Compliance-Statement · Blitzsicht GmbH

Compliance-Statement · Blitzsicht GmbH

(i.Gr.)

Stand: Mai 2026 · **Version:** 1.0 · **Adressat:** Investoren, Series-A-Diligence, Enterprise-Customer-RFPs

> **Kernaussage in einem Satz:** Wir haben Compliance nicht als Pflicht-Bürde behandelt, sondern als Produkt-Default — der gesamte cw-legal-Asset-Pack (TOMs, AVV, TIA, Subprozessoren-Liste, TDDDG-Würdigung) ist bereits Production-grade dokumentiert und versioniert.

1. Compliance-Posture im Überblick

STANDARD / REGULATION	STATUS	BEMERKUNG
DSGVO (Art. 5, 25, 28, 32, 33)	✅ vollständig umgesetzt	TOMs + AVV + Subprozessoren-Doku vorhanden
TDDDG (§ 25)	✅ vollständig umgesetzt	TDDDG-Würdigung pro eingesetztem Dienst dokumentiert (cookieless-Architektur)
§ 5 DDG (Impressumspflicht)	✅ vollständig	Template + Customer-Doku
AVV nach Art. 28 DSGVO	✅ vollständig	DocuSeal-Workflow für jeden Customer + TIA Vercel/Cloudflare
VVT (Art. 30 DSGVO)	✅ vorhanden	Verzeichnis der Verarbeitungstätigkeiten als Excel-Template + Customer-Instanzen

STANDARD / REGULATION	STATUS	BEMERKUNG
EU AI Act	⚠ Monitoring	Multi-Agent-Pipeline = "begrenztes Risiko" (Transparenz), kein Hochrisiko-Use-Case. Wird mit Umsetzungsgesetz nachgeschärft.
NIS2 (NIS2UmsuCG)	⚪ out-of-scope heute	Solo-Founder, < 50 MA, kein KRITIS-Sektor → keine "wesentliche/wichtige Einrichtung". Technische TOMs decken NIS2-Anforderungen trotzdem ab.
ISO/IEC 27001	⏳ Roadmap Q3 2027	Heute: Gap-Analyse-Ready. Full-Cert geplant bei Enterprise-Push 2028+
SOC 2 Type 2	⚪ nicht geplant	US-Standard, irrelevant für DACH-KMU-Markt. Nur bei US-Enterprise-Expansion ab 2029.
§ 5 TMG / § 5a UWG / TDDDG-Werberecht	✅ AGB B2B + Hauptvertrag-Template	Anwalts-Review Q4 2026 mit Funding
BU (Betriebsunterbrechungs-Versicherung)	⏳ Q3 2026 mit GmbH-Gründung	
Cyber-Haftpflicht	⏳ Q3 2026 mit GmbH-Gründung	Erforderlich für Series-A-Diligence

Legende: ✅ done · ⏳ geplant/in Arbeit · ⚠ Monitoring · ⚪ out-of-scope/nicht geplant

2. Was wir bereits haben — cw-legal-Asset-Pack

Das `cw-legal/`-Repository ist die zentrale Source-of-Truth für alle vertraglichen und compliance-relevanten Dokumente. Alle Files sind versioniert (v1.0+) und werden mindestens jährlich oder bei wesentlicher Änderung überprüft.

2.1 Customer-facing Vertragsanlagen

DATEI	INHALT	STATUS
`A0-hauptvertrag-template-v1.0.md`	Hauptvertrag (Werk- + Dienstvertrag), Pricing-Modell, Kündigungs-/Datenexport-Regelung	✅

DATEI	INHALT	STATUS
`A1-impressum-v1.0.md`	§ 5 DDG-konformes Impressum-Template (Blitzsicht + Customer-Sites)	✅
`A3-tdddg-wuerdigung-v1.0.md`	TDDDG-§ 25-Würdigung pro Dienst (warum kein Cookie-Banner)	✅
`A4-vvt-v1.0.xlsx`	Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)	✅
`A5-toms-v1.0.md`	**Technische und Organisatorische Maßnahmen (Art. 32 DSGVO)** — §§ 1–7 vollständig	✅
`A6-subprozessoren-v1.0.md`	Subprozessoren-Liste mit Drittland-Würdigung (Vercel, Cloudflare, Hetzner, …)	✅
`A7-sla-leistungsbeschreibung-v1.0.md`	Service-Level-Agreement	✅
`A8-onboarding-anhang-v1.0.md`	Onboarding-Workflow	✅
`A9-preisliste-v1.0.md`	Preisliste-Anlage	✅
`A10-sepa-mandat-vorlage-v1.0.md`	SEPA-Lastschrift-Mandat	✅
`AVV-A1-beschreibung-verarbeitung-v1.0.md`	AVV-Beschreibung der Verarbeitung	✅
`AVV-A4-tia-vercel-cloudflare-v1.0.md`	Transfer Impact Assessment für US-Subprozessoren	✅
`H4-agb-b2b-v1.0.md`	B2B-AGB	✅

2.2 Technische Compliance-Stacks (Production)

MODUL	FUNKTION	STATUS
cw-dsgvo	Forensische Pre-Consent-Tracking-Detection · RFC-3161-Timestamp-Beweispakete · Art.-77-Beschwerde-Vorbereitung	Beta
cw-audit	82+ Checker (DSGVO, TDDDG, § 5 DDG, A11y, Performance, SEO,	Production

MODUL	FUNKTION	STATUS
	Legal) · programmatic API `runAudit()`	
cw-mta-sts	Mail-Hardening (SPF, DMARC, DKIM, MTA-STS, TLS-RPT) — 1 Worker bedient N Domains	Production
cw-uptime	5-Min-Pings + Telegram-Incident-Alerts	Production
cw-sign	DocuSeal self-hosted für AVV-Abschluss und Hauptverträge	Production

2.3 Operations-Sicherheit (TOMs-konkret)

BEREICH	MASSNAHME
Server-Standort	Hetzner Online GmbH (Falkenstein/Nürnberg, DE) — 24/7-Bewachung, Videoüberwachung, biometrische Zugangskontrolle
Customer-Sites-Hosting	Vercel Edge (DPF-zertifiziert + EU-SCC + TIA) + Cloudflare (CDN/WAF)
Identitäts-Management	1Password mit Master-Passwort ≥ 20 Zeichen, kein Reuse · TOTP-2FA für alle administrativen Accounts
Remote-Zugriff	Tailscale-VPN (WireGuard) für Admin-Zugriff · SSH-Key-only · kein offener SSH-Port
Backup-Strategie	Restic (AES-256, dedupliziert) · 3-2-1-Regel (Hetzner + NAS-Off-Site) · RTO 4h · RPO 24h
Restore-Test	Quartalsweise, dokumentiert in Operations-Journal
Disaster-Recovery-Plan	`cw-legal/internal/disaster-recovery-plan.md` — Vercel-Ausfall, Hetzner-Ausfall, DB-Korruption, Domain-Hijack, Account-Kompromittierung
Logging	Auth-Logs 90 Tage · SaaS-Audit-Logs (Twenty, Sevdesk, Vercel, Cloudflare, GitHub)
IP-Anonymisierung	Server-Logs maskieren Oktette nach 7 Tagen
Verschlüsselung at-rest	FileVault (Mac-Endgeräte) · LUKS (Hetzner-Disks) · Restic-Backup-Verschlüsselung
Verschlüsselung in-transit	TLS 1.3 für alle externen Strecken · HSTS auf allen Domains

3. Status pro Standard im Detail

3.1 DSGVO (EU-2016/679) — vollständig umgesetzt

ARTIKEL	MASSNAHME	BELEG
Art. 5 (Grundsätze)	Privacy-by-Design durch cookieless-Architektur, Datenminimierung	A3-TDDDG-Würdigung
Art. 13/14 (Informationspflichten)	Datenschutzerklärung Template + Customer-spezifische Ausprägungen	cw-legal/01-customer-facing/
Art. 25 (Privacy by Design)	Statische Sites ohne Backend, Plausible cookieless, kein Tracking-Default	A3-TDDDG + technischer Stack
Art. 28 (Auftragsverarbeitung)	AVV-Template mit DocuSeal-Workflow, Subprozessoren-Liste, TIA	AVV-A1, A6 Subprozessoren, AVV-A4 TIA
Art. 30 (VVT)	Verzeichnis der Verarbeitungstätigkeiten als Excel-Template	A4-VVT
Art. 32 (TOMs)	§§ 1–7 vollständig: Vertraulichkeit, Integrität, Verfügbarkeit, Wiederherstellbarkeit, Verfahren, Auftragskontrolle, Incident-Response	**A5-TOMs**
Art. 33 (Meldepflichten)	Incident-Response-Prozess: 24h-Meldung bei Auftragsverarbeitung; 72h an Aufsichtsbehörde wenn Verantwortlicher	A5 § 5
Art. 44 ff. (Drittlandtransfer)	DPF + EU-SCC + Transfer Impact Assessment für Vercel/Cloudflare	AVV-A4 TIA

3.2 TDDDG (§ 25 — Cookie-Consent) — vollständig umgesetzt

Wir betreiben **cookieless-Architektur**: kein Cookie-Banner auf blitzsicht.com und auf Customer-Sites notwendig. Dokumentiert in **A3-tdddg-wuerdigung-v1.0.md** mit Würdigung pro eingesetztem Dienst (Plausible, Vercel, Cloudflare, …). Verifizierungs-Screenshots werden pro Customer-Site vor Go-Live erstellt und versioniert.

3.3 NIS2 — out-of-scope heute, technisch bereit

KRITERIUM	STATUS BLITZSICHT	KONSEQUENZ
Mitarbeitergröße	< 50 (Solo-Founder + Sales-Hires erst Q3 2026)	Out-of-Scope nach NIS2-Größenkriterium
Umsatzschwelle	< €10 Mio (heute €0 MRR, geplant 2030: €3,4 Mio ARR)	Out-of-Scope auf absehbare Zeit
Sektor	Web-Plattform-Provider für KMU	Nicht in NIS2-Anlage 1 (essential) oder Anlage 2 (important)
KRITIS-Status	Keine KRITIS-Kunden derzeit	Nicht NIS2-relevant über Customer-Sub-Lieferanten-Klausel

Aber: Unsere technischen Maßnahmen (siehe TOMs § 3, 4) erfüllen bereits den NIS2-Anforderungs-Katalog (Risikomanagement, Incident-Handling, Business-Continuity, Supply-Chain-Security, Krypto, Multi-Faktor-Authentifizierung). Falls ein Customer NIS2-pflichtig wird und uns als Lieferanten listet, sind wir **technisch ready**, die Sub-Lieferanten-Anforderungen zu bedienen.

3.4 EU AI Act — Monitoring

AI ACT RISIKO-STUFE	TRIFFT AUF BLITZSICHT ZU?	STATUS
Verboten (Art. 5)	Nein — keine Social-Scoring, keine biometrische Echtzeit-Identifikation	✅
Hochrisiko (Annex III)	Nein — kein Einsatz in Kritischer Infrastruktur, Bildung, Beschäftigung, Strafverfolgung, etc.	✅
Begrenztes Risiko (Art. 50 Transparenz)	**Ja, partiell** — AI-generierte Customer-Site-Inhalte werden mit Operator-Review veröffentlicht; Endkunden interagieren nicht direkt mit dem AI-System	⚠ Transparenz-Pflicht-Monitoring
Minimales Risiko	Ja — alle Pipeline-Multi-Agent-Verarbeitungen sind interne Operations-Tools	✅

Maßnahmen: Customer-Sites zeigen keine AI-Chatbots oder AI-Inhalte ohne Kennzeichnung. AI-Voice-Agent (Q1 2027) wird mit eindeutiger "Sie sprechen mit einem KI-Assistenten"-Disclosure ausgeliefert (Art. 50 AI Act). Die Multi-Agent-Pipeline (Captain-Pattern) ist ein internes Operations-Tool und fällt nicht unter Endnutzer-Transparenz-Pflichten.

3.5 ISO/IEC 27001 — Gap-Analyse-Ready, Full-Cert auf Roadmap

Wir haben das ISO-27001-Annex-A-Control-Mapping vorgenommen. Stand Mai 2026: **78 von 93 Controls bereits implementiert** durch die bestehenden TOMs.

CONTROL-FAMILIE (ANNEX A)	ANZAHL CONTROLS	STATUS
A.5 Organizational Controls	37	32 ✅ · 3 ⏳ · 2 ⚪
A.6 People Controls	8	4 ✅ · 4 ⏳ (Hire-Plan-abhängig)
A.7 Physical Controls	14	11 ✅ · 3 ⏳
A.8 Technological Controls	34	31 ✅ · 3 ⏳
Gesamt	**93**	**78 ✅ · 13 ⏳ · 2 ⚪**

Roadmap: - **Q1 2027:** Externe Gap-Analyse durch Audit-Partner (Budget: ~€3–5k) - **Q3 2027:** Stage-1-Audit (Document Review) - **Q4 2027:** Stage-2-Audit (Implementation Review) → ISO-27001-Zertifikat - **Jährlich danach:** Surveillance-Audit (~€5–10k)

Trigger für Vorziehen: Erster Enterprise-Customer mit > 500 MA fordert ISO 27001 als Pre-Sales-Gating. Bis dahin: Pre-Cert-Status („ISO-27001-aligned") reicht für DACH-Mid-Market.

3.6 SOC 2 — nicht geplant

SOC 2 ist ein US-Standard (AICPA) für SaaS-Anbieter, die US-Enterprise-Customers bedienen. Unsere Customer-Base ist DACH-KMU-fokussiert. SOC 2 würde frühestens relevant ab 2029 bei US-Enterprise-Expansion — bis dahin nicht eingeplant. Falls dann benötigt: SOC 2 Type 1 (Snapshot, ~€20–40k) → Type 2 (Beobachtungszeitraum 6–12 Mo, ~€40–80k jährlich).

---

4. Versicherungs-Portfolio (mit GmbH-Gründung Q3 2026)

VERSICHERUNG	ZWECK	STATUS
Berufshaftpflicht (Vermögensschaden + Sach)	Schutz vor Schäden aus IT-Dienstleistung	⏳ Q3 2026 mit Funding
Cyber-Haftpflicht	Schäden durch Hacking, Datenpanne, DSGVO-Bußgelder	⏳ Q3 2026 mit Funding
Betriebsunterbrechung (BU)	Erstattung bei Pipeline-/Hosting-Ausfall	⏳ Q3 2026 mit Funding
D&O (Directors & Officers)	Persönliche Haftung der GmbH-Geschäftsführung	⏳ Q4 2026 (nach GmbH-Gründung)
Rechtsschutz (gewerblich + Internet)	Abmahn-Rechtsschutz, IT-Recht, Markenrecht	⏳ Q4 2026
Krankentagegeld + BU (privat)	Founder-Ausfallabsicherung	⏳ Q4 2026

Budget für Versicherungen Jahr 1: ~€4.500–6.000 (in Use-of-Funds 15 % Legal & Ops eingerechnet).

---

5. Cap-Table & Gesellschafterstruktur

Heute (Pre-Funding)

BETEILIGTER	ANTEIL	STAMM-/SONDERVERMÖGEN
Johannes-Maximilian Gottl (Solo-Founder)	100 % (Einzelunternehmen)	Siluri Clothing als Cash-Bridge

Nach GmbH-Gründung Q3 2026 (Pre-Money €1,5 Mio @ €250k Ticket)

BETEILIGTER	ANTEIL	BEMERKUNG
Johannes-Maximilian Gottl	83,3 %	Stammkapital + IP-Einbringung (Captain-Pattern, cw-core, cw-audit, cw-dsgvo, cw-legal-Asset-Pack)
Pre-Seed-Lead-Investor	16,7 %	€250k @ €1,5 Mio Post-Money
ESOP-Pool (Optionen)	reserviert für Q1 2027	10 % nach Series A geplant (Founder-Anteil dilutet entsprechend)

Nach Target-Funding Q3 2026 (Pre-Money €2 Mio @ €350k Ticket)

BETEILIGTER	ANTEIL
Johannes-Maximilian Gottl	82,5 %
Pre-Seed-Lead	17,5 %
ESOP-Pool (post Series A)	10 % geplant

Nach Aggressiv-Funding (€500k @ €3 Mio)

BETEILIGTER	ANTEIL
Johannes-Maximilian Gottl	83,3 %
Pre-Seed-Lead	16,7 %

Anmerkung: GmbH-Stammkapital €25k wird in voller Höhe einbezahlt (kein UG-Aufbaumodell, kein Stammkapital-Voll-Stellen-Stundung). Das ist saubere Cap-Table-Lösung für Series-A-Diligence.

---

6. Datenschutzbeauftragter (DSB)

KRITERIUM	STATUS BLITZSICHT
Pflicht zur DSB-Bestellung nach Art. 37 DSGVO / § 38 BDSG	**Nein heute.** < 20 ständig beschäftigte Personen mit automatisierter Verarbeitung personenbezogener Daten.
Geplant ab	Q1 2027 nach 2 Sales-FTE + Senior-Eng-Hire (5 Personen Schwelle Auftragsverarbeitung möglich abhängig von Tätigkeitsumfang).
Sourcing	Externer DSB-Service (z.B. Datenschutz-Praxis Regensburg oder ähnlich) bevorzugt, ~€150–250/Mo
Übergangsphase	Aktuell: Johannes als Datenschutz-Verantwortlicher (mit jährlicher Eigen-Auditierung der TOMs gemäß § 5 A5-TOMs).

7. Compliance-Roadmap

QUARTAL	MASSNAHME	BUDGET
Q3 2026	GmbH-Gründung + Anwalts-Review AGB/AVV/Hauptvertrag + Cyber-Haftpflicht + BU	€15–20k einmalig + €4–6k Versicherungen p.a.
Q4 2026	DPMA-Markenanmeldung Klasse 42 · D&O-Versicherung · Rechtsschutz	€3–5k einmalig + €2–3k Versicherungen p.a.
Q1 2027	ISO 27001 Gap-Analyse (extern) · Externer DSB-Service (falls Schwelle erreicht)	€3–5k Gap + €2–3k p.a. DSB
Q3 2027	ISO 27001 Stage-1-Audit	€8–12k
Q4 2027	ISO 27001 Stage-2-Audit → Zertifizierung	€15–25k
Ab 2028	ISO 27001 Surveillance-Audit jährlich	€5–10k p.a.
Falls 2029+	SOC 2 Type 1 / Type 2 (nur bei US-Expansion)	€20–80k p.a.

Gesamt Compliance-Budget bis Q4 2027: ~€60–80k (in Funding-Allocation 15 % Legal & Ops eingerechnet).

8. Was Investoren konkret bekommen

Bei Diligence-Anfrage stellen wir bereit:

- ✅ **TOMs nach Art. 32 DSGVO** (cw-legal/01-customer-facing/A5-toms-v1.0.md)
- ✅ **AVV-Template** mit Subprozessoren-Liste + TIA (Vercel/Cloudflare)
- ✅ **VVT-Excel** (Verzeichnis Verarbeitungstätigkeiten)
- ✅ **TDDDG-Würdigung** für cookieless-Architektur
- ✅ **Disaster-Recovery-Plan** (cw-legal/internal/)
- ✅ **Subprozessoren-Liste** mit Drittlandtransfer-Würdigung
- ✅ **Restore-Test-Berichte** (quartalsweise)
- ✅ **Operations-Journal** (Manuelle Eingriffe in Produktion dokumentiert)
- ✅ **Code-Repository-Audit-Logs** (signed commits, CI-Logs)
- ⏳ **ISO-27001-Gap-Analyse-Bericht** (Q1 2027)
- ⏳ **Pentest-Bericht** (anlassbezogen Q1 2027 vor Series-A-Pitch)

Erstellt: Mai 2026 · Blitzsicht GmbH (in Gründung) · Johannes-Maximilian Gottl Kontakt: servus@blitzsicht.com · blitzsicht.com Adressat: Pre-Seed-Investoren / Series-A-Diligence / Enterprise-RFPs · Vertraulich