CX QUICK GUIDE 4

DATENSICHERHEIT & GOVERNANCE

SO BEHALTEN SIE DIE KONTROLLE ÜBER KI IM KUNDENKONTAKT

INHALT

WESHALB SIND GOVERNANCE UND SICHERHEIT SO WICHTIG? 3

MENSCHLICH AUSGERICHTETE KI ALS AUSGANGSPUNKT 4

COMPLIANCE ALS WEITERE BEDINGUNG 4

SHADOW AI: DIE VERBORGENE GEFAHR 5

PRAKTISCHE UMSETZUNG EINER GUTEN GOVERNANCE 6

DIE BEDEUTUNG VON GOVERNANCE FÜR KUNDEN 7

HÄUFIGE PROBLEME BEIM EINSATZ VON KI 8

ZUSAMMENGEFASST 9

DIE DDM-METHODIK FÜR DEN VERANTWORTUNGSVOLLEN EINSATZ VON KI 10

ÜBER DDM 11

Künstliche Intelligenz (KI) kann die Kundenkommunikation intelligenter, schneller und persönlicher machen, sofern sie mit Sorgfalt eingerichtet wird.

Die Stichworte lauten hierbei Datensicherheit, Governance und menschliche Ausrichtung.

Ohne klare Regelungen bestehen Risiken: von sensiblen Kundendaten, die öffentlich werden, über „Shadow AI“, die außerhalb der Kontrolle der IT-Abteilung genutzt wird, bis zu automatisierten Entscheidungen, die für Kunden nicht nachvollziehbar sind.

In dieser Kurzanleitung wird beschrieben, wie Sie KI auf sichere, transparente und zuverlässige Weise einsetzen – mit Kundenzufriedenheit und Vertrauenswürdigkeit als höchstem Ziel.

WESHALB SIND GOVERNANCE UND SICHERHEIT SO WICHTIG?

Contact Center sind leider ein beliebtes Ziel von Cyberkriminellen. Es gibt viele Anwender, sie sind oft rund um die Uhr in Betrieb und es werden große Mengen sensibler Daten verarbeitet, wie zum Beispiel Gesprächsaufnahmen, Chat-Protokolle oder Kundenprofile.

Ein Risiko besteht darin, dass diese Daten mit künstlicher Intelligenz verarbeitet werden. Dabei kann mangelnde Sorgfalt zu Datenverlusten, Rufschädigung und hohen Strafzahlungen führen. Deshalb ist Datensicherheit keine Nebensächlichkeit, sondern zwingende Voraussetzung – nicht nur, um Risiken zu begrenzen, sondern auch, um Kundenvertrauen zu bewahren und die Befolgung von Gesetzen und Vorschriften zu belegen.

> Mangelnde Sorgfalt bei der Verwendung von KI kann zu Datenverlusten, Rufschädigung und hohen Strafzahlungen führen.
> **Deshalb ist Datensicherheit zwingende Voraussetzung**

MENSCHLICH AUSGERICHTETE KI ALS AUSGANGSPUNKT

Es ist wichtig, zu betonen, dass der Einsatz von künstlicher Intelligenz im Kundenkontakt kein Selbstzweck sein darf. Sie sollte immer messbare Vorteile für Kunden bieten: schnellere Lösungen, weniger Wiederholung und persönlicherer Service. Technik darf nie das menschliche Maß verlieren.

„Menschlich ausgerichtete KI“ bedeutet, dass die Technologie Kunden und Mitarbeitende unterstützt, Entscheidungen erklärbar macht und die Kundenbeziehung verstärkt statt ersetzt. Dafür sind folgende Eigenschaften unverzichtbar:

Transparenz:
Kunden müssen wissen, wann ein KI-Bot antwortet und wie sie jederzeit einen Mitarbeiter erreichen können.

Wahlfreiheit:
Eine KI-Antwort ist praktisch, aber der Kunden muss auf einfache Weise zu einem menschlichen Mitarbeiter wechseln können.

Ehrliche Daten:
Die Modelle dürfen keinen Bias (Voreingenommenheit) verstärken. Dabei helfen repräsentative Datensets und regelmäßige Tests auf Verzerrung.

Überwachung:
Komplexe oder sensible Entscheidungen müssen stets unter menschlicher Kontrolle bleiben.

COMPLIANCE ALS WEITERE BEDINGUNG

Da Organisationen immer mehr sensible kunden- und personenbezogene Daten verarbeiten, steht Compliance in nahezu jeder Branche hoch auf der Tagesordnung. Neben der DSGVO gibt es weitere Vorschriften; in den Niederlanden beispielsweise Wft und DORA für Finanzinstitute, NIS2 für die Netz- und Informationssicherheit oder NEN 7510 für die Pflegebranche. Datensicherheit und Compliance sind dabei untrennbar verbunden: Ohne einen adäquaten Schutz ist eine Einhaltung schlicht nicht möglich.

Der sorglose Einsatz von künstlicher Intelligenz kann risikoreich sein, doch wenn sie ordnungsgemäß eingerichtet und gesteuert wird, bietet KI sogar Möglichkeiten, um Compliance zu unterstützen. Beispiele sind automatische Warnungen bei Abweichungen, das Überwachen von Gesprächen auf Regelverstöße oder schnellere und bessere Berichte. KI ist dann nicht nur ein Risiko, das beherrscht werden muss, sondern auch ein Hilfsmittel für mehr Kontrolle.

SHADOW AI: DIE VERBORGENE GEFAHR

Im Arbeitsalltag nutzen Mitarbeiter durchaus eigene KI-Tools, um schneller zu arbeiten, zum Beispiel ChatGPT oder kostenlose Transkriptions-Apps. Das mag gut gemeint sein, aber liegt meist außerhalb der Kontrolle der IT- oder der Sicherheitsabteilung. Gerade wenn viel Betrieb in einem Contact Center herrscht, ist die Versuchung groß, externe Tools einzusetzen, die Zeit und Aufwand sparen.

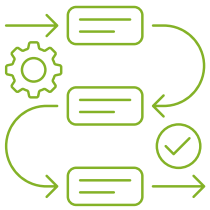
Dieses Phänomen – „Shadow AI“ – kann zu folgenden Gefahren führen:

- Sensible Kundendaten geraten unbeabsichtigt in externe Systeme
- Uneinheitliche Antworten und Prozesse
- Verlust der Kontrolle darüber, welche KI-Hilfsmittel eingesetzt werden

Eine Untersuchung von Zendesk zeigte, dass mittlerweile fast die Hälfte aller Support-Mitarbeitenden eine Form von Shadow AI für ihre Zwecke am Arbeitsplatz benutzt. 1) Das Problem ist also sehr konkret – und zugleich ein Zeichen dafür, dass Ihre Mitarbeitenden bereit für Innovation im Contact Center sind.

Jetzt ist die richtige Gelegenheit, sichere, zugelassene Alternativen bereitzustellen, statt KI einfach zu verbieten.

1) Zendesk: CX-Trends 2025



PRAKTISCHE UMSETZUNG EINER GUTEN GOVERNANCE

Wie sorgen Sie dafür, dass KI in Ihrer Organisation beherrschbar und sicher bleibt? Mit einem Governance-Konzept legen Sie die Leitplanken für den verantwortlichen Einsatz fest, um Risiken strukturell zu begrenzen. Eine effektive Governance kann auf folgenden konkreten Bausteinen basieren:

1. Klare Verantwortlichkeiten

Legen Sie fest, wer beim Einsatz von KI entscheidet. Wer ist Eigentümer der Daten, wer beurteilt ethische Aspekte, wer ist Sicherheitsverantwortlicher und wer genehmigt neue Werkzeuge? Definieren Sie genau, wie Entscheidungen getroffen werden und wie Freigaben erfolgen, damit die Rollen und mögliche Eskalationsstufen klar sind.

2. Datensparsamkeit und Datenschutz

Speichern Sie nur, was für den Nutzungszweck erforderlich ist. Anonymisieren oder maskieren Sie sensible Felder. Legen Sie Speicherfristen bzw. Aufbewahrungsdauern fest und nutzen Sie Zugriffskontrolle und Verschlüsselung, um eine unerwünschte Offenlegung von Kundendaten zu vermeiden.

3. Transparenz gegenüber Kunden

Informieren Sie Kunden auf verständliche Weise, wann und weshalb KI verwendet wird, welche Daten genutzt werden und inwieweit sie selbst entscheiden können (z. B. per Opt-out). Stellen Sie für automatisierte Entscheidungen kurze Erklärungen und Möglichkeiten zur Rückfrage oder zur Beschwerde bereit.

4. Menschliches Eingreifen

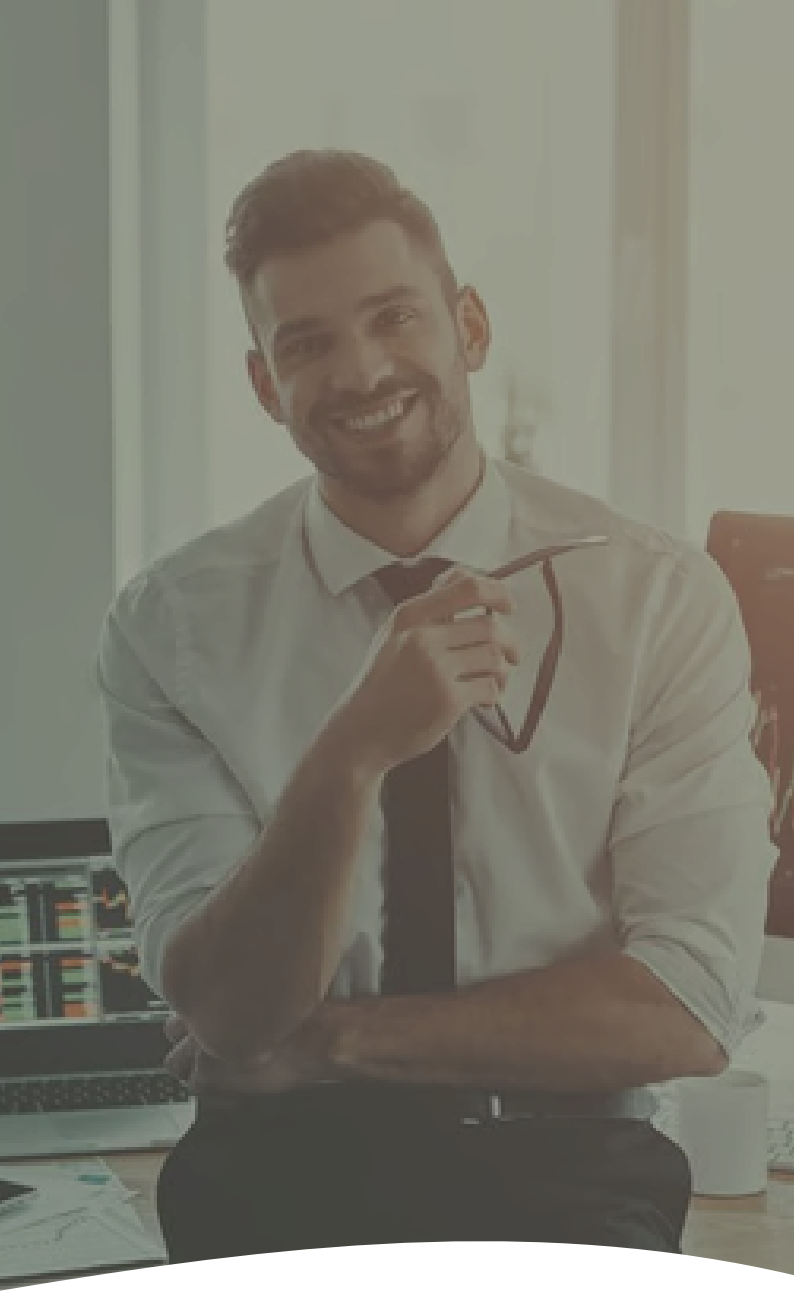
Es sollte stets eine unkomplizierte Übergabe an einen Mitarbeiter möglich sein, wobei der Interaktionskontext bestehen bleiben sollte, und es sollte standardmäßig eine Möglichkeit zur menschlichen Überprüfung bei Zweifeln oder Beschwerden geben. Dadurch erhöhen Sie die Vertrauenswürdigkeit und vermeiden Eskalationen.

5. Qualitätssicherung

Kontrollieren Sie regelmäßig die Korrektheit der Transkriptionen und die Leistung der Modelle. Mit stichprobenartigen Audits und automatischen Warnungen (z. B. bei sinkender Kundenzufriedenheit oder mehr falschen Treffern) können Sie anschließend Updates oder Trainings einplanen.

6. Kontrolle von Shadow AI

Legen Sie Richtlinien für Mitarbeitende fest: Welche KI-Tools sind erlaubt? Zu welchen Zwecken dürfen diese eingesetzt werden? Wie wird Sicherheit gewährleistet? Kommunizieren Sie, welche Alternativen erlaubt sind, geben Sie klare Leitlinien vor und führen Sie Mitarbeitertrainings durch.



DIE BEDEUTUNG VON GOVERNANCE FÜR KUNDEN

Eine gute Governance- und Sicherheitspolitik ist mehr als nur das Einhalten von Vorschriften. Sie verbessert das Kundenerlebnis und sorgt für Vertrauenswürdigkeit und Berechenbarkeit bei jedem Berührungspunkt.

Daraus ergeben sich konkrete Vorteile für Kunden:

- **Schnellere Lösungen** – Der Kunde erhält schneller Hilfe, da KI auf sichere Weise mit aktuellen und vollständigen Kundendaten verknüpft ist.
- **Mehr Zuverlässigkeit** – eindeutige Antworten über alle Kanäle hinweg, ohne widersprüchliche Informationen.
- **Höhere Vertrauenswürdigkeit** – Kunden wissen, dass ihre Daten sorgfältig behandelt und geschützt werden.
- **Weniger Frust** – Es ist stets eine unkomplizierte Übergabe an einen Mitarbeiter möglich, wenn es Probleme mit der KI gibt.

Diese Vorteile entstehen nicht von selbst. In der Praxis zeigt sich, dass ohne klare Regelungen und ohne Überwachung schnell Fehler auftreten. Wir stellen vor, wo es am häufigsten zu Schwierigkeiten kommt – und wieso Sie genau dort handeln sollten.

> Eine gute Governance- und Sicherheitspolitik ist mehr als nur das Einhalten von Vorschriften.

HÄUFIGE PROBLEME BEIM EINSATZ VON KI

Die Verwendung von künstlicher Intelligenz bringt zwangsläufig einige Herausforderungen mit sich. Wir stellen die häufigsten Schwierigkeiten vor, zusammen mit kurzen und praktischen Tipps, wie Sie diese umschiffen.

Blindes Vertrauen in KI-Output

Künstliche Intelligenz kann beeindruckend antworten, aber das schützt nicht vor Fehlern oder ausgedachten Informationen („Halluzination“). Wenn Mitarbeiter oder Kunden den Output unkritisch übernehmen, kann dies zu Missverständnissen und Fehlern führen.

Eine Überprüfung durch Menschen ist daher immer notwendig.

> KI sollte stets einen ‚Notausgang‘ bieten: die Möglichkeit, zu einem menschlichen Mitarbeiter zu wechseln, mitsamt dem vollständigen Kontext.

Das Thema „Governance“ verschieben

Viele Organisationen gehen begeistert mit KI ans Werk, ohne sich Gedanken um Richtlinien und Vorgaben zu machen. In kleinem Maßstab mag das funktionieren, aber sobald die Pilotprojekte hochskaliert werden, entstehen Risiken in Bezug auf Daten, Zuständigkeiten und Compliance. Daher sollte immer erst ein Governance-Rahmen aufgebaut werden.

Keine eindeutige Option zur Übergabe an menschliche Mitarbeiter

Es kann zu Frust und Vertrauensverlust führen, wenn ein Problem in Interaktion mit einem Bot nicht gelöst werden kann und es keinen Weg zu einem Mitarbeiter gibt. KI sollte stets einen „Notausgang“ bieten: die Möglichkeit, zu einem menschlichen Mitarbeiter zu wechseln, mitsamt dem vollständigen Kontext.

Shadow AI ignorieren

Mitarbeitende setzen möglicherweise externe Tools ein, wenn genehmigte Alternativen fehlen. Verbote sind dabei oft kontraproduktiv. Stattdessen sollten klare Regeln aufgestellt und sichere, genehmigte Optionen angeboten werden, kombiniert mit Training und Sensibilisierung.

ZUSAMMENGEFASST

Der Nutzen von künstlicher Intelligenz entsteht nicht nur durch Schnelligkeit und Effizienz, sondern vor allem durch Vertrauenswürdigkeit. Governance und Sicherheit bilden das Fundament dafür. Ohne klare Regelungen zu Daten und Entscheidungen riskieren Sie, Kunden zu verlieren. Organisationen, die ihre KI transparent und menschlich ausgerichtet gestalten, gewinnen etwas Wertvolleres als Technologie, nämlich Loyalität.

Sicher, erklärbar und von Menschen kontrollierbar, von Beginn an: Wenn Sie dies gewährleisten, ist KI nicht nur eine technische Innovation, sondern ein Instrument, um Vertrauen und Kundenbeziehungen zu stärken.

DIE DDM-METHODIK FÜR DEN VERANTWORTUNGSVOLLEN EINSATZ VON KI

Wir von DDM Consulting glauben an einen pragmatischen Ansatz: erst die Basis, dann der Hype. Für KI im Kundenkontakt bedeutet das, dass wir nicht mit einzelnen Tools oder Experimenten beginnen, sondern mit einem soliden Fundament: klare Governance, sichere Datenflüsse und transparente Prozesse.

Wir folgen einer schrittweisen, dynamischen Roadmap nach dem Ansatz der kontinuierlichen Verbesserung, womit KI beherrschbar, flexibel und zielgerichtet bleibt. Diese Roadmap lässt sich immer an alle Veränderungen in Ihrer Organisation und die technologischen Entwicklungen im Contact-Center-Umfeld anpassen.

Unser Ansatz für Governance und menschlich ausgerichtete KI in drei praktischen Schritten:

1. Bestandsaufnahme und Priorisierung – Wir analysieren Ihre derzeitigen KI-Tools, Datenquellen und Prozesse mitsamt den zugehörigen Risiken. Dabei priorisieren wir konkrete Problemstellen und Quick Wins, um anschließend schnell Mehrwert und Sicherheit erzielen zu können.

2. Governance-Einrichtung und -Implementierung – Wir entwickeln ein Governance-Framework mit Fokus auf klar definierten Rollen, Datensparsamkeit und Transparenz. Danach bauen wir sichere KI-Workflows auf, die Kunden tatsächlich helfen und bei Bedarf eine nahtlose Übergabe an einen Servicemitarbeiter ermöglichen.

3. Optimierung und Skalierung – Auch nach der Bereitstellung messen wir kontinuierlich Leistung, Sicherheit und Kundennutzen. Wir skalieren in Phasen und liefern, falls erforderlich, passgenaue Integrationen, sodass Sie innovativ agieren können, ohne von einem Anbieter abhängig zu sein.

Auch wenn Ihre Plattform nicht alle gewünschten Funktionen im Bereich Datensicherheit und Governance bietet, denken wir mit Ihnen gemeinsam weiter. Bei Bedarf entwickeln wir maßgeschneiderte Zusatzfunktionen, damit Sie die Kontrolle über den Einsatz von KI behalten und das Vertrauen Ihrer Kunden stärken.

Orte

Niederlande
Lange Dreef 11-C
4131 NJ Vianen
T: +31 347 322 551

Belgien (HQ)
Campus Blairon 488
2300 Turnhout
T: +32 14 40 50 10

Deutschland (Köln)
Im Mediapark 5
50670 Köln
T: +49 221 9820 9760

Deutschland (Stuttgart)
Tübinger Strasse 61
70178 Stuttgart
T: +49 711 6648 5040

info@ddmconsulting.eu
www.ddmconsulting.eu

ÜBER DDM

Bei DDM Consulting wissen wir: Eine „One-size-fits-all"-Lösung funktioniert bei der Auswahl einer Kundenkontaktplattform nicht. Jedes Unternehmen ist einzigartig.

Deshalb bieten wir Ihnen eine breite Auswahl an etablierten Contact-Center-Lösungen und beraten Sie auf Basis von über 20 Jahren Erfahrung im Kundenkontakt.

Evolution statt Revolution

Gemeinsam mit Ihnen analysieren wir Ihre bestehenden Contact-Center-Prozesse und definieren die Anforderungen an Ihre zukünftige Plattform. Wir beraten Sie und unterstützen Sie dabei, effizientere Workflows zu entwickeln, die – wo sinnvoll – durch KI unterstützt werden.

Auf dieser Grundlage erstellen wir eine dynamische Roadmap, die den Übergang zu einem leistungsfähigeren Contact Center strukturiert und gut umsetzbar macht.

Proaktiv mit moderner Technologie arbeiten

Diese Roadmap bleibt auch nach der Einführung Ihrer neuen Plattform zentraler Bestandteil der Zusammenarbeit. Sie entwickelt sich kontinuierlich weiter – im Einklang mit Veränderungen in Ihrem Unternehmen und neuen Entwicklungen im Bereich der Contact-Center-Technologie. Unsere Expertinnen und Experten bewerten jede neue Version im Hinblick auf ihren konkreten Mehrwert für Sie. Dabei handeln wir proaktiv, damit Sie stets über die relevanten Entwicklungen informiert sind und diese optimal nutzen können.

Individuelle Lösungen für besseren Kundenkontakt

Suchen Sie nach spezifischen Funktionen, die im gewählten System (noch) nicht verfügbar sind? Dann entwickeln wir bei Bedarf passgenaue Erweiterungen, die exakt auf Ihre Anforderungen zugeschnitten sind. Unser Team vereint fachliche und technische Expertise, um das volle Potenzial Ihrer Lösung auszuschöpfen – auch dann, wenn Sie sich für eine Standardplattform entschieden haben.

Mit DDM Consulting entscheiden Sie sich für einen proaktiven und kreativen Ansatz zur Weiterentwicklung Ihrer Customer Experience.