



Software | Consulting | Service

• DATENBLATT & WHITEPAPER • MÄRZ 2026

KI-gestützte Softwareentwicklung & Datenschutz

Alles, was Sie als Kunde über unseren KI-Einsatz, die DSGVO-Konformität und Ihre Rechte wissen müssen.

DSGVO-konform

ISO 27001:2024

ISO 9001:2015

AVV vorhanden

🔗 **Externer DSB: heyData GmbH**

INHALT

- 01 Über Dewware GmbH
- 02 Unsere KI-Tools im Überblick
- 03 Was fließt in die KI?
- 04 Drittlandtransfer – Absicherung
- 05 Chancen & Risiken
- 06 AVV & Ihre Rechte
- 07 FAQ
- 08 Kontakt & nächste Schritte

Devware GmbH – Ihr .NET-Partner für den Mittelstand

• Gegründet 2004 • Wuppertal • 25+ Mitarbeiter • Full Remote • Mittelstand-Fokus

UNTERNEHMENSPROFIL

-  Gründungsjahr
2004 · über 20 Jahre Erfahrung
-  Team
25+ Mitarbeiter · Full Remote
-  Standort
Luhnsfelder Höhe 50 · 42369 Wuppertal
-  Zielgruppe
Deutscher Mittelstand · Business-Software

Devware entwickelt maßgeschneiderte .NET-Softwarelösungen für den Mittelstand. KI-Technologien werden seit 2024 aktiv in den Entwicklungsprozess integriert, um Qualität und Effizienz zu steigern – zum Vorteil unserer Kunden.

KERNKOMPETENZEN & TECHNOLOGIEN

- ASP.NET Core
- Blazor
- .NET MAUI
- Azure
- C#
- SQL / EF Core
- GitHub Copilot
- Claude AI

Über 20 Jahre Erfahrung in der professionellen .NET-Entwicklung für den deutschen Mittelstand. Unsere Projekte reichen von komplexen Enterprise-Plattformen bis hin zu spezialisierten ERP- und Business-Tools. Referenzen: HAWIS, Ambion, NWB Verlag, Kufer Software/Horizon, Gartenbau-Versicherung/Symbios 2.0, Rheinbahn.

ISO 27001

Informationssicherheit
ISO/IEC 27001:2024 –aktuellster ISMS-Standard

ISO 9001

Qualitätsmanagement
ISO 9001:2015 –strukturierte QM-Prozesse

DSB

Externer Datenschutzbeauftragter
heyData GmbH, Berlin

AVV

Auftragsverarbeitungsvertrag
Gem. Art. 28 DSGVO · für alle Projekte

Unsere KI-Tools im Überblick

Alle eingesetzten KI-Werkzeuge mit Anbieter, Einsatzzweck und vollständiger DSGVO-Absicherung.

• Alle Tools mit Teams-DPA • SCCs für alle US-Anbieter • Kein Training gem. Anbieterbedingungen • Business/Enterprise-Accounts

Claude / Claude Code

CL Anthropic PBC · USA/Global · Code-Analyse, Code-Generierung, technische Dokumentation und Recherche

Teams-DPA vorliegend

SCCs gem. Art. 46 Abs. 2 lit. c DSGVO

TIA durchgeführt · Risiko: niedrig

GitHub Copilot

GH GitHub Inc. (Microsoft) · USA/Global · KI-gestützte Code-Vervollständigung direkt im Entwicklungseditor

Teams-DPA vorliegend

SCCs gem. Art. 46 Abs. 2 lit. c DSGVO

DPF-zertifiziert – höchste Schutzstufe

ChatGPT (OpenAI)

OA OpenAI Inc. · USA/Global · Code-Generierung und technische Recherche in Kundenprojekten

Teams-DPA vorliegend

SCCs gem. Art. 46 Abs. 2 lit. c DSGVO

TIA durchgeführt · Risiko: niedrig

ⓘ **Kein Training gemäß aktueller Anbieterbedingungen (Business-/Enterprise-Verträge):** Bei allen drei Tools nutzen wir ausschließlich Business- bzw. Enterprise-Accounts. Das Training auf Nutzerdaten ist vertraglich ausgeschlossen und in den Data Processing Agreements schriftlich festgehalten. Eingaben werden zur Beantwortung der Anfrage genutzt und danach nicht für Modellverbesserungen verwendet.

Was fließt in die KI – und was nicht?

Interne Richtlinie: Keine echten Personendaten in KI-Tools. Privacy by Design gem. Art. 25 DSGVO.

• Privacy by Design (Art. 25) • Interne Richtlinie verbindlich • Pseudonymisierung Pflicht • Regelmäßige Schulungen

✓ Was eingespeist wird

- ✓ Abstrakte Code-Logik und Algorithmen ohne Personenbezug
- ✓ Quellcode-Fragmente (projektbezogen, pseudonymisiert)
- ✓ Technische Konfigurationsdaten (keine Echtnamen, keine IDs)
- ✓ Telemetriedaten der lokalen Entwicklungsumgebung
- ✓ Allgemeine technische Dokumentationsstruktur
- ✓ Anonymisierte Fehlermeldungen und Stack-Traces

✗ Was niemals eingespeist wird

- ✗ Personenbezogene Daten Ihrer Mitarbeiter oder Endkunden
- ✗ Produktionsdaten oder Echtdateien aus laufenden Systemen
- ✗ Passwörter, Zugangsdaten, API-Keys, SSH-Schlüssel
- ✗ Sensible Geschäfts-, Finanz- oder Medizindaten
- ✗ E-Mail-Adressen, Telefonnummern, Klarnamen
- ✗ Datenbank-Dumps oder exportierte Benutzerlisten



Datenminimierung

Nur das absolut Notwendige wird in KI-Tools eingegeben. Jede Eingabe wird intern auf Datenschutzrelevanz geprüft, bevor sie das lokale System verlässt.



Pseudonymisierung

Echte Namen, E-Mail-Adressen und alle Identifikatoren werden vor der KI-Eingabe durch neutrale Platzhalter ersetzt. Keine Klarnamen im Prompt.



Schulung & Richtlinie

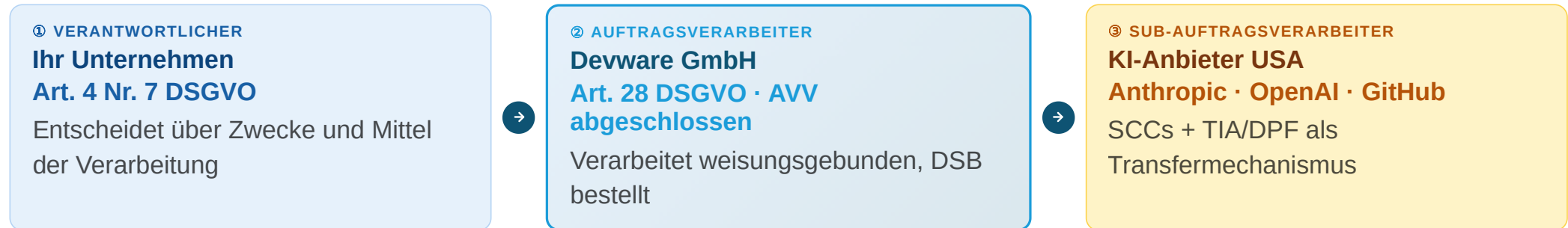
Alle Entwickler werden regelmäßig zum datenschutzkonformen KI-Einsatz geschult. Verstöße sind durch interne Richtlinie ausdrücklich untersagt.

Datentransfer in die USA – so funktioniert die Absicherung

Mehrfach voneinander unabhängige Schutzmechanismen sichern jeden Transfer rechtlich ab.

- Schrems-II-konform
- EU-SCCs aktiv
- TIA: geringes Risiko festgestellt
- DPF: GitHub/Microsoft

RECHTSKETTE DER VERANTWORTLICHKEITEN



EINGESETZTE SCHUTZMECHANISMEN IM DETAIL

§ AVV
Auftragsverarbeitungsvertrag gem. Art. 28 DSGVO
Regelt alle datenschutzrechtlichen Rechte und Pflichten zwischen Ihrem Unternehmen und Devware. Enthält Weisungsrecht, Kontrollrechte, Sub-AV-Regelungen und Widerspruchsrecht.

EU SCCs
EU-Standardvertragsklauseln gem. Art. 46 Abs. 2 lit. c DSGVO
Von der EU-Kommission genehmigte Klauseln – garantieren EU-gleichwertigen Datenschutz auch bei US-Verarbeitung. Aktiv für alle drei KI-Anbieter.

TIA TIA
Transfer Impact Assessment (Anthropic & OpenAI)
Pflichtdokument nach Schrems-II. Bewertet US-Behördenzugriff (FISA § 702, CLOUD Act). Im Rahmen der durchgeführten Transfer Impact Assessments wurde ein geringes Risiko festgestellt.

DPF DPF
EU-US Data Privacy Framework (GitHub / Microsoft)
Höchstes Schutzniveau für EU → USA-Transfers. GitHub/Microsoft ist DPF-zertifiziert und von der EU-Kommission als datenschutzkonform anerkannt.

Chancen & Risiken – transparent kommuniziert

Ehrliche Einschätzung: Vorteile für Ihr Projekt, aktiv gemanagte Risiken und Schutzstufen aller Tools.

- Kein KI-Training
- Keine Datenweitergabe
- Widerspruchsrecht
- Interne Richtlinie aktiv

↗ Chancen für Ihr Projekt

- ✓ Schnellere Entwicklung – weniger Billable Hours für Sie
- ✓ Konsistenterer, qualitativ hochwertiger Code
- ✓ Weniger Bugs durch KI-gestützte Code-Reviews
- ✓ Kürzere Time-to-Market für neue Features
- ✓ Technische Dokumentation wird automatisch miterstellt

⚠ Risiken & unsere Maßnahmen

- US-Behördenzugriff → TIA bestätigt: niedriges Risiko
- Datenweitergabe → vertraglich ausgeschlossen per DPA
- KI-Training auf Ihren Daten → Business-Account, deaktiviert
- Fehlerhafte Vorschläge → Entwickler prüfen immer manuell
- Datenleck → interne Richtlinie & Schulungen

SCHUTZSTUFEN JE KI-TOOL – VOLLSTÄNDIGE ÜBERSICHT

TOOL	ANBIETER	EINSATZ	DPA	SCCS	TIA	DPF	TRAINING AUS
Claude / Claude Code	Anthropic, USA	Code-Analyse & -Generierung	✓	✓	✓	–	✓
GitHub Copilot	GitHub Inc., USA	Code-Vervollständigung	✓	✓	–	✓	✓
ChatGPT (OpenAI)	OpenAI, USA	Code & Recherche	✓	✓	✓	–	✓
Microsoft Azure	Microsoft, EU	Cloud-Hosting	✓	✓	–	✓	EU
Microsoft 365	Microsoft, EU/USA	Kommunikation	✓	✓	–	✓	EU

AVV & Ihre Rechte als Kunde

Was der Vertrag regelt, welche Rechte Sie haben und wie der Prozess abläuft.

• Pflicht nach Art. 28 DSGVO • Widerspruchsrecht 14 Tage • Kontrollrecht jährlich • Löschung nach Projektende



Der AVV ist gesetzlich vorgeschrieben (Art. 28 DSGVO), sobald ein Dienstleister personenbezogene Daten im Auftrag verarbeiten könnte. Da unsere Entwickler bei der Arbeit an Ihrer Software mit datenhaltigen Systemen in Berührung kommen können, ist der AVV Pflicht – er schützt beide Seiten gleichermaßen und schafft rechtliche Klarheit.

Was der AVV regelt

- Eingesetzte KI-Tools und Sub-Auftragsverarbeiter
- Verarbeitete Datenkategorien (Quellcode, Telemetrie – können indirekt personenbez. Daten enthalten, z. B. in Logs oder Kommentaren)
- Technische und organisatorische Maßnahmen (TOM)
- Drittlandtransfer-Mechanismus (SCCs, TIA, DPF)
- Informationspflichten bei Vorfällen (72h-Frist)
- Kontrollrechte des Verantwortlichen (jährlich)
- Löschung / Rückgabe nach Projektende und Ablauf gesetzl. Aufbewahrungsfristen

Ihre Rechte als Kunde

- **Widerspruchsrecht:** Vertraglich vereinbart – 14 Tage bei neuen Sub-Dienstleistern
- **Kontrollrecht:** Jährliche Prüfung der TOM
- **Auskunftsrecht:** Über alle Verarbeitungen jederzeit
- **Weisungsrecht:** Verarbeitung einschränkbar
- **Löschrecht:** Nach Projektende und Ablauf gesetzl. Aufbewahrungsfristen
- **Sonderkündigung:** Bei nicht akzeptierten Sub-AV
- **Schadensersatz:** Bei Pflichtverletzung

01 Projektanfrage

Sie beschreiben Ihr Vorhaben



02 AVV-Zusendung

Wir senden AVV inkl. Anlagen



03 Prüfung & Fragen

Sie prüfen, wir antworten



04 Unterzeichnung

Beidseitig vor Projektstart



05 Projektstart

KI-Einsatz rechtssicher

Häufig gestellte Fragen

Antworten auf die Fragen, die unsere Kunden am häufigsten stellen.

• Keine Weitergabe • Kein Training • Widerspruchsrecht • Löschung

1 Werden meine Daten für KI-Training genutzt?

Nein. Wir nutzen ausschließlich Business- bzw. Enterprise-Accounts. Das Training auf Nutzerdaten ist vertraglich ausgeschlossen und in den DPAs schriftlich festgehalten. Eingaben werden verarbeitet, danach nicht für Modellverbesserungen genutzt.

2 Können US-Behörden auf meine Daten zugreifen?

Theoretisch haben US-Behörden über FISA § 702 und CLOUD Act Zugriffsmöglichkeiten. Die durchgeführten TIAs kommen zum Ergebnis: Risiko niedrig. Abstrakte Code-Fragmente aus kommerziellen Projekten sind kein typisches Geheimdienstziel.

3 Werden Daten an Suchmaschinen weitergegeben?

Nein. Daten verbleiben im jeweiligen KI-System. Es findet keine Weitergabe an Suchmaschinen, soziale Netzwerke oder andere KI-Systeme statt – vertraglich über die Business-DPAs gesichert.

4 Warum muss ich einen AVV unterschreiben?

Der AVV ist gesetzlich vorgeschrieben (Art. 28 DSGVO). Er schützt beide Seiten, dokumentiert alle Verantwortlichkeiten klar und ist Voraussetzung für den rechtskonformen Einsatz von KI-Tools in Ihrem Projekt.

5 Kann ich dem KI-Einsatz widersprechen?

Ja. Der AVV räumt Ihnen ein vertraglich vereinbartes Widerspruchsrecht für den Einsatz neuer Sub-Dienstleister ein (14 Tage). Wir klären gemeinsam, ob das Projekt ohne das neue Tool realisierbar ist. Ein Verzicht kann Auswirkungen auf Timeline und Kosten haben.

6 Bieten Anthropic oder OpenAI EU-Standorte?

Anthropic verarbeitet ausschließlich in den USA – kein EU-Standort verfügbar. Bei OpenAI ist EU-Verarbeitung über Azure EU möglich, aber nur für spezifische Enterprise-Verträge. SCCs + TIA sichern beide Fälle rechtlich ab.

Bereit für rechtssichere KI-Entwicklung?

Wir begleiten Sie transparent – von der ersten Frage bis zur Unterzeichnung des AVV.

- Kostenlose Erstberatung
- AVV sofort verfügbar
- DSB beratend tätig
- Individuelle Lösungen

KONTAKT



ADRESSE

Devware GmbH

Luhnsfelder Höhe 50 · 42369 Wuppertal



E-MAIL

kontaktanfragen@devware.de

Datenschutz: datenschutz@devware.de



TELEFON

+49 202 478269-10

Mo – Fr · 9:00 – 17:00 Uhr



WEBSITE

www.devware.de

Software · Consulting · Service

EXTERNER DATENSCHUTZBEAUFTRAGTER

heyData GmbH

Schützenstr. 5 · 10117 Berlin · datenschutz@heydata.eu

Nächste Schritte für Ihr Projekt

- 1 Erstgespräch vereinbaren**
Sprechen Sie uns direkt an – wir besprechen, wie KI in Ihrem laufenden Projekt optimal eingesetzt wird.
- 2 AVV erhalten & prüfen**
Sie erhalten unseren fertigen AVV inkl. aller Anlagen (KI-Tools, TIA, SCCs). Prüfzeit: 14 Tage.
- 3 Fragen klären**
Bei Bedarf besprechen wir offene Punkte gemeinsam mit unserem externen DSB (heyData GmbH).
- 4 Unterzeichnung & Projektstart**
Nach beidseitiger Unterzeichnung starten wir rechtssicher in das Projekt.

Ihr direkter Ansprechpartner

Wir sind Ihr direkter Ansprechpartner für alle Fragen rund um KI, Datenschutz und Ihr Projekt. Melden Sie sich jederzeit.

datenschutz@devware.de · +49 202 478269-10