AVV Customer-Side (GTM allgemein) — Template-Stack

⚠️ Eigenbau-Risk-Flag

User-Entscheidung 2026-04-20: Alles Eigenbau ohne Anwalt. Für allgemeine B2B-Customer-AVV weniger strafrechtlich kritisch als Kanzlei-Version (kein Mandatsgeheimnis), aber AGB-Kontrolle (§305-310 BGB) gilt. CFO-Risk-Flag:

- Haftungsklauseln nicht geprüft
- Kunden werden eigene Prüfung machen — Verhandlungs-Risiko
- Anwalts-Review nachziehen sobald Budget frei (Härting, SKW Schwarz, ca. 2-4k€)

Template-Stack

Grundgerüst: Bitkom Muster-AVV (IT/SaaS-fokussiert, sehr solide) **Ergänzung:** GDD Muster-AVV (KMU-Praxis, Goldstandard) — TOM-Anlage **Drittland-Modul:** EU SCCs 2021/914, Modul 2 (Controller→Processor) **Fallback:** LfDI BW Muster (amtlich, rechtssicher)

Quellen

Quelle	URL	Lizenz
Bitkom Muster-AVV (empfohlen als Basis)	bitkom.org → Publikationen → Muster-Auftragsverarbeitungsvertrag	kostenlos, keine Weitergabe als Template
GDD Muster-AVV (TOM-Anlage)	gdd.de/downloads/praxishilfen	kostenfrei mit Registrierung
LfDI BW Muster (Fallback)	baden-wuerttemberg.datenschutz.de/muster-zur-auftragsverarbeitung	Public Domain (§5 UrhG)
EU SCCs 2021/914	eur-lex.europa.eu/eli/dec_impl/2021/914/oj	EU Public Domain
GDPR.eu DPA Template (EN-Version)	gdpr.eu/data-processing-agreement	CC BY-SA 4.0 (Attribution pflicht)

AVV-Struktur (Standard B2B)

```
§1  Präambel / Vertragsgegenstand
§2  Begriffsbestimmungen
§3  Gegenstand, Art, Zweck, Dauer (→ Anlage 1)
§4  Weisungsrecht Verantwortlicher
§5  Pflichten Auftragsverarbeiter (Art. 28 Abs. 3 DSGVO)
§6  Vertraulichkeit Beschäftigte (§53 BDSG, NDA-Klausel)
§7  Technisch-organisatorische Maßnahmen (→ Anlage 2)
§8  Sub-Auftragsverarbeiter (→ Anlage 3)
§9  Drittlandstransfer / SCCs (→ Anlage 4)
§10 Betroffenenrechte / Mitwirkung
§11 Meldung von Datenschutzverletzungen (72h)
§12 Prüf- und Audit-Rechte (ISO 27001 / SOC2 als Surrogat)
§13 Löschung und Rückgabe
§14 Haftung (AGB-konform)
§15 Schlussbestimmungen (Schriftform, Gerichtsstand München)

Anlagen:
1 – Beschreibung der Verarbeitung
2 – Technisch-organisatorische Maßnahmen
3 – Genehmigte Sub-Auftragsverarbeiter
4 – SCCs 2021 Modul 2
```

Unterschied zur Kanzlei-AVV: keine §203 StGB-Klausel, keine Mandatsgeheimnis-Einzelverpflichtung, keine BRAO-Aufbewahrungsfristen.

Pflicht-Inhalte Art. 28 Abs. 3 DSGVO

Lit.	Inhalt	Lakeware-Spezifikum
a	Weisungsgebundenheit + Hinweispflicht bei Rechtsverstoß	schriftlich/Textform
b	Vertraulichkeit Beschäftigte	NDA-Klausel, §53 BDSG-Verweis
c	Sicherheit Art. 32	→ TOM-Anlage
d	Sub-AV-Genehmigung	Generalgenehmigung mit 30-Tage-Widerspruch
e	Unterstützung Betroffenenrechte (Art. 12-23)	API/Export-Funktion für Auskunft + Löschung
f	Unterstützung Art. 33-36	72h-Breach-Notification, DSFA-Unterstützung
g	Rückgabe/Löschung nach Vertragsende	Wahlrecht Kunde, 30/90 Tage
h	Nachweispflicht + Audit	Zertifikate (ISO 27001 / SOC2) als Audit-Surrogat

TOM-Anlage 2 — SaaS Standard

Vertraulichkeit

- Zutritt: Cloud-RZ (ISO 27001), Büro-Zugang + Alarm
- Zugang: MFA (TOTP/WebAuthn), SSO/SAML optional, NIST SP 800-63B-Passwort-Policy
- Zugriff: RBAC, Least-Privilege, Separation-of-Duties Dev/Ops
- Trennung: Tenant-ID-basiert, Row-Level-Security in DB
- Pseudonymisierung: Dev-/Test-Umgebung nur mit anonymisierten Daten

Integrität

- Weitergabe: TLS 1.3 (Mindeststandard), HSTS, Certificate-Pinning Mobile
- Eingabe: Audit-Log aller CRUD-Operationen, append-only, 12 Monate Retention

Verfügbarkeit + Belastbarkeit

- Backup: inkrementell täglich, Vollbackup wöchentlich, 30 Tage Retention
- Off-Site verschlüsselt (AES-256 + `age`)
- DR: RTO 4h, RPO 1h, dokumentierter Runbook
- Monitoring: 24/7 (Uptime-Kuma / Datadog), Alerting on-call

Wiederherstellung

- Restore-Test quartalsweise, Protokoll

Datenschutz-Management

- DSB benannt (intern/extern), Verfahrensverzeichnis Art. 30
- Jährliche Schulung Beschäftigte
- DSFA bei neuen Features mit Risiko

Incident-Response

- 72h-Meldung an Verantwortlichen (Art. 33 Abs. 2)
- Runbook + Kontaktkette
- Post-Mortem binnen 14 Tagen

Privacy-by-Design / Default (Art. 25)

- Default-Retention minimiert
- Opt-in für Analytics
- Pen-Test jährlich extern
- CVE-Scan (`trivy`) in CI

Sub-AV-Liste (Anlage 3) — Draft Lakeware

Kategorie	Anbieter	Sitz	Drittland-Status
Hosting/Infra	<TBD – CIO-Entscheidung>	EU bevorzugt	direkt DSGVO
CDN	Cloudflare Inc.	US	EU-US DPF (aktiv seit 07/2023, AdEq-Beschluss gültig)
E-Mail-Versand	Postmark oder SendGrid	US	DPF + SCC-Fallback
Monitoring	Grafana Cloud (EU) oder Datadog	EU/US	EU bevorzugt
AI-Proxy LLM	Anthropic, Google, Groq, Mistral (FR)	US/FR	DPF + SCC / EU
Lokale LLM	Qwen self-hosted	intern	kein Drittland
Ausgeschlossen	DeepSeek + andere CN-Provider	CN	Policy: kein Kundendaten-Routing
Billing	Stripe Payments Europe Ltd.	IE	EU
Support	Crisp (FR) > Intercom (US)	EU/US	EU bevorzugt

Drittlandstransfer-Klausel (§9)

```
§9 Drittlandstransfer
(1) Transfers in Drittländer erfolgen nur auf Basis:
    a) Angemessenheitsbeschluss (Art. 45 DSGVO), insbesondere
       EU–US Data Privacy Framework für zertifizierte US-
Empfänger;
    b) Standardvertragsklauseln 2021/914 (Modul 2) inkl. TIA;
    c) Ausnahmen nach Art. 49 DSGVO nur im Einzelfall.
(2) Transfers in die VR China werden ausgeschlossen, soweit sie
    personenbezogene Kundendaten betreffen.
```

Haftungs-Klausel (§14) — AGB-Kontroll-sicher

CFO-Vorschlag für Grenzen: - Vorsatz und grobe Fahrlässigkeit: unbegrenzt haftbar (zwingend nach §309 Nr. 7 BGB) - Leichte Fahrlässigkeit: Begrenzung auf typischerweise vorhersehbaren Schaden - Bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) Haftung begrenzt auf einen Jahresbeitrag - Mittelbare Schäden (entgangener Gewinn, Datenverlust): nur bei Vorsatz

AGB-Check: Diese Struktur ist BGH-Rechtsprechungs-konform (§307 BGB), sollte Standard-Prüfung bestehen. Nachprüfung durch Anwalt bei Budget-Freigabe trotzdem empfohlen.

Operative CFO-Todos (nach User-Approval)

1. **Bitkom-AVV + GDD-TOMs** herunterladen, in `cfo/decisions/gtm-avv-customer-draft.docx` zusammenführen
2. **SCCs 2021 Modul 2** als Anlage 4 ausfüllen (Lakeware als Processor, Kunde als Controller)
3. **Sub-AV-Liste** mit CIO/COO final besetzen
4. **TOM-Anlage** mit CIO abstimmen (was technisch tatsächlich gilt)
5. **AGB-Integration:** AVV als Addendum zur Lakeware-AGB referenzieren (COO-Scope)
6. **Online-Signing-Flow:** Checkbox im Onboarding mit klickbarer AVV-Akzeptanz + PDF-Download (COO)
7. **Versionierung:** jede AVV-Version mit Datum + Hash archivieren in `cfo/decisions/avv-versions/`

Offene Punkte

#	Punkt	Owner
1	Final-Sub-AV-Liste	CFO + CIO + COO
2	Online-Signing-Tool-Wahl	COO
3	Erste Kunden werden AVV prüfen — iterativer Review	CFO
4	Anwalts-Review sobald Budget	CFO — nachziehen

Unterschied zur Kanzlei-AVV

Aspekt	**Customer-AVV (dieses File)**	**Kanzlei-AVV (`2026-04-23-legal-center-avv.md`)**
§203 StGB	nein	**ja** (strafrechtlich kritisch)
Mandatsgeheimnis	nein	**ja** (§43a BRAO)
Breach-Notification	72h (Art. 33)	**24h** (strenger wegen Kanzlei-Meldepflicht)
Retention	Standard Kunden-Wahl	**BRAO-Aufbewahrungsfristen beachten (§50 BRAO)**
AI-Proxy	nur Kundendaten-Policy	**Mandanten-Content strikt EU/lokal, keine Drittland-LLMs**
Aufwand Template	geringer (Bitkom + TOMs)	höher (amtlich + Kanzlei-Addendum)

Frist

- User-Approval dieses Drafts: bis morgen Abend 2026-04-21
- AVV-PDF finalisieren: parallel zur Kanzlei-Version in Woche 17
- Integration in Customer-Onboarding: COO-Scope, parallel zu GTM-Start

Änderungs-History

Datum	Änderung
2026-04-21	Initial nach Subagent-Recherche + CFO-Analyse