BotCore.

CHECKLISTE

DSGVO-Chatbot-Checkliste

10 Punkte für konforme KI-Kommunikation auf Ihrer Website. Praxisnah, verständlich und direkt umsetzbar — von der Rechtsgrundlage bis zum Verarbeitungsverzeichnis.

Zielgruppe	Stand	Umfang
Unternehmen mit KI-Chatbot	**März 2026**	**10 Prüfpunkte + AVV-Protokoll**

Warum diese Checkliste?

KI-Chatbots verarbeiten personenbezogene Daten — oft ohne dass sich Betreiber dessen bewusst sind. IP-Adressen, Chat-Verläufe, Namen, E-Mail-Adressen und manchmal sogar Gesundheitsdaten fließen durch das System. Seit dem EU AI Act (August 2025 in Kraft) kommen zusätzliche Transparenzpflichten hinzu.

Diese Checkliste hilft Ihnen, Ihren Chatbot DSGVO-konform und AI-Act-kompatibel zu betreiben. Sie ersetzt keine Rechtsberatung, gibt aber eine praxistaugliche Orientierung.

> **Hinweis:** Diese Checkliste gilt für alle KI-Chatbots — unabhängig vom Anbieter. Die Punkte sind allgemeingültig und basieren auf der DSGVO, dem BDSG und dem EU AI Act.

10-Punkte-Checkliste

☐ 01 **Rechtsgrundlage prüfen**

Art. 6 Abs. 1 DSGVO

Für jeden Chatbot brauchen Sie eine Rechtsgrundlage für die Datenverarbeitung. Die zwei relevantesten:

- **Einwilligung (Art. 6 Abs. 1 lit. a):** Empfohlen, wenn der Chat proaktiv Daten erhebt (Lead-Formulare, E-Mail-Abfrage). Muss aktiv, freiwillig und widerrufbar sein.
- **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f):** Möglich für reine FAQ-Bots ohne aktive Datenerhebung. Erfordert eine dokumentierte Interessenabwägung.
- **Vertragserfüllung (Art. 6 Abs. 1 lit. b):** Wenn der Chat direkt Teil einer Vertragsanbahnung ist (z. B. Terminbuchung).

Dokumentieren Sie Ihre Entscheidung und die Begründung. Ein Wechsel der Rechtsgrundlage im Nachhinein ist problematisch.

02 KI-Transparenzhinweis

EU AI Act Art. 50 Abs. 1

Seit August 2025 müssen Nutzer darüber informiert werden, dass sie mit einem KI-System interagieren. Das gilt für alle KI-Chatbots ohne Ausnahme.

- Der Hinweis muss **vor oder zu Beginn der Interaktion** erfolgen — nicht versteckt im Impressum.
- Empfohlene Umsetzung: Begrüßungsnachricht wie „Ich bin ein KI-Assistent von [Firmenname]. Wie kann ich Ihnen helfen?"
- Zusätzlich: Hinweis in der Datenschutzerklärung mit Verweis auf den EU AI Act.
- Bei Voice-Bots: Mündlicher Hinweis zu Beginn des Gesprächs.

03 AVV mit Chatbot-Anbieter abschließen

Art. 28 DSGVO

Jeder Chatbot-Anbieter, der personenbezogene Daten in Ihrem Auftrag verarbeitet, ist Auftragsverarbeiter. Ohne gültigen AVV ist die gesamte Verarbeitung rechtswidrig.

- Prüfen Sie, ob der Anbieter einen **vorbereiteten AVV** bereitstellt — seriöse Anbieter tun das.
- Achten Sie auf die im AVV genannten Unterauftragnehmer (z. B. Hosting, KI-Provider).
- Ein AVV allein reicht nicht: Sie müssen sich von den technisch-organisatorischen Maßnahmen (TOMs) des Anbieters überzeugen.

Siehe AVV-Prüfprotokoll am Ende dieses Dokuments.

04 Hosting-Standort verifizieren

Art. 44–49 DSGVO (Drittlandtransfer)

Der physische Standort der Server ist entscheidend. Nicht nur der Chatbot-Server zählt — auch der KI-Provider und alle Unterauftragnehmer.

- **EU/EWR-Hosting:** Unproblematisch. Ideallösung für maximale Sicherheit.
- **US-Hosting mit DPF:** Seit dem EU-US Data Privacy Framework (Juli 2023) wieder möglich — aber nur für zertifizierte Unternehmen. Prüfen Sie die DPF-Liste.
- **US-Hosting ohne DPF:** Nur mit Standardvertragsklauseln (SCCs) + Transfer Impact Assessment (TIA). Hoher Aufwand.
- Fragen Sie den Anbieter explizit: Wo werden Chat-Daten gespeichert? Wo läuft das KI-Modell? Werden Daten in Drittländer übertragen?

05 KI-Training mit Kundendaten ausschließen

Art. 5 Abs. 1 lit. b DSGVO (Zweckbindung)

Viele KI-Provider nutzen Nutzerdaten standardmäßig zum Training ihrer Modelle. Für europäische Unternehmen ist das ein massives Problem.

- Prüfen Sie die AGB/DPA des KI-Providers: Wird mit Ihren Daten trainiert? Gibt es ein Opt-out?
- Fordern Sie eine **vertragliche Zusicherung**, dass keine Kundendaten zum Modelltraining verwendet werden.
- Achten Sie auch auf die Unterscheidung zwischen „Training" und „Abuse Monitoring" — letzteres kann ebenfalls eine Datenverarbeitung darstellen.
- Dokumentieren Sie die Zusicherung als Teil Ihrer Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO).

06 Datensparsamkeit umsetzen

Art. 5 Abs. 1 lit. c DSGVO

Erheben Sie nur die Daten, die für den Chatbot-Zweck tatsächlich erforderlich sind.

- Braucht der Bot wirklich den vollständigen Namen? Reicht ein Vorname?
- Definieren Sie klare **Aufbewahrungsfristen** für Chat-Verläufe (Empfehlung: 30–90 Tage, je nach Use Case).
- Implementieren Sie eine automatische Löschung nach Fristablauf.
- Anonymisieren oder pseudonymisieren Sie Daten, wo möglich (z. B. für Analytics).
- Leiten Sie sensible Informationen (Kreditkartennummern, Passwörter) nicht über den Chat — weisen Sie auf sichere Kanäle hin.

07 Cookie-Consent für Chat-Widget konfigurieren

§ 25 TDDDG / ePrivacy

Das Chat-Widget setzt in der Regel Cookies oder nutzt Local Storage. Damit fällt es unter die Cookie-Consent-Pflicht.

- Integrieren Sie den Chat-Widget-Code in Ihre CMP (z. B. CCM19, Cookiebot, Usercentrics).
- Das Widget darf erst **nach Einwilligung** geladen werden — nicht vorher.
- Kategorisierung: Üblicherweise unter „Funktionale Cookies" oder „Marketing", je nach Funktionalität.
- Testen Sie: Wird das Widget wirklich blockiert, wenn der Nutzer ablehnt?
- Alternativ: Prüfen Sie, ob Ihr Chatbot-Anbieter eine Cookie-freie Variante anbietet.

08 Auskunfts- und Löschrechte sicherstellen

Art. 15, 17 DSGVO

Betroffene haben das Recht auf Auskunft über ihre gespeicherten Daten und deren Löschung. Das gilt auch für Chat-Verläufe.

- Stellen Sie sicher, dass Sie Chat-Verläufe eines bestimmten Nutzers **identifizieren und exportieren** können.
- Implementieren Sie einen Prozess für Löschanfragen: Wer ist zuständig? Wie schnell wird gelöscht? (Frist: 1 Monat)
- Prüfen Sie, ob Ihr Chatbot-Anbieter Löschungen auf Einzelnutzer-Ebene unterstützt.
- Dokumentieren Sie den Prozess in Ihrer Datenschutzerklärung.

09 Datenschutzfolgenabschätzung prüfen

Art. 35 DSGVO

Eine DSFA ist erforderlich, wenn die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten" der Betroffenen birgt.

- **DSFA wahrscheinlich erforderlich bei:** Chatbots im Gesundheitswesen, systematischer Profilerstellung, Verarbeitung besonderer Datenkategorien (Art. 9), großflächiger Überwachung.
- **DSFA wahrscheinlich nicht erforderlich bei:** Einfacher FAQ-Bot ohne Datenerhebung, kleines Unternehmen, keine besonderen Datenkategorien.
- Prüfen Sie die **Positivliste der zuständigen Datenschutzaufsichtsbehörde** Ihres Bundeslandes.
- Im Zweifel: Führen Sie eine vereinfachte DSFA durch — sie schadet nicht und dokumentiert Ihre Sorgfalt.

10 Verarbeitungsverzeichnis aktualisieren

Art. 30 DSGVO

Der Chatbot ist ein neuer Verarbeitungszweck und muss in Ihr Verarbeitungsverzeichnis aufgenommen werden.

- Neuen Eintrag anlegen mit: Zweck der Verarbeitung, Kategorien betroffener Personen, Kategorien personenbezogener Daten, Empfänger, Drittlandtransfers, Löschfristen.
- Vergessen Sie nicht die **Unterauftragnehmer** des Chatbot-Anbieters (KI-Provider, Hosting, CDN).
- Aktualisieren Sie auch Ihre **Datenschutzerklärung** auf der Website — der Chatbot muss dort erwähnt werden.
- Benennen Sie einen internen Verantwortlichen für die regelmäßige Überprüfung (mindestens jährlich).

AVV-Prüfprotokoll

Nutzen Sie diese Tabelle, um den Auftragsverarbeitungsvertrag (AVV) Ihres Chatbot-Anbieters systematisch zu prüfen. Alle 8 Punkte müssen im AVV geregelt sein (Art. 28 Abs. 3 DSGVO).

NR.	PRÜFPUNKT	WAS MUSS GEREGELT SEIN?	IM AVV ENTHALTEN?	ANMERKUNG
1	**Gegenstand und Dauer**	Klare Beschreibung, welche Verarbeitung stattfindet und für welchen Zeitraum. Nicht nur „Datenverarbeitung", sondern konkret: „Verarbeitung von Chat-Nachrichten zur automatisierten Beantwortung von Kundenanfragen".		
2	**Art der Daten**	Welche personenbezogenen Daten werden verarbeitet? Z. B.: IP-Adressen, Chat-Inhalte, Namen, E-Mail-Adressen, Telefonnummern, ggf. Gesundheitsdaten.		
3	**Kategorien Betroffener**	Wer sind die betroffenen Personen? Z. B.: Website-Besucher, Kunden, Patienten, Interessenten.		
4	**Unterauftragnehmer**	Liste aller Sub-Auftragsverarbeiter mit Name, Standort und Zweck. Genehmigungsverfahren für neue Unterauftragnehmer (allgemein oder spezifisch).		
5	**Technisch-organisatorische Maßnahmen (TOMs)**	Konkrete Beschreibung der Sicherheitsmaßnahmen: Verschlüsselung (Transport + Speicherung), Zugangskontrollen, Backup, Verfügbarkeit, regelmäßige Überprüfung.		
6	**Weisungsgebundenheit**	Der Auftragsverarbeiter darf Daten nur auf Weisung des		

NR.	PRÜFPUNKT	WAS MUSS GEREGELT SEIN?	IM AVV ENTHALTEN?	ANMERKUNG
		Verantwortlichen verarbeiten. Klarer Prozess für Weisungen und deren Dokumentation.		
7	**Löschpflichten**	Nach Ende der Verarbeitung: Löschung oder Rückgabe aller Daten. Fristen und Verfahren müssen definiert sein. Nachweis der Löschung auf Anfrage.		
8	**Audit-Rechte**	Ihr Recht, die Einhaltung des AVV zu überprüfen — durch eigene Audits, Zertifikate (z. B. ISO 27001) oder Berichte unabhängiger Prüfer.		

> **Achtung:** Ein fehlender oder unvollständiger AVV kann zu Bußgeldern von bis zu 10 Mio. Euro oder 2 % des Jahresumsatzes führen (Art. 83 Abs. 4 lit. a DSGVO). Nehmen Sie diesen Punkt ernst.