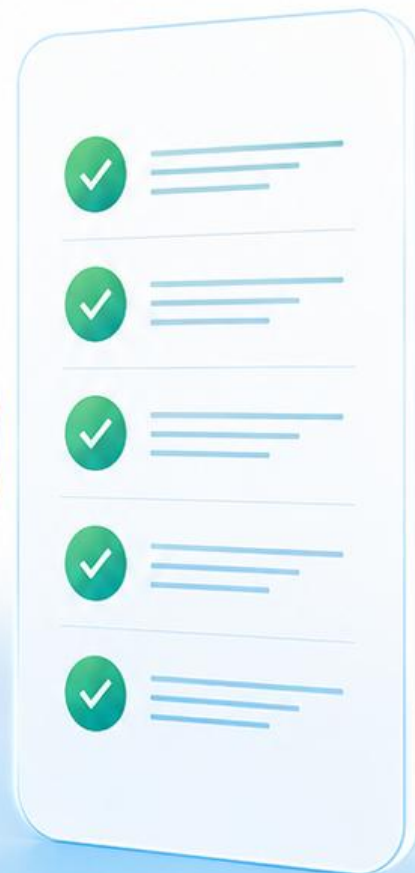


KI-BOTS

Anleitung mit Checklisten für den Einsatz von Voice- und Chatbots für Kundinnen und Kunden unter besonderer Berücksichtigung des Telekommunikationsrechts

©VATM – Version 1/September 2026



Inhaltsverzeichnis

I.	Rechtlicher Rahmen beim Einsatz von Chat- und Voicebots.....	6
1.	Erreichbarkeit und Pflichtangaben	6
2.	Leistungsfähigkeit und Anbieterstruktur	6
3.	Aufzeichnung gesprochener Sprache – strafrechtliche Risiken	7
4.	Transparenz nach KI-VO und DSGVO und die Rechtsgrundlage.....	7
5.	Drittanbieter und Drittlandtransfer	8
6.	Sensible Daten und besondere Einsatzbereiche	8
7.	Keine Irreführung über menschliche Kommunikation im Sinne des Wettbewerbsrechts	9
8.	Potentielle zivilrechtliche Haftung bei Erklärungen des KI-Bots	9
9.	Einschaltung eines Menschen.....	9
10.	Vertragsgestaltung mit dem Anbieter	10
II.	Checkliste mit Kommentaren und Beispielen für den Einsatz des KI-Bot	11
1.	Klassifizierung als KI-System	11
a)	Wurde geprüft, ob der KI-Bot unter den Begriff des KI-Systems im Sinne der KI-VO zu subsumieren ist?	11
b)	Wurde hinreichend geprüft, ob der Chat-Bot ein Hochrisiko-KI-System im Sinne der KI-VO darstellt?.....	11
2.	Erfassung aller KI-Systeme	13
a)	Wurde der KI-Bot und das genutzte KI-System ausreichend dokumentiert und in Ihrem Unternehmen inventarisiert?	13
b)	Wurden hierbei auch KI-Bot-Systeme erfasst, die als Service für Geschäftskunden bereitgestellt werden?	13
3.	Einsatz eines Voice- oder Chatbot-KI-Bots eines anderen Anbieters	13
a)	Wird das System von einem Dritten betrieben oder angeboten?	14
b)	Wurden die Rollen der Parteien nach der KI-VO geklärt?	14
c)	Existiert eine Dokumentation der Verfahren und Anpassungen?.....	15
4.	Training des KI-Systems	15
a)	Wenn Daten für Trainingszwecke genutzt werden – wurden ausreichende Regelungen dafür getroffen?	15
b)	Wurde der Nutzer ausreichend und transparent über das Trainingsverfahren informiert und hat er darin eingewilligt?.....	15
c)	Ist das Trainingsverfahren ausreichend umfassend dokumentiert?	15
d)	Ist deren Einsatz rechtlich zulässig und wurde er soweit möglich minimiert? Wurden Maßnahmen getroffen, um Datenschutzrisiken zu reduzieren?	16
e)	Wird ein fortlaufendes Training oder Adaptieren vorgenommen?	17
f)	Bias-Analysen: Gibt es eine initiale Bewertung, ob das Modell bestimmte Nutzergruppen systematisch benachteiligt?.....	17
5.	Einstufung als Hochrisiko-KI	17
a)	Entspricht das System grundsätzlich den Kriterien einer Hochrisiko-KI?	17
b)	Relevanz nach Anhang III. Ist der Einsatzzweck des Systems in Anhang III der KI-VO genannt?	17

c)	Ist eine nachvollziehbare Dokumentation darüber vorhanden, wie die Einstufung vorgenommen wurde, inkl. Begründungen und ggf. Verweis auf Risikoanalyse oder Ausnahmegründe?	18
d)	Transparenzpflicht bei Interaktion.....	18
6.	Zusätzliche Anforderungen, wenn der Chat- oder Voicebot als Hochrisiko-KI-System einzustufen ist	19
7.	Transparenz- und Dokumentationspflichten (Art. 50 KI-VO).....	19
a)	Direkte Interaktion mit natürlichen Personen (Art. 50 Abs. 1 KI-VO).....	20
b)	Maschinenlesbare Kennzeichnung generierter Inhalte (Art. 50 Abs. 2 KI-VO).....	22
c)	Emotionserkennung und biometrische Kategorisierung (Art. 50 Abs. 3 KI-VO)	22
d)	Deepfakes und Texte zu Angelegenheiten von öffentlichem Interesse (Art. 50 Abs. 4 KI-VO)	23
8.	Risikomanagement-System	25
a)	Die haftungsrechtliche Ausgangslage in der Rechtsprechung	25
b)	Fragen für die Prüfung der organisatorischen und technischen Vorkehrungen	27
9.	Datenschutzrechtliche Grundlagen für den Einsatz von Voice- und Chatbots.....	29
a)	Besteht für den Einsatz und die Nutzung des KI-Bots gegenüber dem Nutzer eine ausreichende datenschutzrechtliche Legitimation?.....	30
b)	Wurde geprüft, ob der KI-Bot oder ein nachgelagerter Prozess eine ausschließlich automatisierte Entscheidung mit rechtlicher Wirkung oder ähnlich erheblicher Beeinträchtigung im Sinne des Art. 22 DSGVO trifft oder maßgeblich vorbereitet?	31
c)	Werden mit dem KI-Bot-System sensible Nutzerdaten nach Art. 9 DSGVO erhoben oder sonst wie verarbeitet?	31
d)	Werden nicht mehr erforderliche Daten nach dem Wegfall des Nutzungszweckes verlässlich gelöscht?.....	31
e)	Wurden die technischen und organisatorischen Maßnahmen eines etwaigen Drittanbieters geprüft und sind diese ausreichend?.....	32
f)	Wurde eine datenschutzfreundliche Technikgestaltung gewählt und implementiert?	32
10.	Nutzung im TK-Umfeld & regulatorische Besonderheiten	33
a)	Einsatzkontext: Wird das KI-System im Netzbetrieb oder im Kundendienst eingesetzt?	33
b)	Sind die telekommunikationsrechtlichen Anforderungen berücksichtigt worden?	33
c)	Besonderheiten bei Sprachmitschnitten oder Transkription im Rahmen von Voicebots.	34
d)	Ist diese Einwilligung zum eigenen Schutz dokumentiert und widerrufbar und wurden die Datenschutzhinweise einbezogen?	34
e)	Besonderheiten bei Sicherheit & Störfallvorsorge im Rahmen der Netzwerksteuerung.	34
f)	Zusätzliche Maßnahmen im Rahmen der Qualitätssteuerung	35
11.	Vertragliche Absicherung mit Anbietern/Betreibern	35
a)	Verträge mit KI-Anbietern	35
b)	Enthalten die Verträge Regelungen zu Audit-Rechten oder Überprüfungs-möglichkeiten?	35
c)	Ist ein den deutschen Vorschriften entsprechender Auftragsverarbeitungsvertrag abgeschlossen, falls der KI-Anbieter in Ihrem Auftrag personenbezogene Daten verarbeitet?	36
d)	Datenverwendung durch Anbieter begrenzt: Wurde vertraglich festgehalten, dass der Anbieter keine Rechte an Ihren Daten erhält bzw. wurden in Bezug auf die Daten eindeutige Regelungen erstellt?	36
e)	Wurden die Rechte zum Training eines KI-Modells durch Dritte und zur Sicherung eventueller Urheberrechte geprüft?	36
12.	Monitoring und Nachbetrieb	37
a)	Ist eine laufende Überwachung der KI-Systeme vorgesehen?	37
b)	Werden Bias und diskriminierende Tendenzen im Betrieb überwacht?	37
c)	Change-Management.....	37

d)	Gibt es einen Melde- und Reaktionsplan für Zwischenfälle?	37
e)	Nicht zwingend, aber sehr sinnvoll ist ein Feedback der Nutzer.....	38
13.	Schulung & Bewusstseinschärfung für Probleme.....	38
a)	Sind die Mitarbeitenden über die Anforderungen des AI-Acts und den korrekten Umgang mit KI-Systemen geschult?	38
b)	Gibt es interne Richtlinien zur Einführung und Nutzung neuer KI-Systeme?	38
c)	Werden Mitarbeiter ausdrücklich darauf hingewiesen, was sie bei Nutzung von generativen KI-Tools nicht machen dürfen?	38
d)	Umfasst die Schulung auch die Beachtung sonstiger Rechtsgüter?	38
e)	Werden der rechtliche Rahmen und die richterlichen Vorgaben kontinuierlich verfolgt?	39
14.	Datenschutz-Folgenabschätzung/Netz- und Informationssicherheit	39
a)	Ist eine Datenschutz-Folgenabschätzung (DSFA) erforderlich?	39
b)	Liegt für alle Verarbeitungen personenbezogener Daten eine gültige Rechtsgrundlage vor (Interessenabwägung)?.....	39
c)	Sind das TKG und die TDDDG-Vorgaben zum Datenschutz einschlägig und wurden deren Vorgaben beachtet?	40
d)	Entspricht der Betrieb des KI-Systems den Anforderungen an Netz- und Informationssicherheit gemäß TKG und gängigen Standards?	40
e)	Wurden die Verantwortlichkeiten für die IT-Sicherheit angemessen berücksichtigt?	40
f)	Wurde der KI-Bot im Rahmen des Löschkonzepts angemessen berücksichtigt?	41
ANHANG		42
I)	Glossar	42
	Anbieter.....	42
	Betreiber.....	42
	Entwickler (nicht definiert in der KI-VO).....	43
	KI-System (nach Art. 3 Nr. 1 KI-VO).....	44
II)	Allgemeiner unverbindlicher Textvorschlag für die Webseite.....	46
III)	Unverbindlicher Textvorschlag für einen allgemeinen Textblock in einer Datenschutzerklärung	46

Verfasser: RA Alexander Ditscheid (alexander.ditscheid@kanzlei-ditscheid.de) und RA Dr. Axel Spies (aspies@potomacclaw.com).

Die Nutzungsrechte an dieser Anleitung (§ 31 UrhG) stehen dem VATM sowie den Autoren jeweils selbständig zu.