen am 30. 12. 2025).

Energieverbrauch, Schulungen, Entsorgung und Produktivitätsausfälle. Nur durch die Vorgabe fiktiver, aber realistischer Nutzungsszenarien in den Vergabeunterlagen können die unterschiedlichen Preiskurven der teilnehmenden Unternehmen auf einen vergleichbaren Nenner gebracht werden.¹⁷⁵

Für IT-Vergaben verlangt das Bestbieterprinzip eine lebenszyklusbezogene Wirtschaftlichkeitsbetrachtung. Im Kontext von Cloud-Diensten treten an die Stelle klassischer Entsorgungskosten insbesondere die Aufwendungen für den Projektabschluss sowie die Datenmigration bei einem Wechsel des Dienstleistungsunternehmens, mithin die typischerweise anfallenden Exit-Kosten.¹⁷⁶ In der Praxis kommt es bei On-Premise-Beschaffungen häufig zu verkürzten Preisvergleichen, welche die betrieblichen Vorhalte- und Betriebskosten nicht vollständig abbilden. Methodisch korrekt zu berücksichtigen sind hierbei insbesondere Hardware- und Erneuerungszyklen, Aufwände für Energie und Klimatisierung sowie Personalressourcen für die Administration, das Update-Management oder Wiederherstellungsszenarien. Auch die Kosten für physische Sicherheit, Notfallvorsorge und die laufenden Compliance-Aufwände müssen in eine valide Kalkulation einfließen.¹⁷⁷

Demgegenüber beinhalten Cloud- und SaaS-Leistungen wesentliche Betriebs- und Sicherheitskomponenten bereits im Serviceentgelt, etwa zentrale Wartung, regelmäßige Updates und die elastische Bereitstellung von Ressourcen. Nur eine Lebenszykluskostenrechnung, die sämtliche Betriebs-, Risiko- und Exit-Kosten einbezieht, verhindert eine strukturelle Unterbewertung von SaaS-Modellen und ermöglicht einen sachgerechten Vergleich mit On-Premise-Lösungen.¹⁷⁸

4.2.2. Operationalisierung durch Referenzszenarien

Um diesem Bestimmtheitsgebot zu genügen, ist die Anwendung einer szenariobasierenden Lebenszykluskostenrechnung zwingend geboten. Die öffentlich auftraggebende Stelle gibt hierfür fiktive, jedoch realistische Nutzungsszenarien in den Vergabeunterlagen vor. Diese Vorgaben, etwa der vollständige Datenexport und die vollständige Datenmigration nach Vertragsende, sind von der anbietenden Seite einheitlich zu

¹⁷⁵ vgl. *Casati in Göllles/Casati*, BVergG 2018 § 92 Rz 4 ff.

¹⁷⁶ § 2 Z 23 BVergG 2018; §§ 20, 91 ff BVergG; Art 67 und Art 68 Abs 2 der Vergaberichtlinie; vgl. *Casati in Göllles/Casati*, BVergG 2018 § 91, Rz 8 ff (insb zu Bestbieterprinzip und Lebenszykluskosten).

¹⁷⁷ Art 67 und 68 Abs 2 RL 2014/24/EU.

¹⁷⁸ § 20 Abs 1 BVergG 2018; vgl. *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f); *Casati in Göllles/Casati*, BVergG 2018, § 92 Rz 1, 4 f, 8 ff.

bepreisen, um eine objektive Vergleichbarkeit zu gewährleisten. Auf diese Weise lassen sich variable Gebühren, etwaige Kündigungsfristen/-gebühren sowie Exit- und Migrationskosten in ein objektivierbares Bewertungsraster überführen. Dies vermeidet Überraschungskosten nach Zuschlagserteilung, gewährleistet Transparenz und ermöglicht eine echte Vergleichbarkeit der Angebote gemäß § 58 VgV bzw § 127 GWB und § 24 BVergG 2018.

In der österreichischen Vergabep Praxis hat sich die Vorgabe strikter Referenzszenarien als praktikabler Lösungsansatz etabliert. Die ausschreibenden Stellen definieren fiktive Nutzungsmuster, die zwingend zu bepreisen sind. Dies transformiert heterogene Abrechnungsmodelle in einen vergleichbaren Gesamtpreis, ohne den Markt auf ein spezifisches Geschäftsmodell einzuengen.¹⁷⁹ Entscheidend für die Rechtssicherheit ist, dass die Vergabestellen in den Vergabeunterlagen verbindliche Parameter vorgeben. Dazu zählen insbesondere standardisierte Nutzungsprofile, normierte Service-Level-Parameter und Exit-Leistungen sowie ein eindeutig definierter Bewertungszeitraum und klare Rechenregeln.¹⁸⁰ Ohne diese Spezifikationen drohen systematische Bewertungsverzerrungen und Verstöße gegen das unionsrechtliche Transparenzgebot.¹⁸¹

4.2.3. Rechtsvergleichende Perspektive

Im Rechtsvergleich zwischen Deutschland und Österreich haben sich unterschiedliche Lösungsansätze herausgebildet, um dieser Heterogenität zu begegnen. In Deutschland wird die Vergleichbarkeit stärker durch die EVB-IT Cloud und methodische Hilfestellungen wie die „Unterlage für Ausschreibung und Bewertung von IT-Leistungen“ (UfAB)¹⁸² gesteuert.¹⁸³ Bei den UfAB handelt es sich um einen umfassenden Leitfaden des Bundesministeriums des Innern der öffentlichen Stellen durch den gesamten Beschaffungsprozess führt und insbesondere standardisierte Bewertungsmatrizen bereitstellt, um komplexe IT-Angebote objektiv vergleichbar zu machen. Beide Instrumente wirken

¹⁷⁹ Zur Technologieneutralität vgl § 106 Abs 1 BVergG 2018; Göllers in Göllers/Casati, BVergG 2018 § 106 Rz 1 ff.

¹⁸⁰ Claßen/Koch/Müller, MMR 2020, 723 (725 f).

¹⁸¹ vgl Lampert in Burgi/Dreher/Opitz (Hrsg), Beck'scher Vergaberechtskommentar Bd 14 § 121 GWB Rz 9 (Stand 2022, beck-online.de); Zimmermann in Summa/Schneevogl, jurisPK-Vergaberecht⁷ § 121 GWB Rz 30.

¹⁸² ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html> (abgerufen am 1. 1. 2026).

¹⁸³ Zur Standardisierung durch das Vertragsmuster und die Anlagenhierarchie der EVB-IT Cloud vgl Möglich in Taeger/Pohle Rn 161 ff; zur funktionalen Leistungsbeschreibung als Standardisierungsinstrument siehe ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 173 f (abgerufen am 1. 1. 2026).

komplementär für einen durchgängigen Beschaffungsprozess: Während Leitfäden wie die UfAB die Methode für die Vergabephase – insbesondere Leistungsbeschreibung und Zuschlagsermittlung – bereitstellen, stellen die EVB-IT Cloud das Rahmenwerk für die Vertragsphase dar. Sie dienen der einheitlichen Gestaltung der IT-Verträge und gewährleisten durch standardisierte Vertragsbedingungen die Vergleichbarkeit der Angebote und die Chancengleichheit der Anbietenden.¹⁸⁴ Für öffentliche Vergabestellen in Deutschland reduziert diese Standardisierung die individuelle Gestaltungslast und erhöht die Transparenz und Rechtssicherheit.¹⁸⁵

Für Österreich, ohne vergleichbares zentrales Regelwerk, wird die Anwendung dieser Prinzipien – insbesondere der szenariobasierten Kostenabfrage – zur Sicherstellung der Transparenz und zur Ermittlung des wirtschaftlichsten Angebots nach dem BVergG ebenfalls empfohlen.¹⁸⁶

Beiden Ansätzen ist das Ziel gleich: die Schaffung einer nachvollziehbaren und objektiven Basis für die Zuschlagserteilung auf das wirtschaftlichste Angebot (vgl. bereits Kapitel 2.3.3)¹⁸⁷

4.2.4. *Praktische Umsetzung in den Vergabeunterlagen*

Im Sinne einer objektiven Vergleichbarkeit sind neben den internen Aufwänden bei SaaS-Modellen daher insbesondere nutzungs- oder funktionsbasierte Entgelte sowie die Bepreisung von Exit-Leistungen einzubeziehen. Die daraus resultierende Bewertungsmethodik – bestehend aus dem Betrachtungszeitraum, den Mengengerüsten und den Umrechnungsformeln – ist gemäß § 92 Abs 2 BVergG 2018 zwingend in den Vergabeunterlagen offenzulegen. Dies stellt nicht nur sicher, dass das wirtschaftlichste Unternehmen auf Basis der tatsächlichen ökonomischen Effizienz über den gesamten Nutzungszeitraum ermittelt wird, sondern garantiert auch, dass die Zuschlagsentscheidung im Sinne des Transparenzgebots des § 20 BVergG 2018 vollumfänglich nachvollziehbar bleibt.¹⁸⁸

¹⁸⁴ vgl. *Möglich*, in *Taege/Pohle* Rz 7 ff, 20 ff; *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff; *Möglich*, in *Taege/Pohle* Rz 160 f.

¹⁸⁵ vgl. *Möglich*, in *Taege/Pohle* Rz 160.

¹⁸⁶ vgl. *Gölles* in *Casati/Gölles*, BVergG 2018, § 91 Rz 15 ff.

¹⁸⁷ Zum Zuschlag auf das wirtschaftlichste Angebot vgl. § 91 Abs 1 BVergG 2018 für Österreich und § 127 Abs 1 GWB für Deutschland.

¹⁸⁸ § 2 Z 23, § 20 Abs 1, § 92 Abs 1 und 2 BVergG 2018; Art 67 Abs 2 lit b, Art 68 der Vergaberichtlinie; *Casati* in *Gölles/Casati*, BVergG 2018 § 92 Rz 4; vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff; *Claßen/Koch/Müller*, MMR 2020, 723 (724 f); *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f).

Ohne eine solche Normierung droht die in Kapitel 3.1 analysierte faktische Unvergleichbarkeit der Angebote aufgrund der Koexistenz diverser Preismodelle. Die gewählte Umrechnungsformel muss daher gewährleisten, dass der relative Preisabstand zwischen den Angeboten – unabhängig vom zugrundeliegenden Vergütungsmodell – angemessen abgebildet wird.¹⁸⁹

Die beschriebene szenariobasierte TCO-Bewertung erweist sich somit als unverzichtbares methodisches Instrument, um die in Kapitel 3.1 identifizierte Herausforderung der Vergleichbarkeit zu bewältigen. Sie überführt die Heterogenität der Preismodelle in ein transparentes, objektives Bewertungsraster und sichert damit die Integrität des Vergabeverfahrens.¹⁹⁰

4.3. Qualitätssteuerung durch Service-Level-Agreements (SLAs)

Während die szenariobasierte TCO-Bewertung die ökonomische Vergleichbarkeit sicherstellt, bedarf es eines komplementären Instruments zur qualitativen Steuerung der Leistungserbringung. Diese Funktion erfüllen SLAs, die als technische und juristische Schnittstelle zwischen der abstrakten Leistungsbeschreibung und der realen Durchführung fungieren. SLAs definieren die geschuldete Servicequalität anhand messbarer Parameter und verknüpfen diese mit Sanktionen bei Nichteinhaltung.¹⁹¹

4.3.1. Die Herausforderung der Vergleichbarkeit von SLA-Parametern

Die zentrale Herausforderung im Vergabeverfahren liegt in der Herstellung einer belastbaren Vergleichbarkeit. Ein rein numerisches Gegenüberstellen von Verfügbarkeitszielen – etwa der Vergleich von 99,9 % und 99,95 % Verfügbarkeitszusagen – greift ohne eine normierte Definition der zugrundeliegenden Parameter zu kurz und ist im Kern irreführend.¹⁹² Unterschiede in der Messmethodik können dazu führen, dass nominell identische oder sogar höhere Werte bei genauerer Analyse ein völlig anderes Qualitätsniveau abbilden. Dies ist keine bloße theoretische Gefahr: Problematisch wird es insbesondere dann, wenn anbietende Unternehmen Ausfallzeiten durch weitreichende Ausnahmetatbestände oder sehr großzügig bemessene Messfenster statistisch

¹⁸⁹ zur Notwendigkeit der TCO-Betrachtung zur Herstellung von Vergleichbarkeit vgl. CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 39 (abgerufen am 21. 1. 2026).

¹⁹⁰ ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 55 ff (abgerufen am 1. 1. 2026).

¹⁹¹ vgl. Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 105 ff.

¹⁹² vgl. Möglich in Taeger/Pohle Rz 188 ff; vgl. Heydn, MMR 2020, 435 (436 ff).

relativieren.¹⁹³

Um derartige Bewertungsverzerrungen und damit eine Verletzung des Transparenz- sowie Gleichbehandlungsgebots zu vermeiden, muss die öffentlich auftraggebende Stelle die wertungsrelevanten Parameter normativ vorgeben. Elementar ist die Festlegung des Verfügbarkeitsziels in strikter Korrelation zum Messfenster. Während die anbietende Seite oft Jahresmittelwerte präferiert, um kurzzeitige Ausfälle statistisch zu glätten, sichert aus Sicht der Beschaffungsstelle nur ein Monatsfenster oder ein rollierender Zeitraum eine kontinuierliche Leistungsqualität.¹⁹⁴

Eng damit verknüpft ist die präzise Definition der Ausfallzeit bzw. Nichtverfügbarkeit des Systems. Es bedarf einer eindeutigen vertraglichen Fixierung, ab welcher Mindestdauer eine Störung als Ausfallzeit gewertet wird und wie die Kumulation kurzer Unterbrechungen zu behandeln ist.¹⁹⁵ Ein weiterer kritischer Parameter betrifft die Handhabung von Wartungsfenstern. Werden geplante Wartungsarbeiten in die Berechnung der Verfügbarkeit einbezogen, sinkt zwar die nominelle Verfügbarkeit, es spiegelt jedoch die reale Nutzungssituation wider. Werden die Wartungsfenster exkludiert, steigt der Wert künstlich an, ohne die faktische Nutzbarkeit zu erhöhen. Eine transparente Leistungsbeschreibung muss daher klar regeln, ob und welche Wartungsfenster in die Verfügbarkeitsberechnung einfließen.¹⁹⁶

Ebenso bedarf es einer restriktiven Definition von Ausnahmetatbeständen, also Ereignissen, die nicht als vertragsverletzende Ausfallzeit gewertet werden. Hierzu zählen typischerweise Fälle höherer Gewalt, aber auch Störungen, die durch Drittkomponenten verursacht werden, die nicht im Verantwortungsbereich des anbietenden Unternehmens liegen.¹⁹⁷ Fehlt es an einer solchen Präzisierung, droht das SLA zu einem stumpfen Schwert zu verkommen, da ohne konkrete Sanktionen die automatische Durchsetzung fehlt und dies dazu führt, dass Anbietende die vertraglich vereinbarten Verpflichtungen ignorieren, weil sie ohnehin sanktionsfrei bleiben.¹⁹⁸

¹⁹³ vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 102 ff.

¹⁹⁴ vgl. *Hunzinger*, CR 2023, 349 (351); vgl. *Möglich* in *Taeger/Pohle* Rz 188 ff.

¹⁹⁵ vgl. *Heydn*, MMR 2020, 435 (436 f).

¹⁹⁶ vgl. *Möglich* in *Taeger/Pohle* Rz 189; vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 105.

¹⁹⁷ vgl. *Tretzmüller*, Handbuch Softwarerecht¹ Rz 1063 ff (zu Haftungsausschlüssen in internationalen Cloud-Verträgen).

¹⁹⁸ eigene Wertung, vgl. auch *Heydn*, MMR 2020, 435 (436); oder *Bischof*, ITRB 2023, 165 (165 ff) mit ähnlicher Conclusio.

4.3.2. Sicherheitsanforderungen und technische Standards

Über die reine Verfügbarkeit hinaus sind von der ausschreibenden Stelle technische Sicherheitsanforderungen an den SaaS-Dienst risikoadäquat und dem aktuellen Stand der Technik entsprechend zu determinieren. Dies umfasst detaillierte Vorgaben zum Informationssicherheitsmanagement, zur Verschlüsselung von Datenübertragung und -speicherung sowie zum Umgang mit Sicherheitsvorfällen.¹⁹⁹

Zur Operationalisierung dieser komplexen Anforderungen bietet sich für den deutschen Raum insbesondere der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Kriterienkatalog C5 an.²⁰⁰ Dieser ermöglicht es, Sicherheitsniveaus vergleichbar zu machen und standardisierte Auditrechte vertraglich zu verankern.²⁰¹ Die Relevanz solcher Standards erschöpft sich jedoch nicht in der rein technischen Absicherung; vielmehr bilden sie das objektive Fundament für die verfahrensrechtliche Steuerung.²⁰²

In Österreich orientiert sich die Verwaltungspraxis bei der Konkretisierung technischer Sicherheitsvorgaben primär am Österreichischen Informationssicherheitshandbuch, welches als zentrales Referenzwerk für öffentlich auftraggebende Stellen fungiert. Es unterstützt öffentlich auftraggebende Stellen dabei, die technischen Anforderungen im Leistungsverzeichnis so zu definieren, dass sie den spezifischen Sicherheitsbedarfen der nationalen Verwaltung entsprechen und den Stand der Technik konkretisieren.²⁰³

4.3.3. Vergaberechtliche Einordnung von SLA-Parametern

In diesem Sinne fungieren SLA-Parameter vergaberechtlich als notwendige Konkretisierung der Leistungsbeschreibung. Je nach strategischer Zielsetzung lassen sie sich entweder als zwingende Mindestanforderungen festlegen, deren Nichterfüllung zum Ausschluss aus dem Verfahren führt, oder als qualitative Zuschlagskriterien nutzen, um die technologische Leistungsfähigkeit der Angebote im Wettbewerb differenziert zu

¹⁹⁹ vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 102 ff.

²⁰⁰ Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloud Computing Compliance Criteria Catalogue (C5), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html (abgerufen am 2. 1. 2026).

²⁰¹ vgl. *Hunzinger*, CR 2023, 349 (353).

²⁰² vgl. *Hunzinger*, CR 2023, 349 (352).

²⁰³ Digitales Österreich, Österreichisches Informationssicherheitshandbuch, <https://www.sicherheitshandbuch.at> (abgerufen am 08. 02. 2026).

bewerten.²⁰⁴ Der unionsrechtliche Transparenzmaßstab verlangt dabei zwingend, dass aus den Vergabeunterlagen für den Kreis der Teilnehmenden zweifelsfrei hervorgeht, welche Anforderungen zu erfüllen sind und nach welcher Methodik die Bewertung erfolgt.²⁰⁵ Die deutsche Rechtsprechung hat in diesem Zusammenhang wiederholt Bewertungs- und Wertungssysteme beanstandet, die wegen intransparenter Maßstäbe oder fehlender Nachvollziehbarkeit keine verlässliche Angebotskalkulation bzw. Vergleichbarkeit zuließen.²⁰⁶ Ermangelt es den SLA-Parametern an dieser notwendigen Bestimmtheit, ist eine objektive Vergleichbarkeit nicht mehr gegeben, was den Ausschluss der betroffenen Angebote nach sich ziehen muss oder das Verfahren rechtswidrig macht.²⁰⁷

4.3.4. Rechtsvergleichende Perspektive: Österreich vs. Deutschland

In der Vergabepraxis zeigen sich im Vergleich zwischen Österreich und Deutschland signifikante Unterschiede in der strategischen Handhabung dieser Komplexität. In Österreich dominiert ein eher restriktiver Ansatz: Gemäß § 91 Abs 6 BVergG 2018 müssen Zuschlagskriterien nicht nur mit dem Auftragsgegenstand zusammenhängen, sondern so präzise gefasst sein, dass eine wirksame Überprüfung der Angebote möglich ist. Aufgrund der strengen Judikatur zur Bestimmtheit von Kriterien werden SLAs in der österreichischen Praxis häufig als rein technische Mindestanforderungen in Form von K.O.-Kriterien definiert.²⁰⁸ Dieser Ansatz sichert zwar eine einheitliche Qualitätsbasis, verzichtet jedoch auf das Potenzial, qualitative Unterschiede wettbewerblich zu honorieren. Eine wertende Berücksichtigung im Zuschlagszenario ist zwar nach § 91 Abs 6 BVergG 2018 zulässig, setzt jedoch voraus, dass die Bewertungsregeln keinerlei Ermessensspielraum lassen – eine Anforderung, die bei komplexen SLA-Metriken eine erhebliche juristische Hürde darstellt.²⁰⁹

In Deutschland hingegen hat sich durch die EVB-IT Cloud eine stärkere Standardisierung etabliert. Die Vertragsmuster bieten vordefinierte Regelungen zu Verfügbarkeit

²⁰⁴ §§ 91, 114 BVergG 2018; vgl. Göllles in *Göllles/Casati*, BVergG 2018 § 114 Rz 34; *Casati* in *Göllles/Casati*, BVergG 2018 § 91 Rz 12 ff.

²⁰⁵ EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 25, 88 ff.

²⁰⁶ BVerwG 13. 12. 2012, 3 C 32.11 Rn 34, 39 f.; OLG Düsseldorf 16. 12. 2015, Verg 25/15 Rn 45 ff.

²⁰⁷ VwGH 1. 7. 2010, 2006/04/0139; OLG Düsseldorf 19. 6. 2013, Verg 8/13, Rn 21; vgl. OLG Celle 24. 2. 2015, 13 Verg 1/15, Rn 94, 105; OLG Düsseldorf 21. 10. 2015, Verg 28/14, Rn 74 f.; OLG Düsseldorf 22.11.2017, VII-Verg 16/17, Rn. 20; vgl. Göllles in *Göllles/Casati*, BVergG 2018 § 105 Rz 13, 21.

²⁰⁸ vgl. VwGH 27. 2. 2019, Ra 2017/04/0054, Rn 15; vgl. *Heid/Kondert* in *Heid Schiefer Rechtsanwälte / Preslmayr Rechtsanwälte* (Hrsg.), Handbuch Vergaberecht² (2015) Rz 1210 ff.

²⁰⁹ §§ 20, 91 BVergG 2018; vgl. *Tretzmüller*, Handbuch Softwarerecht¹ Rz 1063 ff.

und Messmethodik, die als Best Practice anerkannt sind.²¹⁰ In Kombination mit der UfAB-Methodik lassen sich differenzierte SLA-Niveaus überszenariobasierte Preisblätter objektiv gegenüberstellen. Während die deutsche Vergabepraxis qualitative Vorzüge – wie etwa verkürzte Wiederherstellungszeiten – häufig über monetäre Äquivalente direkt in die Wirtschaftlichkeitsberechnung einbezieht, beschränkt sich die österreichische Handhabung oft auf das binäre Abprüfen von Mindestvorgaben.²¹¹

4.3.5. Vertragliche Absicherung und Durchsetzbarkeit

Die vergaberechtliche Bedeutung der SLAs als Wertungsmaßstab findet ihre notwendige Fortsetzung in der vertraglichen Absicherung. Während die öffentlich auftraggebende Stelle im Vergabeverfahren die Vergleichbarkeit sicherstellt, muss das Vertragswerk die tatsächliche Durchsetzbarkeit der versprochenen Service-Niveaus garantieren. Hierbei sind spezifische nationale Nuancen in der rechtlichen Einordnung zu beachten: Da SaaS-Verträge dogmatisch überwiegend mietvertragliche Elemente aufweisen, sind die anbietenden Unternehmen sowohl nach deutschem als auch nach österreichischem Recht gesetzlich verpflichtet, die Software während der Vertragslaufzeit in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu erhalten.²¹² Die Pflicht zur Störungs- und Mängelbeseitigung besteht eigenständig neben vereinbarten Service Levels; Dienstgutschriften kompensieren nur Verfügbarkeitsunterschreitungen, beseitigen den Mangel aber nicht. In der Gestaltung der Vergabeunterlagen muss daher das Verhältnis von pauschalierten Pönalen – die als verschuldensunabhängige Kompensation für das Unterschreiten der Service Levels fungieren – zu den gesetzlichen Minderungs- und Schadensersatzansprüchen eindeutig geregelt werden.²¹³

Service-Level-Agreements erweisen sich somit als unverzichtbares Instrument zur

²¹⁰ Ministerium für Digitales und Staatsmodernisierung, EVB-IT Cloud – Vertrag, https://www.digitale-verwaltung.de/SharedDocs/downloads/Webs/DV/DE/digitale-loesungen/it-einkauf/evb-it-bvb/basisvertraege/cloud/it-cloud-vertrag.docx?__blob=publicationFile&v=2 (abgerufen am 2. 1. 2026); vgl. Hunzinger, CR 2023, 349 (351 ff).

²¹¹ Ministerium für Digitales und Staatsmodernisierung, EVB-IT Cloud – Vertrag, https://www.digitale-verwaltung.de/SharedDocs/downloads/Webs/DV/DE/digitale-loesungen/it-einkauf/evb-it-bvb/basisvertraege/cloud/it-cloud-vertrag.docx?__blob=publicationFile&v=2 (abgerufen am 2. 1. 2026); ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html> (abgerufen am 1. 1. 2026); vgl. methodisch hierzu Hunzinger, CR 2023, 349 (353).

²¹² BGH 15. 11. 2006 – XII ZR 120/04; vgl. auch Tretzmüller, Handbuch Softwarerecht¹ Rz 1063; für Österreich vgl. Rassi in Bydlinski/Perner/Spitzer (Hrsg.), ABGB: Kommentar zum ABGB⁷ (2023), § 1096 Rz 1, 3; für Deutschland vgl. Münch in Herberger/Martinek/Rüßmann/Weth/Würdinger (Hrsg.), jurisPK-BGB¹⁰ §353 Rz 172 (Stand 29. 8. 2024, juris.de)

²¹³ vgl. Bischof/Intveen, ITRB 2022, 157 (160 f); Hunzinger, CR 2023, 349 (351 ff); vgl. Hoeren/Pinelli, Rn 376 f.

qualitativen Steuerung von SaaS-Beschaffungen. Sie übersetzen abstrakte Leistungsanforderungen in messbare, überprüfbare Parameter und schaffen damit die Grundlage für eine objektive Angebotsbewertung und eine rechtssichere Vertragsdurchführung.²¹⁴

4.4. Risikominimierung durch vertragliches Exit-Management

Die in Kapitel 3.2 analysierte Problematik des Vendor-Lock-in erfordert eine proaktive vertragliche Absicherung bereits in der Ausschreibungsphase. Die Reversibilität der Leistungserbringung und die Gewährleistung eines reibungslosen Exit-Managements stellen im Kontext von SaaS keine operativen Randaspekte dar, sondern fungieren als essenzielle, eigenständige Leistungsbestandteile, die bereits im Vergabeverfahren konstitutiv zu berücksichtigen sind.²¹⁵

4.4.1. Exit-Management als vergaberechtliche Notwendigkeit

Da Cloud-Verträge dogmatisch als Dauerschuldverhältnisse zu qualifizieren sind, entsteht durch die Speicherung und Verarbeitung von Daten in der Sphäre der anbietenden Unternehmen eine strukturelle Abhängigkeit.²¹⁶ Um die vergaberechtlich gebotene Vergleichbarkeit der Angebote zu gewährleisten und unkalkulierbare Kostenrisiken für die öffentlich auftraggebende Stelle zu minimieren, ist eine präzise technische und juristische Spezifikation der Exit-Leistungen in der Leistungsbeschreibung sowie deren methodische Einbeziehung in die TCO-Betrachtung zwingend erforderlich.²¹⁷

Die bloße theoretische Möglichkeit der Datenherausgabe, wie sie in vielen Standard-AGB pauschal zugesichert wird, genügt nicht, um die tatsächliche Portabilität und Interoperabilität in der Verwaltungspraxis sicherzustellen. Vielmehr muss die Leistungsbeschreibung den Prozess der Rückabwicklung so eindeutig und erschöpfend festlegen, dass er operativ durchführbar und vor allem kalkulierbar ist.²¹⁸

4.4.2. Technische Anforderungen an die Datenportabilität

Zentrales Element ist die Definition des Exportumfangs. Es reicht nicht aus, lediglich die Herausgabe der Stamm- und Bewegungsdaten zu fordern; vielmehr müssen auch die zugehörigen Metadaten, Protokolldaten und Konfigurationsparameter umfasst sein,

²¹⁴ vgl. zur detaillierten Regelung von SLAs und Verfügbarkeit in einem Standardvertragswerk *Möglich in Taeger/Pohle* Rz 188 ff.

²¹⁵ *Claßen/Koch/Müller*, MMR 2020, 723 (725); *Heydn*, MMR 2020, 435 (436); *Bischof/Intveen*, ITRB 2022, 157 (161 f); *Hunzinger*, CR 2023, 349 (350 f).

²¹⁶ vgl. *Möglich in Taeger/Pohle* Rz 194.

²¹⁷ vgl. *Tretzmüller*, ZIIR 2019, 255 (256 f); vgl. *Hunzinger*, CR 2023, 349 (351).

²¹⁸ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726).

soweit diese für die Weiternutzung, die revisionssichere Archivierung oder die Migration in ein Folgesystem technisch erforderlich sind.²¹⁹

Korrespondierend hierzu ist die Vorgabe offener, maschinenlesbarer und dokumentierter Exportformate wie CSV, JSON oder XML unabdingbar. Diese Formate zeichnen sich dadurch aus, dass sie herstellerunabhängig und standardisiert sind, wodurch die Daten ohne proprietäre Barrieren in Folgesysteme migriert werden können. Die Nutzung herstellereigener, nicht-standardisierter Formate führt zu immensen Migrationsaufwänden und verzerrt den Wettbewerb bei einer Neuausschreibung. Sie versetzt die öffentliche Hand in eine Zwangslage: Die Wiederbeauftragung des bestehenden Vertragspartners oder eine teure Migration sind dann die einzigen Alternativen.²²⁰

Zusätzlich sind verbindliche Bereitstellungsfristen von beispielsweise 60 oder 90 Tagen nach Vertragsbeendigung sowie Löschkonzepte zu vereinbaren.²²¹ So wird gewährleistet, dass sämtliche Daten nach der Migration datenschutzkonform und unwiederbringlich aus den Systemen des vormaligen Dienstleistungsunternehmens entfernt werden.²²² Zudem sind die Mitwirkungspflichten seitens der Anbietenden im Exit-Fall konkret auszugestalten, etwa durch fest vereinbarte Personentage-Kontingente zur Unterstützung der Migration oder durch verbindliche Einheitspreise. Solche Regelungen verhindern, dass die beauftragte Seite in der Exit-Phase eine monopolartige Stellung zu Lasten der öffentlichen Hand ausnutzt.²²³

4.4.3. *Ökonomische Dimension: Exit-Kosten in der TCO-Bewertung*

Aufbauend auf der in Kapitel 3.2 dargestellten ökonomischen Problematik strategischer Mischkalkulationen ist die Einbeziehung der Exit-Kosten in die Wirtschaftlichkeitsbewertung zwingend erforderlich.²²⁴ Aus dieser ökonomischen Problematik resultiert vergaberechtlich die zwingende Pflicht zu einer TCO-orientierten Bewertungsmethodik.²²⁵ Der unionsrechtliche Transparenzmaßstab verlangt zwingend, dass aus den Vergabeunterlagen klar hervorgeht, welche Kostenbestandteile in die Wertung einfließen und wie diese gewichtet werden. Unklare Bewertungslogiken, die keine

²¹⁹ vgl. Claßen/Koch/Müller, MMR 2020, 723 (724 f); Heydn, MMR 2020, 435 (436); Hunzinger, CR 2023, 349 (350).

²²⁰ vgl. Heydn, MMR 2020, 435 (438); Hunzinger, CR 2023, 349 (352).

²²¹ vgl. Möglich in Taeger/Pohle Rz 194 ff.

²²² Claßen/Koch/Müller, MMR 2020, 723 (725).

²²³ vgl. Hunzinger, CR 2023, 349 (352); Möglich in Taeger/Pohle Rz 194 ff.

²²⁴ Möglich in Taeger/Pohle Rz 194 ff.

²²⁵ Claßen/Koch/Müller, MMR 2020, 723 (726 f); Hunzinger, CR 2023, 349 (352).

verlässliche Prognose der Gesamtkosten erlauben, sind unzulässig und angreifbar.²²⁶

Die in Kapitel 4.2.2 entwickelte Methodik der szenariobasierten Kostenabfrage findet bei der Bewertung von Exit-Kosten ihre spezifische Anwendung.²²⁷ Ein typisches Referenzszenario bildet etwa der vollständige Datenexport und die Migration nach einer Laufzeit von 48 Monaten ab.²²⁸ Durch die einheitliche Bepreisung dieser Exit-Leistungen werden die in Kapitel 3.2 identifizierten Risiken strategischer Mischkalkulationen effektiv adressiert.

4.4.4. Rechtsvergleichende Perspektive: Unterschiedliche Lösungsansätze

Im rechtsvergleichenden Blick zeigen sich trotz der gemeinsamen unionsrechtlichen Basis signifikante Unterschiede in der regulatorischen Verankerung und praktischen Handhabung zwischen Österreich und Deutschland. Die Grundstruktur dieses Vergleichs – Deutschland mit institutionalisierter Standardisierung, Österreich mit prozessualer Flexibilität – wurde bereits in Kapitel 2.3.3 dargestellt und wird in Kapitel 5 umfassend analysiert. An dieser Stelle werden nur die spezifischen Unterschiede im Bereich des Exit-Managements hervorgehoben.

In Österreich existiert keine spezifische vergaberechtliche Norm, die den Datenexport explizit regelt. Die Verpflichtung zur Festlegung von Reversibilitätsanforderungen leitet sich vielmehr dogmatisch aus der Systematik des BVergG 2018 ab. Aus vergaberechtlicher Sicht einerseits verlangt das Bestimmtheitsgebot gemäß § 104 BVergG 2018, dass die Leistungsbeschreibung für den gesamten Kreis der Teilnehmenden gleichermaßen verständlich ist. Da der Exit ein wesentlicher Bestandteil der Leistung ist, führt das Fehlen von Exit-Regelungen zur Unbestimmtheit des Leistungsgegenstandes und damit zu einer möglichen Rechtswidrigkeit der Ausschreibung.²²⁹

Auf der anderen Seite ist in diesem Zusammenhang auch die zivilrechtliche Einbettung von Bedeutung: Da SaaS-Verträge in Österreich überwiegend als Bestandverträge gemäß §§ 1090 ff ABGB qualifiziert werden, trifft die anbietende Seite eine umfassende Pflicht zur Aufrechterhaltung der Gebrauchstauglichkeit der Software. Bleibt der Exit vertraglich ungeregelt, besteht das Risiko, dass die anbietende Partei Daten zurückhält

²²⁶ EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 87 f

²²⁷ ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 55 ff (abgerufen am 1. 1. 2026).

²²⁸ Möglich in *Taeger/Pohle* Rz 194 ff; vgl. EVB-IT Cloudvertrag (2022) Nr. 3.2.3.

²²⁹ vgl. *Schima*, *ecolex* 2024, 197 (199 f); vgl. *Heid/Kondert* in *Heid Schiefer Rechtsanwälte / Preslmayr Rechtsanwälte* Rz 1174 ff.

oder den Datenexport nur gegen überhöhte Entgelte zulässt eine solche faktische „Pfandstellung“ der Daten kann unter dem Gesichtspunkt der Sittenwidrigkeit gemäß § 879 ABGB problematisch sei. Um solche negativen Szenarien während der Vertragsdurchführung bzw am Ende zu verhindern, ist es bereits im Vergabeverfahren zwingend erforderlich eine präventive Lösung durch klare Leistungsbeschreibungen sicherzustellen.²³⁰

Demgegenüber ist die Handhabung in Deutschland durch eine stärkere Standardisierung und eine spezifische AGB-rechtliche Diskussion geprägt. Mit den EVB-IT Cloud stehen amtliche Vertragsmuster zur Verfügung, die Reversibilität und Datenportabilität detailliert regeln.²³¹ Dies führt dazu, dass die Anforderungen an die Leistungsbeschreibung gemäß § 31 VgV in der Praxis oft effizient durch den Verweis auf diese Standardbedingungen erfüllt werden.²³² Zudem spielt in Deutschland die AGB-Kontrolle im Business-to-Business-Bereich, geregelt in §§ 307 ff BGB, eine zentrale Rolle bei der Bewertung von Exit-Klauseln. Anders als im Geschäftsverkehr mit Verbraucher:innen wird hier zwar eine höhere Professionalität der Vertragsparteien unterstellt, dennoch unterliegen standardisierte Klauseln auch zwischen Unternehmen einer strengen Inhaltskontrolle.²³³ Die Rechtsprechung tendiert dazu, Klauseln, die den Datenexport faktisch verhindern oder unverhältnismäßig erschweren, als unangemessene Benachteiligung zu werten, da sie den Vertragszweck gefährden.²³⁴ Methodisch flankiert die UfAB diesen Ansatz durch die explizite Empfehlung, Exit-Kosten in die Wertung einzubeziehen, was zu einer höheren Verbreitung standardisierter TCO-Matrizen im Vergleich zur österreichischen Praxis führt.²³⁵

4.4.5. *Synthese: Exit-Management als Wettbewerbsvoraussetzung*

In der Gesamtbetrachtung zeigt sich: Während in Österreich die Reversibilität primär als Frage der Leistungsbestimmtheit im Vergabeverfahren gelöst wird, greift in Deutschland ein Zusammenspiel aus standardisierten Vertragsmustern und AGB-

²³⁰ vgl. *Tretzmüller*, ZIIR 2019, 255 (257) unter Verweis auf die Bestandnehmereigenschaft.

²³¹ Ministerium für Digitales und Staatsmodernisierung, EVB-IT Cloud – Vertrag, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/evb-it-und-bvb/evb-it/evb-it-node.html> (abgerufen am 2. 1. 2026); EVB-IT-Cloud – AGB Z 13.2.

²³² vgl. *Hunzinger*, CR 2023, 349 (351 ff); *Möglich* in *Taeger/Pohle* Rz 194 f.

²³³ vgl. *Leßner/Gäntgen*, (Un)Wirksamkeit von B2B-AGB bei (internationalen) SaaS-Verträgen, KuR 2021, 766 (767 f).

²³⁴ vgl. *Möglich* in *Taeger/Pohle* Rz 195; vgl. BGH 16.1.1985 – VIII ZR 153/83, BGHZ 93, 252 (255).

²³⁵ ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 55 ff (abgerufen am 1. 1. 2026).

Kontrolle, um den Vendor-Lock-in effektiv zu verhindern. Unabhängig von der nationalen Dogmatik bleibt die *ex ante* definierte Exit-Strategie jedoch die zwingende Voraussetzung für eine rechtskonforme Wirtschaftlichkeitsprüfung.

Die in Kapitel 3.2 identifizierte Problematik des Vendor-Lock-in ist somit keine nachgelagerte Vertragsmodalität, sondern eine zwingende Prämisse für die Rechtmäßigkeit des gesamten Vergabeverfahrens. Nur wenn die öffentlich auftraggebende Stelle bereits in der Ausschreibungsphase klare Anforderungen an Reversibilität und Portabilität definiert und diese in die Wirtschaftlichkeitsbewertung einbezieht, kann sie sicherstellen, dass der Wettbewerb nicht nur bei der Erstbeschaffung, sondern auch bei künftigen Neuausschreibungen funktionsfähig bleibt.²³⁶

5. Rechtsvergleich Österreich vs. Deutschland: Standardisierung vs. Flexibilität

Die vorangegangenen Kapitel haben gezeigt, dass die vergaberechtlichen Herausforderungen bei SaaS-Beschaffungen – Vergleichbarkeit, Vendor-Lock-in und Datenschutz – in beiden Rechtsordnungen strukturell identisch sind. Beide Systeme basieren auf denselben unionsrechtlichen Vorgaben der Vergaberichtlinie 2014/24/EU und müssen die Grundsätze der Transparenz, Gleichbehandlung und des Wettbewerbs wahren. Dennoch haben sich in der praktischen Umsetzung fundamental unterschiedliche Lösungsstrategien herausgebildet: Deutschland setzt auf eine proaktive Standardisierung durch amtliche Vertragsmuster (EVB-IT Cloud)²³⁷, Österreich auf eine verfahrensmäßige Anpassungsfähigkeit durch einzelfallbezogene Leistungsbeschreibungen.²³⁸

Dieses Kapitel untersucht die strukturellen Unterschiede dieser beiden Ansätze und bewertet ihre jeweiligen Stärken und Schwächen im Hinblick auf Rechtssicherheit, Effizienz und Innovationsoffenheit. Dabei wird deutlich, dass beide Modelle dasselbe Ziel verfolgen – die Herstellung von Vergleichbarkeit und Transparenz bei dynamischen Cloud-Leistungen –, dieses jedoch mit unterschiedlichen Mitteln und unterschiedlichen Risikoprofilen erreichen.

²³⁶ vgl. *Möglich* in *Taeger/Pohle* Rz 194; vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (727) (zur Bedeutung von Regelungen über das Vertragsende und Migrationsunterstützung); *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 20 (zur Insolvenzproblematik und Datenherausgabe).

²³⁷ Zur Standardisierung durch das Vertragsmuster und die Anlagenhierarchie der EVB-IT Cloud vgl. *Möglich* in *Taeger/Pohle* Rz 156 ff; zur funktionalen Leistungsbeschreibung als Standardisierungsinstrument siehe ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 173 f (abgerufen am 1. 1. 2026).

²³⁸ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (725).

5.1. Deutschland: Institutionalisierte Lösung durch EVB-IT Cloud und UfAB

Die deutsche Vergabep Praxis bei IT-Beschaffungen ist seit den frühen 2000er Jahren durch ein hohes Maß an Standardisierung geprägt. Mit den „Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen“ (EVB-IT)²³⁹ hat das Bundesministerium des Innern ein umfassendes System von Musterverträgen geschaffen, das zwischen öffentlicher Hand und IT-Wirtschaft ausgehandelt wurde und seither kontinuierlich weiterentwickelt wird. Diese Standardisierung wurde am 1. März 2022 durch die EVB-IT Cloud auf Cloud-Leistungen ausgedehnt und durch die UfAB methodisch flankiert.²⁴⁰

Das Vertragsmuster der EVB-IT Cloud adressiert systematisch die zentralen Regelungsfelder von Cloud-Beschaffungen: Leistungsgegenstand und -ort, Datenschutz und IT-Sicherheit, Verfügbarkeit und Störungsmanagement, Pflichten beim Vertragsende einschließlich Migration und Portabilität, Nutzungsrechte, Unterauftragnehmer, Vergütung, Mängelrechte, Haftung und Kündigung.²⁴¹ Durch diese umfassende Abdeckung wird der individuelle Gestaltungsaufwand der Vergabestellen erheblich reduziert. Anstatt für jede Beschaffung ein vollständig neues Vertragswerk zu entwickeln, können die Behörden auf ein erprobtes, rechtssicheres Grundgerüst zurückgreifen, das lediglich an die spezifischen Anforderungen des konkreten Projekts anzupassen ist.²⁴²

Besonders bemerkenswert ist die in den EVB-IT Cloud vorgesehene kontrollierte Öffnung für die AGB der anbietenden Unternehmen. Während die Einbeziehung privatrechtlicher AGB bei öffentlichen Vergaben traditionell ausgeschlossen ist, lässt das Vertragsmuster in eng gesteuerter Form eine nachrangige Einbeziehung über Anhang I bzw. Nr. 1.2.4 zu. Die Anwendungshinweise begründen diesen Paradigmenwechsel wie folgt: Diese wird mit dem hohen Standardisierungsgrad von Cloud-Leistungen begründet: Um umfangreiche, technisch hochgradig standardisierte Portfolios adäquat abzubilden, ist ein Rückgriff auf Bedingungen der Anbietenden oft unumgänglich. Diese

²³⁹ Ministerium für Digitales und Staatsmodernisierung, EVB-IT-Archiv, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/evb-it-und-bvb/evb-archiv/evb-archiv.html> (abgerufen am 31. 1. 2026).

²⁴⁰ IT-Recht Kanzlei GmbH & Co. KG, Keller-Stoltenhoff Elisabeth, Geschichte und Zukunft der EVB-IT, Blogbeitrag vom 8. 6. 2026, https://www.it-recht-kanzlei.de/evb-it-Geschichte_und_Zukunft.html (abgerufen am 27. 12. 2025).

²⁴¹ vgl. *Möglich* in Taeger/Pohle Rz 161 ff.

²⁴² vgl. *Möglich* in Taeger/Pohle Rz 156 ff; Hunzinger, CR 2023, 349 (352).

Öffnung ist jedoch kein Blankoscheck, sondern wirft komplexe Abgrenzungs-, Prioritäts- und AGB-Kontrollfragen auf. Diese bewusste Abweichung vom Dogma des AGB-Ausschlusses ist der systematische Dreh- und Angelpunkt, um hochgradig standardisierte, aber komplexe Cloud-Leistungen vergaberechtlich handhabbar zu machen.²⁴³

Die vergaberechtliche Bedeutung dieser Konstruktion liegt in der Herstellung von Vergleichbarkeit: Indem alle Bietenden ihre Leistungen auf Basis desselben vertraglichen Rahmens kalkulieren, werden strukturelle Bewertungsverzerrungen minimiert. Die Vergabestelle muss nicht mehr befürchten, dass unterschiedliche Vertragsmodelle – etwa hinsichtlich Haftungsobergrenzen, Kündigungsfristen oder Exit-Leistungen – die Angebote faktisch unvergleichbar machen.²⁴⁴ Zugleich wird durch die standardisierte Regelung von Datenschutz- und Sicherheitsanforderungen sichergestellt, dass alle Angebote ein Mindestniveau an DSGVO-Konformität aufweisen.²⁴⁵

Während die EVB-IT Cloud das vertragliche Rahmenwerk für die Durchführungsphase bereitstellen, adressiert die UfAB die Vergabephase selbst. Sie bietet öffentlichen Stellen einen strukturierten Leitfaden für den gesamten Beschaffungsprozess – von der Bedarfsanalyse über die Leistungsbeschreibung bis zur Zuschlagsermittlung. Besonders relevant für SaaS-Beschaffungen sind die standardisierten Bewertungsmatrizen, die es ermöglichen, komplexe IT-Angebote objektiv vergleichbar zu machen.²⁴⁶

Die UfAB operationalisiert dabei die in Kapitel 4.2 entwickelte Methodik der szenariobasierten Kostenabfrage: Sie gibt vor, wie Referenzszenarien zu definieren sind, welche Kostenbestandteile in die TCO-Betrachtung einfließen müssen und wie die Umrechnung unterschiedlicher Preismodelle in einen vergleichbaren Gesamtwert zu erfolgen hat.²⁴⁷ Durch diese Standardisierung wird verhindert, dass Vergabestellen bei jeder Beschaffung das methodische Rad neu erfinden müssen. Zugleich wird die Rechtssicherheit erhöht, da die UfAB als anerkannte *Best Practice* gilt und ihre Anwendung im Nachprüfungsverfahren als Indiz für eine ordnungsgemäße Verfahrensgestaltung gewertet wird.²⁴⁸

²⁴³ vgl. *Möglich* in *Taeger/Pohle* Rz 160; AT-Vergleich: Keine vergleichbare Öffnung.

²⁴⁴ vgl. *Lampert* in *Burgi/Dreher/Opitz*, Beck'scher Vergaberechtskommentar Bd 14 § 121 GWB Rz 9 (Stand 2022, beck-online.de); *Zimmermann* in *Summa/Schneevogl*, jurisPK-Vergaberecht⁷ § 121 GWB Rz 30

²⁴⁵ vgl. *Möglich* in *Taeger/Pohle* Rz 184 ff.

²⁴⁶ vgl. *Möglich* in *Taeger/Pohle* Rz 7 ff, 20 ff, 160 f; *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff.

²⁴⁷ ZIB, Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html>, 59 ff (abgerufen am 1. 1. 2026).

²⁴⁸ *Hürthen*, Vergabeblog.de, Unterlage für Ausschreibung und Bewertung von IT-Leistungen: Die UfAB

EVB-IT Cloud und UfAB wirken als komplementäres System für einen durchgängigen Beschaffungsprozess: Während die UfAB die Methode für die Vergabephase – insbesondere Leistungsbeschreibung und Zuschlagsermittlung – bereitstellt, stellen die EVB-IT Cloud das Rahmenwerk für die Vertragsphase dar. Diese Verzahnung gewährleistet, dass die in der Ausschreibung definierten Anforderungen nahtlos in die vertragliche Ausgestaltung überführt werden.²⁴⁹ Die Vergabestelle kann sich darauf verlassen, dass die in der UfAB vorgesehenen Bewertungskriterien – etwa zu Verfügbarkeit, Sicherheitsniveau oder Exit-Leistungen – in den EVB-IT Cloud bereits vertraglich operationalisiert sind.²⁵⁰

Für die deutsche Vergabepaxis bedeutet diese Standardisierung eine erhebliche Entlastung: Die individuelle Gestaltungslast wird reduziert, die Transparenz und Rechtssicherheit erhöht.²⁵¹ Vergabestellen müssen nicht mehr befürchten, durch unklare Leistungsbeschreibungen oder intransparente Bewertungsmethoden gegen das Transparenzgebot zu verstoßen. Diese Standardisierung schafft zudem einheitliche Erwartungshaltungen, die Angebotskalkulationen erleichtern und Wettbewerbsintensität steigern.²⁵²

Die institutionalisierte Lösung ist jedoch nicht ohne Nachteile. Die EVB-IT Cloud sind hochkomplex und setzen ein erhebliches juristisches und technisches Verständnis voraus.²⁵³ Kleinere Vergabestellen ohne spezialisierte IT-Beschaffungsabteilungen können mit der Anwendung überfordert sein.²⁵⁴ Zudem besteht das Risiko einer gewissen Starrheit: Während standardisierte Muster Rechtssicherheit bieten, können sie innovative Geschäftsmodelle oder atypische Leistungskonstellationen nur begrenzt abbilden.²⁵⁵ Die kontrollierte Öffnung für AGB der Anbietenden versucht dieses Spannungsfeld zu lösen, schafft aber neue Komplexität bei der Prüfung der Vertragshierarchie und der AGB-Kontrolle.²⁵⁶

2018 – Oldie but Goldie (29.6.2023), <https://vergabeblog.de/2023-06-29/unterlage-fuer-ausschreibung-und-bewertung-von-it-leistungen-die-ufab-2018-oldie-but-goldie/> (abgerufen am 1. 2. 2026).

²⁴⁹ vgl. *Möglich* in *Taeger/Pohle* Rz 7 ff, 20 ff, 160 f; *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff.

²⁵⁰ vgl. *Hunzinger*, CR 2023, 349 (351 ff, 357); *Möglich* in *Taeger/Pohle* Rz 188 ff, 194 ff.

²⁵¹ vgl. *Möglich* in *Taeger/Pohle* Rz 160.

²⁵² vgl. EuGH C-45/87, *Kommission/Irland*, ECLI:EU:C:1988:435, Rn 22 f; *Hunzinger*, CR 2023, 349 (350).

²⁵³ *Hunzinger*, CR 2023, 349 (353).

²⁵⁴ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

²⁵⁵ *Möglich* in *Taeger/Pohle* Rz 160.

²⁵⁶ Schwientek, Die Vergabe von Cloud-Leistungen (EVB-IT Cloud) (01/2023), Leinemann Partner Rechtsanwälte: <https://www.leinemann-partner.de/newsletter/neues-zum-vergaberecht-01-2023/die->

Dennoch überwiegen aus Sicht der Rechtssicherheit und Effizienz die Vorteile: Die deutsche Vergabep Praxis verfügt mit EVB-IT Cloud und UfAB über ein erprobtes, rechtssicheres Instrumentarium, das die in Kapitel 3 identifizierten Herausforderungen – Vergleichbarkeit, Vendor-Lock-in und Datenschutz – systematisch adressiert und operationalisiert.²⁵⁷

5.2. Österreich: Prozessuale Lösung durch Einzelfallgestaltung

Die österreichische Vergabep Praxis steht in einem deutlichen Kontrast zum deutschen Standardisierungsansatz. Wie bereits in Kapitel 2.3.3 dargelegt, fehlt in Österreich ein Standardvertragswerk für IT-Beschaffungen, das spezifisch auf die Besonderheiten von Cloud-Services und SaaS-Lösungen zugeschnitten ist. Zwar existieren standardisierte Vertragsbedingungen wie die ÖNORMEN, doch erweisen sich diese aufgrund ihres Fokus auf Bereiche wie das klassische Bauwesen für die komplexen Anforderungen digitaler Dienstleistungen als weitgehend ungeeignet.²⁵⁸

Anstatt auf prädefinierte Vertragsmuster zurückzugreifen, begegnet Österreich der Komplexität von SaaS-Beschaffungen primär auf der Ebene der verfahrensrechtlichen Gestaltung.²⁵⁹ Das BVergG 2018 bietet mit § 104 Abs 2 die Möglichkeit der funktionalen Leistungsbeschreibung: Die Leistung muss nicht in jedem technischen Detail vollständig spezifiziert sein, sondern kann als hinreichend genaue, zu lösende Aufgabenstellung definiert werden.²⁶⁰ Dies ermöglicht es den Vergabestellen, den Fokus weg von starren technischen Vorgaben hin zu den angestrebten Leistungs- und Funktionszielen zu verschieben, was insbesondere der technologischen Dynamik von SaaS-Lösungen gerecht wird.²⁶¹

Diese methodische Weichenstellung verlagert die Verantwortung für die konkrete technologische Lösungsspezifikation bewusst in den Wettbewerb. Dies bietet den Vorteil, Innovationen des Marktes optimal auszuschöpfen, fordert von der ausschreibenden Stelle jedoch eine hohe fachliche Kompetenz: Es gilt, Funktionsziele so präzise zu

[vergabe-von-cloud-leistungen-evb-it-cloud/](#) (abgerufen am 21. 1. 2026)

²⁵⁷ vgl. *Möglich* in *Taeger/Pohle* Rz 160; *Hunzinger*, CR 2023, 349 (352 f).

²⁵⁸ vgl. PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

²⁵⁹ vgl. *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 29 ff; *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 25 f; ergänzend zu den erhöhten Anforderungen an die Beschaffungskompetenz bei fehlenden Standardmustern *Claßen/Koch/Müller*, MMR 2020, 723 (724 ff).

²⁶⁰ vgl. *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 19 ff; *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 25 f.

²⁶¹ vgl. *Gölles* in *Gölles/Casati*, BVergG 2018 § 105 Rz 12.

definieren, dass sie einerseits technologieneutral bleiben, um den Wettbewerb nicht einzuschränken, und andererseits eine objektive Vergleichbarkeit der eingehenden Angebote sicherstellen.²⁶²

Dieser Mangel an Standardisierung setzt erhebliche juristische und technische Beschaffungskompetenz im Falle einer Neubeschaffung voraus. Da diese Expertise in der Breite der Verwaltung nicht flächendeckend vorausgesetzt werden kann, erhöht sich das Risiko für intransparente oder faktisch diskriminierende Ausschreibungsvorgaben signifikant. Die Komplexität von SaaS-Produkten, die durch dynamische Preis- und Leistungsmodelle sowie kurze Innovationszyklen geprägt sind, verschärft diese Problematik zusätzlich.²⁶³

In Ermangelung klarer vertraglicher Leitplanken treten Risiken wie die digitale Souveränität sowie der Vendor-Lock-in-Effekt deutlich zutage. Ohne standardisierte Ausstiegs- und Migrationsstrategien drohen öffentliche Vergabestellen langfristig ihre operative Handlungsfähigkeit einzubüßen.²⁶⁴ Die in Kapitel 4.4 entwickelten Anforderungen an Exit-Management und Datenportabilität müssen in Österreich für jede einzelne Ausschreibung individuell formuliert und in die Leistungsbeschreibung integriert werden.²⁶⁵

Um die Vergleichbarkeit heterogener SaaS-Preismodelle herzustellen, behilft sich die österreichische Praxis mit der Vorgabe strikter Referenzszenarien. Die ausschreibenden Stellen definieren fiktive Nutzungsmuster – etwa „500 User, 1 TB Speicher, 100 GB Datentransfer/Monat“ –, die zwingend zu bepreisen sind. Dies transformiert heterogene Abrechnungsmodelle in einen vergleichbaren Gesamtpreis, ohne den Markt auf ein spezifisches Geschäftsmodell einzuengen.²⁶⁶

Diese Methodik entspricht der TCO-Bewertung, muss jedoch – anders als in Deutschland mit der UfAB – für jede Beschaffung individuell entwickelt werden. Die Vergabestelle trägt das volle Risiko, dass die gewählten Szenarien die tatsächliche Nutzung

²⁶² vgl. *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 29 ff; *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 25 f; ergänzend zu den erhöhten Anforderungen an die Beschaffungskompetenz bei fehlenden Standardmustern *Claßen/Koch/Müller*, MMR 2020, 723 (724 ff).

²⁶³ vgl. PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

²⁶⁴ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (726).

²⁶⁵ vgl. *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 29 ff; *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 25 f; ergänzend zu den erhöhten Anforderungen an die Beschaffungskompetenz bei fehlenden Standardmustern *Claßen/Koch/Müller*, MMR 2020, 723 (724 ff).

²⁶⁶ Zur Technologieneutralität vgl. § 106 Abs 1 BVergG 2018; *Gölles* in *Gölles/Casati*, BVergG 2018 § 106 Rz 1 ff.

nicht adäquat abbilden oder dass die Umrechnungsformeln zu systematischen Verzerrungen führen. Ohne standardisierte Bewertungsmatrizen fehlt zudem die Orientierung an einer anerkannten Best Practice, was die Angreifbarkeit der Zuschlagsentscheidung im Nachprüfungsverfahren erhöht.²⁶⁷

Die österreichische Lösung bietet zweifellos eine höhere Flexibilität: Vergabestellen können die Leistungsbeschreibung präzise auf die spezifischen Anforderungen des konkreten Projekts zuschneiden, ohne durch standardisierte Muster eingeschränkt zu sein. Dies ermöglicht eine optimale Anpassung an atypische Bedarfslagen oder innovative Geschäftsmodelle, die in standardisierten Vertragsmustern möglicherweise nicht abgebildet sind.²⁶⁸

Diese Flexibilität hat jedoch ihren Preis: Sie verlagert die Last der präzisen Definition von Zielen und Mindestanforderungen vollständig auf die jeweilige Vergabestelle, die für jede einzelne Ausschreibung einen rechtssicheren Rahmen schaffen muss.²⁶⁹ Ohne die Unterstützung durch prädefinierte Klauselwerke müssen die Vergabestellen sicherstellen, dass die Leistungsbeschreibung dennoch den strengen unionsrechtlichen und nationalen Anforderungen an Bestimmtheit und Transparenz genügt. Dies erfordert ein überdurchschnittliches Maß an Vergabe- und IT-Kompetenz, das in der Praxis nicht immer vorhanden ist.²⁷⁰

Die Folgen dieser fehlenden Standardisierung zeigen sich in der österreichischen Vergabepraxis deutlich. Der österreichische Rechnungshof (RH) kritisiert wiederholt unzureichende vertragliche Regelungen zu Leistungsumfang, Preisgleitklauseln und Exit-Regelungen.²⁷¹ Die Auftragsverhältnisse seien durch kontinuierlich steigende Wartungs- und Lizenzkosten gekennzeichnet, wobei die laufenden Kosten die

²⁶⁷ vgl Art 67 Abs 2 lit b RL 2014/24/EU; § 92 iVm § 2 Z 23 BVergG 2018; zur Erforderlichkeit vorher bekannt gemachter Bewertungsmaßstäbe und zur Vergleichbarkeit der Angebote Schrotz/Zdanowiecki, CR 2015, 485 (486 f); CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 38 f (abgerufen am 21. 1. 2026).

²⁶⁸ vgl Claßen/Koch/Müller, MMR 2020, 723 (725).

²⁶⁹ vgl Gölles in Gölles/Casati, BVergG 2018 § 106 Rz 6, 9f.

²⁷⁰ vgl PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

²⁷¹ Rechnungshof Österreich (RH), Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, [Bericht des Rechnungshofes: Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium](#), 5.1 ff, 6.1 ff (abgerufen am 31. 12. 2025); RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, 7.1, 8.1, 17 (abgerufen am 31. 12. 2025).

Einmalkosten nach wenigen Jahren um ein Vielfaches übersteigen. Zugleich würden bestehende Bindungen an spezifische Anbietende und Infrastrukturen fortgeschrieben und vertraglich weiter verfestigt, ohne dass tragfähige Alternativen systematisch ausgelotet werden.²⁷²

Diese Praxis führt zu einer dauerhaften Zementierung technologischer Pfadabhängigkeiten, die den vergaberechtlichen Grundsatz des Wettbewerbs sowie die IT-Souveränität der öffentlichen Hand zunehmend untergraben.²⁷³ Mangels standardisierter Muster greifen Vergabestellen mitunter auf unpassende Vertragsentwürfe zurück, was angesichts heterogener Marktbedingungen rasch zu Vergabeunterlagen führt, die andere Marktakteure diskriminieren und bestehende Vendor-Lock-in-Effekte verstärken.²⁷⁴

Die österreichische Lösung setzt auf Gestaltungsspielraum und einzelfallbezogene Gestaltung. Dies bietet Vorteile bei atypischen Bedarfslagen, erhöht jedoch das Risiko intransparenter oder diskriminierender Ausschreibungen erheblich. Ohne die Unterstützung durch standardisierte Vertragsmuster und Bewertungsmatrizen sind österreichische Vergabestellen stärker gefordert, die in Kapitel 3 identifizierten Herausforderungen – Vergleichbarkeit, Vendor-Lock-in und Datenschutz – individuell zu lösen. Die Qualität der Beschaffung hängt damit maßgeblich von der Kompetenz der einzelnen Vergabestelle ab, was zu erheblichen Qualitätsunterschieden in der Verwaltungspraxis führt.²⁷⁵

5.3. Vergleichende Bewertung der Ansätze

Die vorstehende Analyse hat zwei fundamental unterschiedliche Lösungsstrategien offengelegt: Deutschland verfolgt mit EVB-IT Cloud und UfAB einen institutionalisierten, vertraglichen Ansatz, Österreich verfolgt verfahrensseitige Anpassungsfähigkeit durch funktionale Leistungsbeschreibungen.²⁷⁶ Beide Modelle dienen demselben

²⁷²RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, TZ 16.1–16.2, 27.1–27.2 (abgerufen am 31. 12. 2025).

²⁷³ RH, Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, 6.2; RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, 8.2, 16.2 (abgerufen am 31. 12. 2025).

²⁷⁴ vgl. Claßen/Koch/Müller, MMR 2020, 723 (724 f).

²⁷⁵PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

²⁷⁶ vgl. für Deutschland Möglich, in Taeger/Pöhle Rz 156 ff; für Österreich Gölles in Gölles/Casati, BVergG 2018 § 106 Rz 6, 9f.

vergaberechtlichen Ziel – der Herstellung von Transparenz und Vergleichbarkeit bei dynamischen SaaS-Leistungen²⁷⁷ –, unterscheiden sich jedoch fundamental in der Risikoverteilung und den Anforderungen an die Vergabekompetenz.

Der deutsche Ansatz bietet zweifellos die höhere Rechtssicherheit. Durch die Standardisierung von Vertragsklauseln und Bewertungsmethoden wird das Risiko vergaberechtlicher Fehler minimiert. Vergabestellen können sich darauf verlassen, dass die EVB-IT Cloud die wichtigen Aspekte – von Datenschutz über SLAs bis zu Exit-Leistungen – rechtssicher abdecken.²⁷⁸ Die UfAB operationalisiert zudem die Bewertungsmethodik, sodass die Gefahr intransparenter oder willkürlicher Zuschlagsentscheidungen reduziert wird.²⁷⁹

Demgegenüber bietet der österreichische Ansatz eine höhere Anpassungsmöglichkeit bei gleichzeitig geringerer Rechtssicherheit. Die funktionale Leistungsbeschreibung ermöglicht eine präzise Anpassung an spezifische Anforderungen, verlagert jedoch die volle Verantwortung für die rechtssichere Gestaltung auf die einzelne Vergabestelle.²⁸⁰ Ohne standardisierte Muster fehlt die Orientierung an einer anerkannten Best Practice, was die Angreifbarkeit der Ausschreibung im Nachprüfungsverfahren erhöht.²⁸¹

Der deutsche Standardisierungsansatz reduziert die individuelle Gestaltungslast erheblich. Vergabestellen müssen nicht für jede Beschaffung ein vollständig neues Vertragswerk entwickeln, sondern können auf erprobte Muster zurückgreifen.²⁸² Dies spart Zeit und Ressourcen und ermöglicht es auch kleineren Behörden, komplexe Cloud-Beschaffungen rechtssicher durchzuführen.²⁸³ Zugleich wird durch die einheitliche Behördenpraxis eine gewisse Markterwartung geschaffen, die den Wettbewerb intensiviert.²⁸⁴ Der österreichische Ansatz erfordert demgegenüber einen deutlich höheren Aufwand bei jeder einzelnen Beschaffung. Die Vergabestelle muss die Leistungsbeschreibung, die Bewertungsmethodik und die vertraglichen Regelungen individuell entwickeln und dokumentieren.²⁸⁵ Dies bindet erhebliche Ressourcen und setzt eine

²⁷⁷ Zum Zuschlag auf das wirtschaftlichste Angebot vgl § 127 Abs 1 GWB; § 91 Abs 1 BVergG 2018.

²⁷⁸ vgl *Möglich* in *Taeger/Pohle* Rz 161 ff.

²⁷⁹ Beschaffungsamt des Bundesministeriums des Innern Zentralstelle IT-Beschaffung (ZIB), Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, insb Teil 4.

²⁸⁰ 104 Abs 2 BVergG 2018.

²⁸¹ vgl *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f); *Nowak*, Das Bundesvergabegesetz 2018 aus Sicht der Neuen Institutionenökonomie (Dissertation TU Wien 2024), 45 ff.

²⁸² vgl *Möglich* in *Taeger/Pohle* Rz 161 ff; *Claßen/Koch/Müller*, MMR 2020, 723 (726).

²⁸³ vgl *Claßen/Koch/Müller*, MMR 2020, 723 (726).

²⁸⁴ vgl *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 21 f.

²⁸⁵ vgl RH, Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und

überdurchschnittliche Vergabe- und IT-Kompetenz voraus. Fehlt diese Expertise, steigt das Risiko fehlerhafter Ausschreibungen, was zu Nachprüfungsverfahren, Verzögerungen und im schlimmsten Fall zur Aufhebung des Vergabeverfahrens führen kann.²⁸⁶

Ein wesentlicher Vorteil des österreichischen Ansatzes liegt in der Innovationsoffenheit. Durch die funktionale Leistungsbeschreibung werden technologisch unterschiedliche Lösungsansätze gleichberechtigt in den Wettbewerb einbezogen.²⁸⁷ Die Vergabestelle definiert Schutzziele und Funktionsanforderungen, überlässt jedoch die konkrete technische Umsetzung den Bietenden.²⁸⁸ Dies ermöglicht es, innovative Geschäftsmodelle oder neuartige Sicherheitskonzepte – etwa CC oder BYOC – zu berücksichtigen, die in standardisierten Vertragsmustern möglicherweise noch nicht abgebildet sind.²⁸⁹

Der deutsche Ansatz ist demgegenüber stärker auf bewährte, etablierte Lösungen ausgerichtet. Die EVB-IT Cloud bilden den aktuellen Stand der Technik ab, können jedoch bei disruptiven Innovationen eine gewisse Verzögerung aufweisen, bis diese in die Standardmuster integriert werden.²⁹⁰

Ein wesentlicher Vorteil der EVB-IT Cloud liegt in der systematischen Adressierung datenschutzrechtlicher Anforderungen. Die Vertragsmuster enthalten vordefinierte Regelungen zu Auftragsverarbeitung, technischen und organisatorischen Maßnahmen, Drittlandtransfers und Auditrechten.²⁹¹ Dies stellt sicher, dass alle Angebote ein Mindestniveau an DSGVO-Konformität aufweisen und reduziert das Risiko datenschutzrechtlicher Verstöße erheblich.²⁹² In Österreich müssen diese Anforderungen für jede Beschaffung individuell in die Leistungsbeschreibung integriert werden.²⁹³ Dies erfordert ein fundiertes Verständnis der DSGVO und der in Kapitel 3.3 dargestellten *Schrems-II*-Problematik. Fehlt dieses Verständnis, besteht das Risiko, dass datenschutzrechtliche

Landwirtschaftsministerium, Reihe Bund 2024/16, [Bericht des Rechnungshofes: Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium](#), 28 ff (abgerufen am 31. 12. 2025).

²⁸⁶ RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, 43 ff (abgerufen am 31. 12. 2025).

²⁸⁷ § 103 BVergG 2018; ErläutRV BVergG 2018, 165 BlgNR 26. GP, 38.

²⁸⁸ vgl. *Schrotz/Zdanowiecki*, CR 2015, 485 (486).

²⁸⁹ European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version 18.06.2021, [edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf](#), Rn 79 ff (abgerufen am 3. 1. 2026).

²⁹⁰ vgl. *Hunzinger*, CR 2023, 349 (353 f).

²⁹¹ vgl. *Möglich* in *Taeger/Pohle* Rz 179 ff.

²⁹² vgl. *Bischof*, ITRB 2023, 165 (167).

²⁹³ vgl. *Bogendorfer* in *Knyrim*, Der DatKomm Art 28 DSGVO Rz 34 ff; *Tretzmüller*, Handbuch Software-recht¹ Rz 1063 ff.

Anforderungen unzureichend operationalisiert werden oder dass pauschale Ausschlüsse von Cloud-Lösungen vorgenommen werden, die vergaberechtlich nicht haltbar sind.²⁹⁴

Die vergleichende Bewertung zeigt, dass beide Ansätze komplementäre Stärken aufweisen. Deutschland gewinnt bei Rechtssicherheit und Effizienz durch reduzierte Gestaltungslast, Österreich bei Flexibilität und Innovationsoffenheit durch höhere lokale Beschaffungskompetenz.²⁹⁵ Gemeinsam ist beiden das Bestreben, die in Kapitel 3 identifizierten Herausforderungen – Vergleichbarkeit, Vendor-Lock-in und Datenschutz – zu bewältigen und Überraschungskosten bei Vertragsdurchführung durch eine ex ante festgelegte, transparente Bewertungsmethodik zu vermeiden.²⁹⁶

6. Kritische Analyse der österreichischen Praxis

Die vorangegangenen Kapitel haben die vergaberechtlichen Herausforderungen bei SaaS-Beschaffungen systematisch analysiert. Dabei wurde deutlich, dass sowohl das österreichische als auch das deutsche Vergaberecht grundsätzlich über die notwendigen Instrumente verfügen, um diese Herausforderungen zu bewältigen. Die entscheidende Frage ist jedoch, ob diese Instrumente in der Verwaltungspraxis auch tatsächlich sachgerecht angewendet werden. Dieses Kapitel widmet sich der kritischen Analyse der österreichischen Beschaffungspraxis bei SaaS-Dienstleistungen. Dabei zeigt sich ein erheblicher Widerspruch zwischen den rechtlichen Möglichkeiten und der tatsächlichen Umsetzung: Trotz der in Kapitel 4 dargestellten Lösungsansätze – insbesondere der funktionalen Leistungsbeschreibung nach § 104 Abs 2 BVergG 2018 – dominiert in der österreichischen Verwaltungspraxis eine faktische „On-Premise-only“-Präferenz, die Cloud-Lösungen systematisch benachteiligt oder gänzlich ausschließt.

Diese Praxis ist nicht nur vergaberechtlich problematisch, sondern führt auch zu erheblichen ökonomischen Ineffizienzen und Innovationshemmnissen. Die folgende Analyse untersucht zunächst den empirischen Befund dieser Präferenz, bewertet diese sodann aus vergaberechtlicher, ökonomischer und datenschutzrechtlicher Perspektive und zeigt auf, dass die gängige Praxis gegen zentrale Grundsätze des Vergaberechts

²⁹⁴ Datenschutzkonferenz, Orientierungshilfe – Cloud-Computing, Stand 09.10.2014, https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf, 15 f (abgerufen am 1. 2. 2026).

²⁹⁵ vgl. Strittmatter in Auer-Reinsdorff/Conrad § 22 Rn 10 ff; Claßen/Koch/Müller, MMR 2020, 723 (728).

²⁹⁶ OLG Düsseldorf 21. 10. 2015, Verg 28/14, Rn 167 ff, 214; vgl. Claßen/Koch/Müller, MMR 2020, 723, (727 f).

verstößt.

6.1. Empirischer Befund: Die „On-Premise-only“-Präferenz

In der österreichischen Vergabep Praxis lässt sich trotz der technologischen Reife von SaaS-Modellen eine bemerkenswerte Beharrlichkeit klassischer On-Premise-Strukturen beobachten. Während in der Privatwirtschaft die Transformation hin zu Cloud- und insbesondere SaaS-Modellen in weiten Teilen fortgeschritten ist – laut einer Studie von A1 aus dem Jahr 2024²⁹⁷ nutzen 80% der österreichischen Unternehmen bereits Cloud-Services - erscheint der öffentliche Sektor in seiner Gesamtheit zurückhaltender und uneinheitlich: Eine Analyse des öffentlichen Sektors durch eine PwC-Studie aus dem Jahr 2023²⁹⁸ nennt als wesentliche Gründe dieser Zurückhaltung: (1) Datenschutz- und IT-Sicherheitsbedenken, insbesondere im Kontext der DSGVO und des *Schrems-II*-Urteils,²⁹⁹ (2) fehlende Cloud-Kompetenz auf Behördenseite,³⁰⁰ und (3) mangelhafte Standardisierung.³⁰¹

Obwohl keine behördliche Statistik über das Verhältnis von SaaS- zu On-Premise-Ausschreibungen vorliegt, lassen sich diese eher punktuellen Befunde diverser Markterkundungen inzwischen durch systematische Prüfungen des Rechnungshofes bestätigen und vertiefen. Im Bericht „Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium“³⁰² hält der Österreichische Rechnungshof fest, dass die IT-Architektur des Bundes stark auf bestehende, überwiegend im Bundesrechenzentrum betriebene Infrastrukturen zugeschnitten sei. Dies sei unter anderem darauf zurückzuführen, dass das bereits 2012 geschaffene

²⁹⁷ A1 Telekom Austria AG, A1 Cloud Studie (2024), [A1 Cloud Studie 2024: 4 von 5 Unternehmen in Österreich nutzen die Cloud - A1.net Newsroom](#) (abgerufen am 3. 1. 2026); vgl auch Claßen/Koch/Müller, MMR 2020, 723 (723 f).

²⁹⁸ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf (abgerufen am 27. 12. 2025).

²⁹⁹ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 5 (abgerufen am 27. 12. 2025).

³⁰⁰ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27. 12. 2025).

³⁰¹ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 7 (abgerufen am 27. 12. 2025).

³⁰² Rechnungshof Österreich (RH), Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, [Bericht des Rechnungshofes: Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium](#) (abgerufen am 31. 12. 2025).

IKT-Konsolidierungsgesetz³⁰³ welches eigentlich die rechtliche Basis für eine einheitliche und moderne IT-Infrastruktur bilden sollte – mangels notwendiger Durchführungsverordnungen kaum Wirkung entfalten konnte. Auch strategische Projekte wie das „Security Framework Bund“, das einen einheitlichen Sicherheitsmaßstab für moderne Cloud-Anwendungen definieren sollte, verblieben im Stadium der Konzeption.³⁰⁴ Der Rechnungshof kritisiert hierbei, dass durch das Fehlen dieser Standards faktisch veraltete On-Premise-Strukturen zementiert werden und der Weg zu einer technologieoffenen SaaS-Nutzung blockiert bliebe.³⁰⁵

Noch deutlicher sind die Pfadabhängigkeiten auf kommunaler Ebene: Im Bericht „Digitales Leistungsspektrum ausgewählter Gemeinden“³⁰⁶, am Beispiel von Groß-Enzersdorf, Hallein, Mödling oder St. Johann im Pongau, stellte der Rechnungshof fest, dass die geprüften Gemeinden ihre E-Government-Angebote, also Websites, digitale Amtstafeln, Mobil-Apps, Formularserver, Kindergarten-Webanwendungen etc, ausschließlich als zugekaufte Standardsoftware beziehen. Dabei zeige sich eine erhebliche Abhängigkeit von jeweils einem dominierenden kommunalen IT-Dienstleistungsunternehmen.³⁰⁷ Diese Entscheidungen seien weder durch Kosten-Nutzen-Analysen noch durch strategische Digitalisierungsüberlegungen dokumentiert.³⁰⁸ Die Auftragsverhältnisse seien durch kontinuierlich steigende Wartungs- und Lizenzkosten gekennzeichnet; die laufenden Kosten für Webaufttritt, digitale Amtstafel und Mobilapplikation übersteigen nach wenigen Jahren die einmaligen Anschaffungskosten um ein Vielfaches.

Besonders problematisch ist in diesem Zusammenhang auch die Tendenz, datenschutzrechtliche Anforderungen pauschal als Ausschlussgrund für Cloud-Lösungen heranzuziehen.³⁰⁹ Häufig wird argumentiert, dass die Verarbeitung personenbezogener

³⁰³ Bundesgesetz, mit dem IKT-Lösungen und IT-Verfahren bundesweit konsolidiert werden BGBl I 2012/35 idF BGBl I 2018/104 (IKT-Konsolidierungsgesetz – IKTKonG).

³⁰⁴ RH, Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, 5.1 ff, 6.2 ff.

³⁰⁵ RH, Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, 5.2, 7.2.

³⁰⁶ RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf (abgerufen am 31. 12. 2025).

³⁰⁷ RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, 8.2 (abgerufen am 31. 12. 2025).

³⁰⁸ RH, Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf, 7.1–7.2 (abgerufen am 31. 12. 2025).

³⁰⁹ vgl. Claßen/Koch/Müller, MMR 2020, 723 (726 ff); Möglich in Taeger/Pohle Rz 179 ff; zu den technischen Maßnahmen (Verschlüsselung, Pseudonymisierung) vgl. Pollirer in Knyrim, Der DatKomm DSGVO

Daten in der Cloud – insbesondere bei Einbindung US-amerikanischer Anbietenden – nach der *Schrems-II*-Rechtsprechung unzulässig sei.³¹⁰ Diese pauschale Bewertung verkennt jedoch die differenzierten Lösungsansätze, die das Datenschutzrecht bereithält.³¹¹

Dieser beschriebenen Praxis steht die politische und unionsrechtliche Stoßrichtung in einem deutlichen Spannungsverhältnis gegenüber. Die Cloud-Strategie der Europäischen Union sowie das „European Interoperability Framework“ betonen die Notwendigkeit technologieneutraler, interoperabler Beschaffung. Die Kommission fordert ausdrücklich, Cloud-Lösungen als gleichberechtigte Option zu berücksichtigen und strategische Abhängigkeiten, also Vendor-Lock-in, zu vermeiden.³¹² Das Programm „Digitale Dekade 2030“ sieht vor, dass bis zum Jahr 2030 rund 75 % der europäischen Unternehmen Cloud-Dienste nutzen und die öffentliche Verwaltung eine Vorreiterrolle einnehmen soll.³¹³

6.2. Vergaberechtliche Bewertung: Verstoß gegen Wettbewerb und Technologieneutralität

Die beschriebene „On-Premise-only“-Präferenz steht in fundamentalem Widerspruch zu den vergaberechtlichen Grundsätzen der Technologieneutralität, des Wettbewerbs und der Gleichbehandlung. Vergaberechtlich besonders relevant ist, dass die beschriebene „On-Premise-only“-Präferenz gegen das Gebot der Produkt- und Technologie-neutralität verstoßen können. Werden technische Umsetzungen vorgegeben, obwohl funktionale Spezifikationen ausreichen würden, führt dies zu einer unzulässigen Wettbewerbsverengung und kann andere Anbietende – insbesondere Cloud-Anbieter – ohne sachliche Rechtfertigung ausschließen. Damit droht ein vergaberechtswidriger Eingriff in Gleichbehandlung und offenen Wettbewerb.³¹⁴

Art 32 Rz 45.

³¹⁰ EuGH C-311/18, *Schrems II*, ECLI:EU:C:2020:559; vgl. *Tretzmüller*, Handbuch Softwarerecht¹ Rz 903 ff.

³¹¹ §§ 24, 106 Abs 1 BVergG 2018; BVwG 12. 9. 2018, W138 2203735-2; vgl. *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff; *Claßen/Koch/Müller*, MMR 2020, 723 (724 ff); ergänzend *Tretzmüller* Rz 903 ff.

³¹² Europäische Kommission, European Interoperability Framework – Implementation Strategy, COM(2017) 134 final [cellar_2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02_DOC_1.pdf](#) (abgerufen am 3. 1. 2026); Europäische Kommission, A European strategy for data, COM(2020) 66 final, 18 ff [EUR-Lex - 52020DC0066 - EN - EUR-Lex](#), (abgerufen am 3. 1. 2026).

³¹³ Europäische Kommission, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, 7 [eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118](#) (abgerufen am 3. 1. 2026).

³¹⁴ § 20 Abs 1 BVergG 2018; §§ 78 ff BVergG 2018; §§ 106 BVergG 2018; LVwG NÖ 7. 6. 2018, LVwG-VG-3/002-2018; vgl. auch Gölles in *Gölles/Casati* BVergG, § 20 Rz 14 ff; Gölles in *Gölles/Casati*, BVergG 2018, § 78 Rz 1 ff. vgl. *Diem* in *Gölles/Casati*, BVergG 2018, §106 Rz 22.

Die in Kapitel 4.1.2 und 4.1.3 entwickelten Grundsätze der Sachlichkeitsprüfung und des Gleichwertigkeitsprinzips werden in der österreichischen Praxis jedoch häufig nicht beachtet. Statt einer differenzierten Prüfung, ob technologieoffene Spezifikationen das Beschaffungsziel ebenso gut erreichen könnten, werden pauschale Ausschlüsse vorgenommen, ohne dass die Notwendigkeit und Verhältnismäßigkeit dieser Einschränkung substantiiert dargelegt wird.³¹⁵ Dies verstößt gegen das in § 106 BVerG 2018 normierte Gebot der Produktneutralität und gegen den allgemeinen Grundsatz des Wettbewerbs nach § 20 Abs 1 BVerG 2018.³¹⁶

Die faktische Bevorzugung von On-Premise-Lösungen führt zudem zu einer Verfestigung bestehender Marktstrukturen. Etablierte Anbietende, die bereits On-Premise-Lösungen in der Verwaltung installiert haben, werden systematisch begünstigt, während innovative Cloud-Anbietende – insbesondere kleinere und mittlere Unternehmen – faktisch vom Wettbewerb ausgeschlossen werden. Dies widerspricht dem Ziel des Vergaberechts, durch offenen Wettbewerb die wirtschaftlichste Lösung zu ermitteln.³¹⁷

6.3. Ökonomische Bewertung: Verkürzte Wirtschaftlichkeitsprüfung und Innovationshemmnisse

Die vergaberechtlichen Defizite der „On-Premise-only“-Präferenz manifestieren sich auch in erheblichen ökonomischen Ineffizienzen. Die in der österreichischen Praxis übliche Fokussierung auf Anschaffungskosten führt zu einer systematischen Verzerrung der Wirtschaftlichkeitsbewertung.³¹⁸

Statt einer umfassenden Lebenszykluskostenrechnung kommt es bei On-Premise-Beschaffungen häufig zu verkürzten Preisvergleichen.³¹⁹ Diese bilden die tatsächlichen betrieblichen Vorhalte- und Betriebskosten – wie etwa für Hardware-Erneuerungen, Energie oder Administrationspersonal – nicht vollständig ab.³²⁰ Im Gegensatz dazu sind

³¹⁵ § 20 Abs 1 BVerG 2018; §§ 78 ff BVerG 2018; §§ 106 BVerG 2018; BVwG 26. 6. 2018, W139 2162939-2; vgl auch Gölles in Gölles/Casati BVerG, § 20 Rz 14 ff; Gölles in Gölles/Casati, BVerG 2018, § 78 Rz 1 ff. vgl Diem in Gölles/Casati, BVerG 2018, §106 Rz 22.

³¹⁶ vgl Diem in Gölles/Casati, BVerG 2018, §106 Rz 22.

³¹⁷ Claßen/Koch/Müller, MMR 2020, 723 (725).

³¹⁸ vgl Casati in Gölles/Casati, BVerG 2018 § 20 Rz 5.

³¹⁹ CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 35 (abgerufen am 21. 1. 2026).

³²⁰ vgl Zarnekow, Grundlagen des Cloud Computing - Cloud Computing in der öffentlichen Verwaltung (TU Berlin 2013), 4 ff; Claßen/Koch/Müller, MMR 2020, 723 (725); CISPE, CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), https://cispe.cloud/website_cispe/wp-content/uploads/2022/04/German_CISPE-Buying-Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf, 35 (abgerufen am 21. 1. 2026).

bei Cloud- und SaaS-Leistungen zentrale Betriebs- und Sicherheitskomponenten bereits im Serviceentgelt enthalten (vgl die detaillierte Darstellung der methodisch korrekt zu berücksichtigenden Kosten in Kap. 4.2.1).

Diese verkürzte Wirtschaftlichkeitsbetrachtung führt zu einer systematischen Unterbewertung von SaaS-Modellen und widerspricht dem in § 91 BVergG 2018 normierten Bestbieterprinzip, das eine ganzheitliche Bewertung der Wirtschaftlichkeit verlangt.³²¹

Hinzu kommt, dass die pauschale Bevorzugung von On-Premise-Lösungen erhebliche Innovationshemmnisse schafft.³²² Cloud-Technologien ermöglichen neue Formen der Zusammenarbeit, der Skalierbarkeit und der Ressourcennutzung, die mit traditionellen On-Premise-Modellen nicht oder nur mit erheblichem Aufwand realisierbar sind.³²³ Durch den faktischen Ausschluss von Cloud-Lösungen wird die öffentliche Verwaltung von diesen Innovationen abgeschnitten.³²⁴ Dieser theoretische Vorteil der funktionalen Leistungsbeschreibung wird jedoch in der Praxis nicht genutzt, wenn Vergabestellen durch konstruktive Vorgaben den Wettbewerb auf On-Premise-Lösungen verengen.³²⁵

Besonders problematisch ist die langfristige Wirkung dieser Praxis. Durch die kontinuierliche Bevorzugung etablierter On-Premise-Anbietenden entstehen Lock-in-Effekte, die künftige Beschaffungen präjudizieren.³²⁶ Die Problematik des Vendor-Lock-in wird durch die österreichische Beschaffungspraxis nicht verhindert, sondern aktiv gefördert. Dies führt zu einer schleichenden Erosion der Verhandlungsposition der öffentlichen Hand und zu steigenden Kosten bei Folgebeschaffungen.³²⁷

³²¹ vgl *Casati* in *Gölles/Casati*, BVergG 2018 § 92 Rz 1 ff.

³²² vgl *Claßen/Koch/Müller*, MMR 2020, 723 (725 ff); *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 5 ff, 10 f, 21 ff.

³²³ *Fenz/Göllner/Heurix/Meurers/ Neubauer/Tjoa/Quirchmayr/Hitz/Schatten/Neuhold*, Cloud-Sicherheit: Leitfaden für Behörden und Klein- und Mittelbetriebe (Studie TU Wien/Universität Wien/SophiSystems in Koop mit BMLVS und BSIC der WKO; KIRAS/ BMVIT) 2014, https://www.bmlv.gv.at/pdf_pool/publikationen/08_cs.pdf, 16 (abgerufen am 27.12.2025).

³²⁴ *Fenz et al*, Cloud-Sicherheit: Leitfaden für Behörden und Klein- und Mittelbetriebe (Studie TU Wien/Universität Wien/SophiSystems in Koop mit BMLVS und BSIC der WKO; KIRAS/ BMVIT) 2014, https://www.bmlv.gv.at/pdf_pool/publikationen/08_cs.pdf, 12 (abgerufen am 27.12.2025).

³²⁵ *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 6 ff; *Casati* in *Gölles/Casati*, BVergG 2018 § 20 Rz 12; EuGH Rs C-413/17 *Roche Lietuva* ECLI:EU:C:2018:898 Rz 33 ff.

³²⁶ *Fenz et al*, Cloud-Sicherheit: Leitfaden für Behörden und Klein- und Mittelbetriebe (Studie TU Wien/Universität Wien/SophiSystems in Koop mit BMLVS und BSIC der WKO; KIRAS/ BMVIT) 2014, https://www.bmlv.gv.at/pdf_pool/publikationen/08_cs.pdf, 24 (abgerufen am 27.12.2025).

³²⁷ vgl PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 (abgerufen am 27.12.2025).

6.4. Datenschutzrechtliche Bewertung: Schrems II als unzulässige Pauschalbegründung

Ein zentrales Argument für den Ausschluss von Cloud-Lösungen in der österreichischen Praxis ist die Berufung auf datenschutzrechtliche Bedenken, insbesondere im Zusammenhang mit der *Schrems-II*-Rechtsprechung des EuGH. Auf Basis der in Kapitel 3.3 detailliert dargelegten Judikatur wird jedoch deutlich, dass aus dem Wegfall des Privacy-Shield keineswegs eine pauschale vergaberechtliche Cloud-Sperre resultiert. Vielmehr obliegt es der öffentlichen Vergabestelle, Schutzziele so zu definieren, dass ein DSGVO-konformes Niveau nachprüfbar erreicht wird.³²⁸

In der österreichischen Beschaffungspraxis zeigt sich jedoch häufig eine Tendenz zur überschießenden Vorsicht: Anstatt die vom EuGH explizit eröffneten Möglichkeiten technischer Zusatzmaßnahmen – wie etwa eine Ende-zu-Ende-Verschlüsselung mit ausschließlicher EU-Schlüsselhoheit oder Pseudonymisierung – proaktiv in die Leistungsbeschreibung einzubauen, wird die Rechtssache *Schrems II* als pauschaler Ausschlussgrund angeführt.³²⁹ Vergaberechtlich ist diese Praxis bedenklich, da eine technologiebezogene Vorgabe nach § 106 Abs 1 BVergG 2018 erst dann zulässig ist, wenn ein dokumentiertes TIA negativ ausfällt.³³⁰ Eine generische Berufung auf *Schrems II* ohne Einzelfallprüfung genügt dem Transparenz- und Wettbewerbsgebot nicht. Die unter Kapitel 3.3.2 und 4.3.2 diskutierten technischen Kompensationsmaßnahmen müssen daher zwingend Teil des vergaberechtlichen Abwägungsprozesses sein. Erst die Dokumentation im Vergabevermerk – gegebenenfalls gestützt auf eine Markterkundung gemäß § 24 BVergG 2018 – kann belegen, ob technologieoffene Alternativen tatsächlich kein gleichwertiges Schutzniveau gewährleisten können.³³¹

Ein häufiges Problem in österreichischen Vergabeunterlagen besteht darin, dass

³²⁸ PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 5 (abgerufen am 27. 12. 2025).

³²⁹ vgl PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 5 f (abgerufen am 27. 12. 2025).

³³⁰ vgl *Diem* in *Gölles/Casati*, BVergG 2018 § 106 Rz 5; vgl dazu einen deutschen Blogbeitrag, der explizit darauf hinweist, dass Transfer in die USA nicht pauschal verboten ist: CMS law, Heinzke, [\(K\)ein Ausschluss von US-Cloud-Anbietern bei öffentlichen Aufträgen](#) (4. 10. 2022) (abgerufen am 1. 7. 2026).

³³¹ §§ 24, 106 BVergG 2018; BVwG 12.9.2018, W138 2203735-2; vgl auch *Heid/Ring* in *Heid/Deutsmann/Hofbauer/Reisner*, BVergG 2018 § 24 BVergG 2018, Rz 1 ff, *Kurz* in *Heid/Deutsmann/Hofbauer/Reisner*, BVergG 2018 § 106 BVergG 2018, Rz 13 ff, 9 ff.

öffentliche Vergabestellen pauschal – insbesondere US-basierte – Cloud-Angebote ausschließen, ohne zuvor eine einzelfallbezogene Prüfung der Datenkategorien, der konkreten Drittland-Transferpfade und möglicher technischer oder organisatorischer Kompensationsmaßnahmen vorzunehmen.³³² Gemäß § 106 Abs 1 BVergG 2018 müssen technologiebezogene Festlegungen durch den Auftragsgegenstand objektiv gerechtfertigt sein. Eine pauschale Ablehnung von Cloud-Diensten unter Verweis auf eine vermeintlich mangelnde Datenschutzkonformität wird dieser Anforderung nicht gerecht.

Ein solches Vorgehen ist aus drei Gründen unzulässig: Erstens ersetzt es die notwendige differenzierte Betrachtung des konkreten Verarbeitungsvorgangs und des tatsächlichen Schutzbedarfs – insbesondere die wesentliche Unterscheidung zwischen sensiblen personenbezogenen Daten und bloßen Verwaltungsdaten – durch generalisierte Annahmen. Zweitens werden mögliche technische oder organisatorische Kompensationsmaßnahmen bereits ex ante ausgeblendet. Drittens läuft eine solche Pauschalierung auf eine unzulässige Diskriminierung der Anbietenden hinaus – ungeachtet der im Einzelfall implementierten Sicherheitsarchitekturen, Zertifizierungen und ergänzenden Garantien.³³³

Durch die Rechtssache *Schrems II* werden verantwortliche Datenverarbeiter – also auftraggebende Stellen – verpflichtet, bei Drittlandübermittlungen eine einzelfallbezogene Prüfung des Schutzniveaus vorzunehmen und – soweit erforderlich – zusätzliche Maßnahmen zu implementieren; das Urteil begründet jedoch keinen pauschalen Ausschluss von Cloud-Anbietenden.³³⁴ In vergaberechtlicher Hinsicht sind technische Einschränkungen nachvollziehbar und dokumentiert zu begründen; eine formelhafte Behauptung der Erforderlichkeit ohne detaillierte Begründung genügt hierfür nicht. Erforderlich ist vielmehr eine tragfähige Dokumentation im Vergabevermerk, warum technologieoffene

³³² Zur faktischen Zurückhaltung des öffentlichen Sektors aufgrund von Rechtsunsicherheiten vgl. PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 5 f. (abgerufen am 27. 12. 2025); zur vergaberechtlichen Problematik diskriminierender Vorgaben bei Cloud-Leistungen vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (724).

³³³ vgl. § 106 Abs 1 BVergG 2018; EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284, Rn 61, 87, 109 (technische Spezifikationen dürfen den Wettbewerb nicht künstlich einengen); EuGH C-496/99 P, *Kommission/CAS Succhi di Frutta*, ECLI:EU:C:2004:236, Rn 110 f.; *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f.) zur Notwendigkeit sachlich gerechtfertigter, am Auftragsgegenstand orientierter Vorgaben; *Claßen/Koch/Müller*, MMR 2020, 723 (724 f., 728 f.); European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version 18.06.2021, [edpb_recommendations_202001vo.2.0_supplementarymeasures-transfer-tools_en.pdf](https://edpb.europa.eu/media/1000000000/1000000000_202001vo.2.0_supplementarymeasures-transfer-tools_en.pdf), Abschnitt 2 (Steps 1–6) (abgerufen am 3. 1. 2026).

³³⁴ EuGH C-311/18, *Schrems II*, ECLI:EU:C:2020:559; vgl. dazu auch *Tretzmüller*, Handbuch Software-recht¹ Rz 913 ff.

Alternativen – wie etwa vertraglich zugesicherte Datenspeicherung in der EU oder fortgeschrittene Verschlüsselungskonzepte mit lokaler Schlüsselhoheit – im konkreten Fall nicht ausreichen, um das spezifische Sicherheitsniveau zu gewährleisten. Eine On-Premise-Vorgabe ist vergaberechtlich erst dann haltbar, wenn diese milderer Maßnahmen nachweislich ungeeignet sind, den Schutzbedarf der betroffenen Datenkategorien zu decken.³³⁵

7. Handlungsempfehlungen für eine innovationsoffene Vergabepaxis

Die vorstehende Analyse hat gezeigt, dass das Gebot der Technologieneutralität – verankert in §§ 103, 106 BVergG 2018 – nicht nur ein formales Prinzip, sondern eine materielle Voraussetzung für funktionsfähigen Wettbewerb darstellt.

Dieses Kapitel entwickelt konkrete Handlungsempfehlungen, die sich an zwei Adressatenkreise richten: Zum einen an die Vergabestellen selbst, die unmittelbar für die Gestaltung und Durchführung von Vergabeverfahren verantwortlich sind. Zum anderen an den Gesetzgeber und die Verwaltungsorganisation, die durch Standardisierung, Leitfäden und Schulungen die strukturellen Rahmenbedingungen für eine rechtssichere und wirtschaftliche SaaS-Beschaffung schaffen können.

7.1. Für Vergabestellen: Markterkundung, Leistungsbeschreibung und TCO-Modelle

Eine objektive Entscheidungsgrundlage für die Wahl einer bestimmten Betriebsform kann durch eine vorgelagerte Markterkundung gemäß § 24 BVergG 2018 geschaffen werden. Die Markterkundung sollte ergebnisoffen durchgeführt werden und eine technologische Bestandsaufnahme umfassen: Welche Bereitstellungsmodelle sind für den konkreten Anwendungsfall verfügbar? Welche Sicherheitsstandards und Zertifizierungen bieten die verschiedenen Lösungen? Wie unterscheiden sich die Lebenszykluskosten? Die Ergebnisse sind im Vergabevermerk zu dokumentieren, um gegenüber Nachprüfungsinstanzen nachzuweisen, dass die Vergabestelle ihre Entscheidung auf einer fundierten Grundlage getroffen hat.³³⁶

Anstatt mittels einer konstruktiven Beschreibung die Hardware- oder Betriebsumgebung spezifisch vorzugeben, sollten Anforderungen rein zielorientiert und funktionsbezogen definiert werden. Dies entspricht der in § 103 BVergG 2018 angelegten

³³⁵ EuGH C-311/18, *Schrems II*, ECLI:EU:C:2020:559, VwGH 1. 2. 2017, Ro 2016/04/0054; § 24, 106 Abs 1 BVergG 2018; *Claßen/Koch/Müller*, MMR 2020, 723 (727 f); *Tretzmüller*, Handbuch Softwarerecht¹ Rz 855 ff.

³³⁶ vgl *Ziniel* in *Gölles/Casati*, BVergG 2018 § 24 Rz 4 ff.

Vorrangstellung der funktionsbezogenen Leistungsbeschreibung bei komplexen IT-Beschaffungen und trägt dem unionsrechtlichen Konzept technischer Spezifikationen Rechnung. Ein praxisorientiertes Beispiel für eine solche technologieneutrale Formulierung lautet:

„Das beauftragte Unternehmen hat eine Softwarelösung bereitzustellen, die [Funktion X] für [Anzahl Y] gleichzeitige Nutzende ermöglicht. Zur Sicherstellung der Integrität und Vertraulichkeit der Daten sind Verschlüsselungsverfahren einzusetzen, die dem aktuellen Stand der Technik entsprechen und nachweislich behördlichen Sicherheitsanforderungen genügen. Die exklusive kryptografische Schlüsselgewalt muss dabei bei der Vergabestelle verbleiben.“³³⁷

Eine derartige Formulierung lässt sowohl klassische On-Premise-Modelle als auch Private- oder Public-Cloud-Lösungen zu und wahrt damit das Gebot der Produkt- und Technologieneutralität nach § 106 Abs 1 BVergG 2018. Diese Vorgabe knüpft an wesentliche Schutzziele wie Vertraulichkeit und Integrität sowie an messbare Anforderungen an, ohne eine sachlich nicht gerechtfertigte Festlegung des Bereitstellungsmodells vorzunehmen.

Um die Wirtschaftlichkeit von SaaS-Beschaffungen sachgerecht beurteilen zu können, sollte die Preiswertung über einen repräsentativen Betrachtungszeitraum erfolgen. Dabei ist sicherzustellen, dass die fiktiven Kosten für den internen Betrieb als fester Bestandteil in das Bewertungsraster einfließen. Im Sinne einer objektiven Vergleichbarkeit sind neben den internen Aufwänden bei SaaS-Modellen insbesondere nutzungs- oder funktionsbasierte Entgelte sowie die Bepreisung von Exit-Leistungen einzubeziehen.³³⁸ Die daraus resultierende Bewertungsmethodik – bestehend aus dem Betrachtungszeitraum, den Mengengerüsten und den Umrechnungsformeln – ist gemäß § 92 Abs 2 BVergG 2018 zwingend in den Vergabeunterlagen offenzulegen. Dies stellt sicher, dass das wirtschaftlichste Angebot auf Basis der tatsächlichen ökonomischen Effizienz über den gesamten Nutzungszeitraum ermittelt wird und die Zuschlagsentscheidung im Sinne des Transparenzgebots des § 20 BVergG 2018 nachvollziehbar bleibt.³³⁹

³³⁷ Eigene Formulierung in Anlehnung an *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f).

³³⁷ §§ 103, 106 Abs 1 BVergG 2018; vgl zur Verpflichtung, den Wettbewerb durch neutrale Leistungsbeschreibungen möglichst weit zu öffnen, *Diem in Göllles/Casati*, BVergG 2018 § 106 Rz 38 ff

³³⁸ vgl *Claßen/Koch/Müller*, MMR 2020, 723 (725); zur Vielfalt der Vergütungsmodelle (Pay-as-you-go vs Pauschale) siehe auch *Möglich in Taeger/Pohle* Rz 203.

³³⁹ vgl *Casati in Göllles/Casati*, § 92 BVergG 2018 Rz 1 ff.

Neben der Preiswertung sind zudem SLAs essenziell, um das geforderte Qualitäts- und Sicherheitsniveau eindeutig zu definieren und die Angebote vergleichbar zu machen – ein Aspekt, der in Kapitel 4.3 vertieft wurde.³⁴⁰ Dies ergänzen vertragliche Regelungen der Leistungskomponenten – miet-, dienst- und gegebenenfalls werkvertragliche Anteile – um Qualitätssicherung zu gewährleisten.³⁴¹ Solch detaillierte Ausgestaltung in den Dokumenten erhöht nicht nur die Transparenz für die Angebotslegung, sondern erleichtert auch die Handhabung im Streitfall, da die dispositiven gesetzlichen Regelungen oft nur unzureichend auf die Spezifika von Cloud-Leistungen passen.³⁴²

Ein Hauptgrund für die On-Premise-Präferenz vieler öffentlicher Stellen ist die Sorge vor einem Vendor-Lock-in. Da die Datenhoheit während der Laufzeit faktisch in der Sphäre des beauftragten Unternehmens liegt, droht am Vertragsende ein Migrationsaufwand, der ohne klare Exit-Regelungen kaum kalkulierbar ist.³⁴³ Damit ein Vendor-Lock-in effektiv vermieden werden kann, müssen die vertraglich vereinbarten Übergabepflichten den unter Punkt 4.4.2 spezifizierten technischen Standards entsprechen – insbesondere hinsichtlich maschinenlesbarer Exportformate und Metadatenstrukturen. Ohne hinreichend bestimmte Exit-Leistungen ist der Leistungsgegenstand im Sinne der §§ 103, 105 BVergG 2018 unvollständig beschrieben; zudem lassen sich ohne diese Angaben die lebenszyklusbezogenen Gesamtkosten nicht belastbar vergleichen.³⁴⁴

7.2. Für den Gesetzgeber: Standardisierung, Leitfäden und Schulungen

Im Lichte des aufgezeigten Rechtsvergleichs wird deutlich, dass in Österreich – im Gegensatz zur Situation in Deutschland mit den EVB-IT Cloud und der UfAB – ein allgemein anerkanntes und behördenseitig nutzbares Standardwerk für IT-Beschaffungen fehlt. Dieses strukturelle Defizit erhöht die Abhängigkeit von den Vertragsmustern der anbietenden Unternehmen und damit das Risiko intransparenter oder faktisch diskriminierender Leistungsbeschreibungen.³⁴⁵ Zur Abmilderung dieser Defizite bietet sich primär die Erarbeitung bundesweit einsetzbarer Musterklauseln an. Diese sollten einen

³⁴⁰ vgl zur detaillierten Regelung von SLAs und Verfügbarkeit in einem Standardvertragswerk *Möglich in Taeger/Pohle* Rn 188 ff.

³⁴¹ vgl zur Unzulänglichkeit der Standard-Vertragstypen *Strittmatter in Auer-Reinsdorff/Conrad* § 22 Rn 33

³⁴² vgl zur detaillierten Regelung von SLAs und Verfügbarkeit in einem Standardvertragswerk *Möglich in Taeger/Pohle* Rn 188 ff.

³⁴³ vgl *Claßen/Koch/Müller*, MMR 2020, 723 (724); *Strittmatter in Auer-Reinsdorff/Conrad* § 22 Rn 10 ff.; *Schrotz/Zdanowiecki*, CR 2015, 485 (486 ff); *Möglich in Taeger/Pohle* Rz 194 ff.

³⁴⁴ vgl *Schrotz/Zdanowiecki*, CR 2015, 485 (486, 490 f); *Claßen/Koch/Müller*, MMR 2020, 723 (724 f); vgl auch *Möglich in Taeger/Pohle* Rz 194 ff.

³⁴⁵ vgl *Schrotz/Zdanowiecki*, CR 2015, 485 (486 f).

modularen Aufbau aufweisen mit Bausteinen für unterschiedliche Cloud-Servicemodelle (IaaS, PaaS, SaaS) und Bereitstellungsformen (Public-, Private-, Hybrid-Cloud). Die zentralen Punkte sollten umfassen: präzise Definition des Leistungsgegenstands, standardisierte SLA-Definitionen, Datenschutz- und Sicherheitsanforderungen gemäß DSGVO, Regelungen zu Drittlandtransfers, umfassende Exit-Regelungen sowie Vergütungsmodelle. Ergänzend sollten standardisierte Bewertungsmatrizen für szenariobasierte Kosten- und TCO-Abfragen entwickelt werden. Darüber hinaus ist die Formulierung klarer, technologieoffener Gleichwertigkeitskriterien essenziell, insbesondere in Bezug auf Sicherheitsniveau, Verfügbarkeit, Interoperabilität und Portabilität, wobei auch die jeweils akzeptierten Nachweisformen zu definieren sind.³⁴⁶

Die Umsetzung einer technologieneutralen Cloud-Offenheit scheitert in Österreich häufig weniger an der Verfügbarkeit technischer Angebote als vielmehr an einer punktuell fehlenden IT- und Cloud-Vergabekompetenz in den Rechtsabteilungen. Flankiert werden sollten die Standardisierungsmaßnahmen daher durch einen systematischen Aufbau von Cloud-Vergabekompetenz mittels Schulungen und praxisnahen Leitfäden, die sich an internationalen Referenzwerken wie dem Kriterienkatalog C5 des BSI oder dem CISPE-Handbuch orientieren können.³⁴⁷ Der vom deutschen BSI entwickelte Kriterienkatalog C5 kann dabei als Referenz für die inhaltliche Ausgestaltung von Sicherheitsanforderungen und Auditrechten dienen. Eine vergleichbare Standardisierung für den österreichischen Rechtsraum würde die Rechtssicherheit in Cloud-Beschaffungsvorgängen signifikant erhöhen und das Risiko fehlerhafter Vergabeentscheidungen minimieren.³⁴⁸

8. Zusammenfassung und Ausblick

Die vorliegende Arbeit hat die Besonderheiten der Beschaffung von SaaS-Diensten

³⁴⁶ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (723 f); *Schrotz/Zdanowiecki*, CR 2015, 485 (486); *Hunzinger*, CR 2023, 349 (350); zu den praktischen Herausforderungen der österreichischen Beschaffungspraxis PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 ff (abgerufen am 27. 12. 2025).

³⁴⁷ vgl. *Claßen/Koch/Müller*, MMR 2020, 723 (723 f); *Schrotz/Zdanowiecki*, CR 2015, 485 (486); *Hunzinger*, CR 2023, 349 (350); zu den praktischen Herausforderungen der österreichischen Beschaffungspraxis PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf, 6 ff (abgerufen am 27. 12. 2025).

³⁴⁸ vgl. BSI, Cloud Computing Compliance Criteria Catalogue (C5), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html (abgerufen am 2. 1. 2026); *Strittmatter* in *Auer-Reinsdorff/Conrad* § 22 Rn 10 ff, 32 ff; vgl. zur Relevanz des C5 für die EVB-IT Cloud auch *Hunzinger*, CR 2023, 349 (350).

durch öffentliche Vergabestellen mit Blick auf Vergleichbarkeit und Transparenz im Vergabeverfahren untersucht. Im Mittelpunkt stand ein rechtsvergleichender Ansatz zwischen Österreich und Deutschland.

Die Analyse hat drei zentrale Herausforderungen identifiziert, die aus den strukturellen Unterschieden von SaaS-Modellen zu traditionellen On-Premise-Lösungen resultieren: die durch heterogene Preismodelle erschwerte Vergleichbarkeit der Angebote, das Risiko eines Vendor-Lock-in durch die Verlagerung der Datenhoheit in die Sphäre des beauftragten Unternehmens sowie die komplexen datenschutzrechtlichen Anforderungen bei Drittlandtransfers personenbezogener Daten.

Das geltende Vergaberecht verfügt grundsätzlich über die notwendigen Instrumente zur Bewältigung dieser Herausforderungen. Die funktionale Leistungsbeschreibung nach § 104 Abs 2 BVergG 2018 ermöglicht eine technologieoffene Ausschreibung, die sowohl On-Premise- als auch Cloud-Lösungen zulässt. Die szenariobasierte Lebenszykluskostenrechnung nach § 92 BVergG 2018 überführt heterogene Preismodelle in ein vergleichbares Bewertungsraster. Präzise definierte Service-Level-Agreements schaffen die Grundlage für eine objektive qualitative Angebotsbewertung, und verbindliche Exit-Regelungen sichern die Wettbewerbsfähigkeit künftiger Neuausschreibungen.

Der Rechtsvergleich zeigt zwei deutlich divergierende Herangehensweisen: In Deutschland sorgt der Einsatz der EVB-IT Cloud für eine stark standardisierte Vertragsgrundlage, die durch feste Dokumentenhierarchien ein hohes Maß an Rechtssicherheit schafft. Österreich verfolgt hingegen einen individualisierten Ansatz, bei dem funktionale Leistungsbeschreibungen fallweise ausgearbeitet werden. Dieser größere Gestaltungsspielraum erhöht zwar die Flexibilität, verlangt aber erhebliche vergabe- und IT-fachliche Expertise und birgt ein höheres Risiko unklarer oder uneinheitlicher Vorgaben.

Die kritische Analyse der österreichischen Praxis hat einen erheblichen Widerspruch zwischen den rechtlichen Möglichkeiten und der tatsächlichen Umsetzung aufgezeigt. Die beobachtbare Bevorzugung von On-Premise-Modellen und die im öffentlichen Sektor vielfach bestehenden Datenschutz- und Souveränitätsbedenken stehen potenziell in einem Spannungsverhältnis zu den vergaberechtlichen Grundprinzipien der Technologieutralität, des Wettbewerbs und der Gleichbehandlung. Die identifizierten Defizite verorten sich dabei weniger auf der normativen Ebene als vielmehr in der praktischen Rechtsanwendung.

Die entwickelten Handlungsempfehlungen setzen daher nicht bei einer Reform des Vergaberechts an, sondern bei einer Verbesserung der Beschaffungspraxis: durch ergebnisoffene Markterkundung, funktionale Leistungsbeschreibung mit klaren Schutzziele, szenariobasierte TCO-Bewertung, verbindliche Exit-Regelungen sowie die differenzierte Operationalisierung datenschutzrechtlicher Anforderungen. Auf struktureller Ebene erscheint die Entwicklung standardisierter Vertragsbausteine nach dem Vorbild der EVB-IT Cloud, flankiert durch praxisnahe Leitfäden und einen systematischen Kompetenzaufbau, dringend geboten.

Die zentrale Erkenntnis dieser Arbeit lässt sich wie folgt verdichten: Digitale Souveränität im öffentlichen Sektor entsteht nicht durch Abschottung und pauschale Ausschlüsse, sondern durch Offenheit, die durch klare rechtliche und technische Anforderungen strukturiert wird. Technologieneutralität erweist sich dabei nicht als Hindernis, sondern als Voraussetzung einer zukunftsfähigen Beschaffung: Sie sichert den Zugang zu skalierbaren SaaS-Lösungen, ohne das erforderliche Schutzniveau preiszugeben, und ermöglicht eine digitale Souveränität, die durch Interoperabilität und die Vermeidung einseitiger Abhängigkeiten praktisch wirksam wird.

Die Untersuchung hat gezeigt, dass die österreichische Vergabep Praxis nicht an einem Mangel rechtlicher Instrumente scheitert, sondern an deren unzureichender Anwendung. Die in Kapitel 6 dokumentierte On-Premise-Präferenz lässt sich weder vergaberechtlich noch ökonomisch oder datenschutzrechtlich rechtfertigen. Sie resultiert vielmehr aus einer Kombination von Faktoren: mangelnde Beschaffungskompetenz in Bezug auf Cloud-Technologien, fehlendes Bewusstsein für die Lebenszykluskosten, pauschale Datenschutzbedenken ohne differenzierte Einzelfallprüfung sowie das Fehlen standardisierter Vertragsmuster.

Diese Defizite manifestieren sich in konkreten Vergabebefehlern. Konstruktive Leistungsbeschreibungen, die faktisch nur On-Premise-Lösungen zulassen, verstoßen gegen das Gebot der Technologieneutralität nach § 106 BVergG 2018. Verkürzte Wirtschaftlichkeitsprüfungen, die nur Anschaffungskosten berücksichtigen, widersprechen dem Bestbieterprinzip nach § 91 BVergG 2018. Pauschale Berufungen auf Schrems II ohne Transfer Impact Assessment verletzen das Transparenz- und Wettbewerbsgebot nach § 20 BVergG 2018.

Die Überwindung dieser Defizite erfordert einen Paradigmenwechsel in der

Beschaffungskultur. Vergabestellen müssen Cloud-Lösungen nicht als Risiko, sondern als gleichwertige Alternative zu On-Premise-Modellen begreifen. Dies setzt voraus, dass die in Kapitel 4 entwickelten Instrumente – funktionale Leistungsbeschreibung, TCO-Bewertung, SLA-Steuerung und Exit-Management – konsequent angewendet werden.

Der Rechtsvergleich hat die zentrale Bedeutung der Standardisierung für eine rechtssichere und effiziente SaaS-Beschaffung offengelegt. Die deutschen EVB-IT Cloud demonstrieren, dass standardisierte Vertragsmuster die Beschaffungspraxis erheblich entlasten können, ohne die Flexibilität zu beeinträchtigen. Die kontrollierte Öffnung für Anbieter-AGB ermöglicht es, die technische Standardisierung von Cloud-Leistungen vertraglich abzubilden, ohne die Vergleichbarkeit der Angebote zu gefährden.

Für Österreich bedeutet dies nicht, dass die EVB-IT Cloud eins zu eins übernommen werden sollten. Die österreichische Rechtsordnung kennt eigene Traditionen und Strukturen, die zu berücksichtigen sind. Dennoch erscheint die Entwicklung vergleichbarer Standardverträge unabdingbar. Diese sollten modular aufgebaut sein und verschiedene Cloud-Servicemodelle sowie Bereitstellungsformen abdecken. Zentrale Regelungsbereiche umfassen die Leistungsbeschreibung, SLA-Definitionen, Datenschutz- und Sicherheitsanforderungen, Drittlandtransfers, Exit-Regelungen und Vergütungsmodelle.

Ergänzend bedarf es standardisierter Bewertungsmatrizen für die TCO-Bewertung. Diese sollten Referenzszenarien vorgeben, die eine objektive Vergleichbarkeit unterschiedlicher Preismodelle ermöglichen. Nur so lässt sich verhindern, dass strategische Mischkalkulationen den Wettbewerb verzerren.

Die Schrems-II-Judikatur hat die datenschutzrechtlichen Anforderungen an Drittlandtransfers präzisiert, ohne Cloud-Lösungen pauschal auszuschließen. Die Untersuchung hat gezeigt, dass technische Kompensationsmaßnahmen – wie Ende-zu-Ende-Verschlüsselung mit EU-Schlüsselhoheit, Confidential Computing oder Bring Your Own Key – ein DSGVO-konformes Schutzniveau gewährleisten können. Die pauschale Berufung auf Schrems II als Ausschlussgrund für Cloud-Lösungen ist daher vergaberechtlich unzulässig.

Vergabestellen sind vielmehr verpflichtet, im Rahmen eines Transfer Impact Assessment zu prüfen, ob technologieoffene Alternativen ein gleichwertiges Schutzniveau gewährleisten können. Erst wenn diese Prüfung negativ ausfällt, ist eine

technologiebezogene Festlegung auf On-Premise-Lösungen zulässig. Diese Prüfung muss im Vergabevermerk dokumentiert werden und kann durch eine Markterkundung nach § 24 BVergG 2018 unterstützt werden.

9. Schlussbemerkung

Die Beschaffung von SaaS-Diensten stellt keinen technischen Sonderfall dar, sondern markiert einen grundlegenden Wandel in der Art und Weise, wie öffentliche Verwaltungen IT-Leistungen beziehen. Die vergaberechtlichen Instrumente zur Bewältigung dieses Wandels sind vorhanden. Entscheidend ist jedoch, dass Vergabestellen diese Instrumente konsequent anwenden und dabei die Balance zwischen Rechtssicherheit und Innovationsoffenheit wahren. Die digitale Transformation der öffentlichen Verwaltung wird maßgeblich davon abhängen, ob es gelingt, die vergaberechtlichen Grundsätze so zu operationalisieren, dass sie technologische Innovation nicht behindern, sondern ermöglichen. Die vorliegende Arbeit hat gezeigt, dass dies möglich ist – vorausgesetzt, die Vergabepaxis überwindet ihre On-Premise-Fixierung und nutzt die Potenziale, die das geltende Vergaberecht bereits heute bietet.

Literaturverzeichnis

Monographien / Handbücher / Kommentare

Auer-Reinsdorff Astrid / Conrad Isabell (Hrsg), Handbuch IT- und Datenschutzrecht³ (2019)

Burgi Martin / Dreher Meinrad / Opitz Marc (Hrsg), Beck'scher Vergaberechtskommentar Bd 1⁴ (beck-online.de)

Bydlinski Peter / Perner Stefan / Spitzer Martin (Hrsg), ABGB: Kommentar zum ABGB⁷ (2023)

Gölles Hans / Casati Claus (Hrsg), Bundesvergabegesetz 2018 (BVerG 2018) (rdb.at)

Heid Stepan / Deutschmann Daniel / Hofbauer Berthold / Reisner Hubert (Hrsg), BVerG 2018 (2019)

Heid Schiefer Rechtsanwälte / Preslmayr Rechtsanwälte (Hrsg), Handbuch Vergaberecht² (2025)

Herberger Maximilian / Martinek Michael / Rüßmann Helmut / Weth Stephan / Würdinger Markus (Hrsg), jurisPK-BGB¹⁰ (juris.de)

Hoeren Thomas / Pinelli Stefan, IT-Vertragsrecht (2024)

Knyrim Rainer (Hrsg), Der DatKomm (rdb.at)

Moick Karlheinz / Gföhler Andreas, BVerG 2018^{1.01} (rdb.at)

Nowak Christoph, Das Bundesvergabegesetz 2018 aus Sicht der Neuen Institutionenökonomie (Dissertation TU Wien 2024)

Summa Hermann / Schneevogl Kai-Uwe (Hrsg), juris PraxisKommentar Vergaberecht⁷ (juris.de)

Taeger Jürgen / Pohle Jan (Hrsg), Computerrechts-Handbuch (40. EL März 2025)

Tretzmüller Christoph, Handbuch Softwarerecht¹ (2023)

Zankl Wolfgang (Hrsg), Rechtshandbuch der Digitalisierung (2021)

Zarnekow Rüdiger, Grundlagen des Cloud Computing - Cloud Computing in der öffentlichen Verwaltung (TU Berlin 2013).

Aufsätze in Zeitschriften

Bischof Elke, Die EVB-IT Cloud – Anwendung, Besonderheiten und Herausforderungen, ITRB 2023, 165

Bischof Elke / Intveen Michael, Die neuen EVB-IT Cloud aus Anwendersicht, ITRB 2022, 157

Claßen Nadine / Koch Moritz Philipp / Müller Norman, Beschaffung von Cloud-Services durch öffentliche Auftraggeber, MMR 2020, 723

Förster Christian, IT-Vertragsrecht: Teil 4 – Miete und Kauf von Standardsoftware, MMR 2024, 960

García-Fernández Ignacio / Parejo José / Ruiz-Cortés Antonio, Pricing4SaaS, arXiv:2404.00311v1 (2024)

Heydn Truiken, Software-as-a-Service – Probleme und Vertragsgestaltung, MMR 2020, 435

Hunzinger Sven, Die neuen EVB-IT Cloud aus Anbietersicht: Ein Jahr Praxis, CR 2023, 349

Leßner Anne / Gäntgen Julius, (Un)Wirksamkeit von B2B-AGB bei (internationalen) SaaS-Verträgen KuR 2021, 766.

Müller Maximilian A., Zur vergaberechtlichen Einordnung von ASP-/Cloud-Leistungen, ZIIR 2014, 372

Schima Sonam, Zur rechtlichen Einordnung von Software-as-a-Service-Verträgen, ecolex 2024, 197

Schrotz Jan-Oliver / Zdanowiecki Konrad, Cloud Computing für die öffentliche Hand – Rechtliche Schlüsselthemen und Lösungsansätze, CR 2015, 485

Schröder Christian / Haag Nils Christian, Neue Anforderungen an Cloud Computing für die Praxis – Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing“, ZD 2011, 147

Schulz Sönke E., Cloud Computing in der öffentlichen Verwaltung – Chancen – Risiken – Modelle, MMR 2010, 75

Tretzmüller Christoph, Wann muss ein Auftragsverarbeitervertrag nach Art 28 DSGVO abgeschlossen werden? Dako 2019/1, 7

Tretzmüller Christoph, Zur rechtlichen Qualifikation von Softwareverträgen, ZIIR 2019, 255

Judikaturverzeichnis

Gerichtshof der Europäischen Union

EuGH C-45/87, *Kommission/Irland*, ECLI:EU:C:1988:435

EuGH C-19/00, *SIAC Construction*, ECLI:EU:C:2001:553

EuGH C-59/00, *Bent Moustén Vestergaard*, ECLI:EU:C:2001:652

EuGH C-448/01, *EVN AG und Wienstrom GmbH*, ECLI:EU:C:2003:65

EuGH C-496/99 P, *Kommission/CAS Succhi di Frutta*, ECLI:EU:C:2004:236

EuGH C-454/06, *Presstext*, ECLI:EU:C:2008:351

EuGH C-368/10, *Kommission/Niederlande*, ECLI:EU:C:2012:284

EuGH C-278/14, *Enterprise Focused Solutions*, ECLI:EU:C:2015:228

EuGH C-413/17, *Roche Lietuva*, ECLI:EU:C:2018:865

EuGH C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd und Maximilian Schrems (Schrems II)*, ECLI:EU:C:2020:559

Verwaltungsgerichtshof

VwGH 17. 11. 2004, 2002/04/0078

VwGH 1. 7. 2010, 2006/04/0139

VwGH 1. 2. 2017, Ro 2016/04/0054

VwGH 27. 2. 2019, Ra 2017/04/0054

VwGH 1. 3. 2022, Ra 2019/04/0139

Bundesverwaltungsgericht

BVerwG 13. 12. 2012, 3 C 32.11 (Deutschland)

BVwG 26. 6. 2018, W139 2162939-2
BVwG 12. 9. 2018, W138 2203735-2

Bundesgerichtshof

BGH 16. 1. 1985 – VIII ZR 153/83, BGHZ 93, 252
BGH 18. 1. 2000, X ZR 101/97
BGH 15. 11. 2006, XII ZR 120/04
BGH 10. 6. 2008, X ZR 78/07
BGH 31. 1. 2017, X ZB 10/16

Oberlandesgerichte und Kammergericht

OLG München 6. 7. 2000, U (K) 5047/99
OLG Düsseldorf 8. 5. 2000, Verg 6/00
OLG Düsseldorf 28. 07. 2011, VII-Verg 20/11
OLG Düsseldorf 27. 6. 2012, VII-Verg 7/12
OLG Düsseldorf 1. 8. 2012, VII-Verg 10/12
OLG Düsseldorf 19. 6. 2013, Verg 8/13
OLG Celle 24. 2. 2015, 13 Verg 1/15
OLG Düsseldorf 21. 10. 2015, Verg 28/14
OLG Düsseldorf 16. 12. 2015, Verg 25/15
OLG Düsseldorf 1. 6. 2016, VII-Verg 6/16
OLG Düsseldorf 8. 3. 2017, VII-Verg 39/16
OLG Brandenburg 28. 3. 2017, 6 Verg 5/16
OLG Düsseldorf 13. 12. 2017, VII-Verg 19/17
KG Berlin 4. 6. 2019, Verg 8/18
OLG Celle 12. 10. 2021, 13 Verg 7/21

Landesverwaltungsgerichte

LVwG NÖ 7. 6. 2018, LVwG-VG-3/002-2018

Verzeichnis der Studien, Leitfäden und Behördendokumente

A1 Telekom Austria AG, A1 Cloud Studie (2024), A1 Cloud Studie 2024: 4 von 5 Unternehmen in Österreich nutzen die Cloud, <https://newsroom.a1.net/news-a1-cloud-studie-2024-4-von-5-unternehmen-in-oesterreich-nutzen-die-cloud?id=206931&menuid=12657&l=deutsch> (abgerufen am 3. 1. 2026)

Art.-29-Datenschutzgruppe, WP 248, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf (abgerufen am 8. 2. 2026)

Beschaffungsamt des Bundesministeriums des Innern Zentralstelle IT-Beschaffung (ZIB), Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB), Version 2018, <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/ufab/ufab-node.html> (abgerufen am 1. 1. 2026)

Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloud Computing Compliance Criteria Catalogue (C5), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html (abgerufen am 2. 1. 2026)

CISPE, Erwerb von Cloud-Services im öffentlichen Sektor (2022), [German CISPE-Buying](https://www.cispe.eu/)

[Cloud-Services-in-Public-Sector-Handbook-v2-FEB-2022_de.pdf](#) (abgerufen am 21. 1. 2026)

Datenschutzkonferenz, Orientierungshilfe – Cloud-Computing, Stand 09.10.2014, https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf (abgerufen am 1. 2. 2026)

Datenschutzbehörde, Erläuterungen zur DSFA-V, https://dsb.gv.at/sites/site0344/media/downloads/erlaeuterungen_zur_dsfa-v.pdf, (abgerufen am 8. 2. 2026)

Digitales Österreich, Österreichisches Informationssicherheitshandbuch, <https://www.sicherheitshandbuch.at> (abgerufen am 8. 2. 2026)

European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, final version 18.06.2021, [edpb recommendations 202001vo.2.0 supplementarymeasurestransfer-tools_en.pdf](#) (abgerufen am 3. 1. 2026)

European Data Protection Board (EDPB), Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems (23.07.2020), [20200724 edpb fa-goncjeuc31118_de.pdf](#) (abgerufen am 16. 1. 2026)

Europäische Kommission, European Interoperability Framework – Implementation Strategy, COM(2017) 134 final, [eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0134](#) (abgerufen am 3. 1. 2026)

Europäische Kommission, A European strategy for data, COM(2020) 66 final, [EUR-Lex - 52020DC0066 - EN - EUR-Lex](#) (abgerufen am 3. 1. 2026)

Europäische Kommission, 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, [EUR-Lex - 52021DC0118 - EN - EUR-Lex](#) (abgerufen am 3. 1. 2026)

Fenz Stefan / Göllner Johannes / Heurix Johannes / Meurers Thomas / Neubauer Thomas / Tjoa A Min / Quirchmayr Gerald / Hitz Martin / Schatten Alexander / Neuhold Eva, Cloud-Sicherheit: Leitfaden für Behörden und Klein- und Mittelbetriebe (Studie TU Wien/Universität Wien/SophiSystems in Koop mit BMLVS und BSIC der WKO; KIRAS/ BMVIT) 2014, https://www.bmlv.gv.at/pdf_pool/publikationen/08_cs.pdf (abgerufen am 27. 12. 2025)

Ministerium für Digitales und Staatsmodernisierung, EVB-IT Cloud – Vertrag, , https://www.digitale-verwaltung.de/SharedDocs/downloads/Webs/DV/DE/digitale-loesungen/it-einkauf/evb-it-bvb/basisvertraege/cloud/it-cloud-vertrag.docx?__blob=publicationFile&v=2 (abgerufen am 2. 1. 2026)

National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, Special Publication (NIST SP) (2011) [nvl-pubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf](#) (abgerufen am 20. 5. 2025)

PwC Austria / Amazon Web Services, Perspektiven zur Cloudnutzung im öffentlichen Sektor in Österreich (2023), https://www.pwc.at/de/publikationen/pwc-aws_cloud-studie.pdf (abgerufen am 27. 12. 2025)

Rechnungshof Österreich (RH), Digitales Leistungsspektrum ausgewählter Gemeinden, Reihe NÖ 2024/4, Reihe S 2024/2, https://www.rechnungshof.gv.at/rh/home/home/2024_NOE_S_Digitales_Leistungsspektrum_Gemeinden.pdf (abgerufen am 31. 12. 2025)

Rechnungshof Österreich (RH), Management der IT-Sicherheit im Finanzministerium, Klimaschutzministerium und Landwirtschaftsministerium, Reihe Bund 2024/16, [Bericht des](#)

Rechnungshofes: Management der IT-Sicherheit im Finanzministerium, Klimaschutz- ministerium und Landwirtschaftsministerium (abgerufen am 31. 12. 2025)

Internetquellen

Baier Michael, Software-as-a-Service (SaaS) Verträge: Einordnung und Möglichkeiten, SRD-Rechtsanwälte Blog, 9. 4.2025, <https://www.srd-rechtsanwaelte.de/blog/saas-vertraege-einordnung-moeglichkeiten> (abgerufen am 27. 12. 2025)

BTL Rechtsanwälte, RA Dr. Tobias Beltle, Blogbeitrag, 11. 7. 2022, <https://www.btl-recht.de/blog/evb-it-cloud-vertrag/> (abgerufen am 7. 3. 2026)

CMS law, Heinzke Philippe, (K)ein Ausschluss von US-Cloud-Anbietern bei öffentlichen Aufträgen (4. 10. 2022) (abgerufen am 1. 7. 2026)

Härtel Ralf, Software-as-a-Service-Vertrag, ITMediaLaw Wissensbank, 11. 4. 2025, <https://itmedialaw.com/wissensdatenbank/software-as-a-service-vertrag-saas-vertrag/> (abgerufen am 27. 12. 2026)

Hürthen Sebastian, Vergabeblog.de, Unterlage für Ausschreibung und Bewertung von IT-Leistungen: Die UfAB 2018 – Oldie but Goldie (29.6.2023), <https://vergabeblog.de/2023-06-29/unterlage-fuer-ausschreibung-und-bewertung-von-it-leistungen-die-ufab-2018-oldie-but-goldie/> (abgerufen am 1. 2. 2026).

IT-RechtKanzlei GmbH & Co. KG, Keller-Stoltenhoff Elisabeth, Geschichte und Zukunft der EVB-T, Blogbeitrag vom 8. 6. 2026, Geschichte und Zukunft der EVB-IT (abgerufen am 27. 12. 2025)

Ministerium für Digitales und Staatsmodernisierung, Archiv (EVB-IT), <https://www.digitale-verwaltung.de/Webs/DV/DE/aktuelles-service/it-einkauf/evb-it-und-bvb/evb-archiv/evb-archiv.html> (abgerufen am 31. 1. 2026)

Schima Christoph, Wie sind SaaS-Verträge rechtlich einzuordnen? digital-recht.at (Blog Kanzlei Dr Tretzmüller) (2023), <https://www.digital-recht.at/blog/wie-sind-saas-vertraege-rechtlich-einzuordnen> (abgerufen am 27. 12. 2025)

Schwientek, Die Vergabe von Cloud-Leistungen (EVB-IT Cloud) (01/2023), Leinemann Partner Rechtsanwälte: <https://www.leinemann-partner.de/newsletter/neues-zum-vergaberecht-01-2023/die-vergabe-von-cloud-leistungen-evb-it-cloud/> (abgerufen am 21. 1. 2026)

Total Cost of Ownership (TCO): So behält der Einkauf die Gesamtkosten im Blick, Beschaffung aktuell, 29. 7. 2024, Total Cost of Ownership (TCO): So behält der Einkauf die Gesamtkosten im Blick (abgerufen am 30. 12. 2025)

[Ende des Dokuments]