



AGENTISCHE BÜRGER- INTERAKTION

WIE KI-AGENTEN
VERWALTUNGSARBEIT
NEU ORGANISIEREN

ORIENTIERUNGSPAPIER

INHALT

EXECUTIVE SUMMARY	3
DER WEG ZUR HANDLUNGSFÄHIGEN VERWALTUNG	4
DREI STUFEN DER AGENTISCHEN BÜRGERINTERAKTION	5
DIE WEGBEREITER DES AGENTISCHEN KI-ZEITALTERS	14
RESPONSIBLE AI UND GOVERNANCE ALS VERTRAUENSSTIFTER	18
AGENTISCHE KI UMSETZEN	20
FAZIT	25

EIN WORT VORAB

Dieses Orientierungspapier gibt eine strategische Einordnung für Führungskräfte der öffentlichen Verwaltung und ist keine Technologiespezifikation. Es skizziert die Vision agentischer Bürgerinteraktion in drei Entwicklungsstufen und zeigt, unter welchen Voraussetzungen sie realisierbar ist.

Wir wünschen Ihnen eine spannende Lektüre und wertvolle Impulse!

EXECUTIVE SUMMARY

Agentische KI-Systeme ermöglichen einen fundamentalen Wandel der Interaktion zwischen Verwaltung und Bürgern. Aktuell zeigen sich mit Agentic Commerce und neuen KI-Agentenlösungen wie OpenClaw (vormals Clawdbot / Moltbot) oder Manus ein erstes Bild und anfängliche Lösungen, mit denen Erfahrungen gesammelt und Möglichkeitsräume für ein anderes Erbringen von Verwaltungsleistungen gedacht werden können.

Diese KI-Systeme unterscheiden sich signifikant von klassischen Chatbots und auch von den Basisversionen bekannter GenAI-Tools wie ChatGPT, Gemini oder Claude. Sie bedienen Browser, greifen auf Dateien zu und orchestrieren Abläufe über verschiedene Systeme hinweg. Sie verfolgen komplexe Aufgaben und verbinden sich selbstständig mit den nötigen Plattformen. Diese neue KI-Ausbaustufe ermöglicht eine nahtlose 24/7-Interaktion in natürlicher Sprache, eliminiert Medienbrüche und senkt den Aufwand für Bürgerinnen und Bürger sowie Mitarbeitende in Behörden.

Der öffentlichen Verwaltung bietet sich die Chance auf einen echten Übergang von der reaktiven und formularbasierten hin zu einer aktiven, antizipierenden und datenbasierten Verwaltungsarbeit. Die Transformation ist notwendig, denn durch demografischen Wandel, Fachkräftemangel und steigende Bürgererwartungen stößt das bisherige Modell der Verwaltungsdigitalisierung an seine Grenzen.

Skalierbarkeit ist dabei der entscheidende strategische Hebel. Repetitive Aufgaben binden heute wertvolle Kapazitäten. Agentische Systeme schaffen Freiräume für wertschöpfende Tätigkeiten und steigern damit die Effizienz. 62 Prozent aller Verwaltungsaufgaben umfassen Schreiben, Lesen und Kommunizieren. Davon sind 60 Prozent durch KI automatisierbar. Rund 40 Prozent der Arbeitszeit könnten also effizienter genutzt werden, wie entsprechende Studien zeigen.

Agentische Bürgerinteraktion lässt sich in drei Evolutionsstufen einteilen:

1. die assistierende 24/7-Verwaltung
2. die souveräne Bürgerinteraktion
3. die autonome Agent-zu-Agent-Verhandlung

Wir stellen die drei Entwicklungsstufen anhand eines konkreten Beispiels vor und zeigen, welche technologischen und organisatorischen Voraussetzungen für eine vertrauenswürdige Umsetzung notwendig sind. Das Papier bietet eine fundierte Grundlage, wie agentische KI frühzeitig in aktuelle Überlegungen zur Verwaltungsdigitalisierung einbezogen werden kann.

DER WEG ZUR HANDLUNGSFÄHIGEN VERWALTUNG

Die Zukunft der öffentlichen Verwaltung liegt nicht in der einfachen Digitalisierung von Prozessen, sondern in deren fundamentaler Neugestaltung. Proaktive Verwaltungsleistungen antizipieren Bedürfnisse und kommen ohne formale Anträge aus. Der Staat wandelt sich vom (zu) bürokratischen Apparat zum Begleiter im Alltag. Bürgerinnen und Bürger nutzen natürliche Sprache statt komplexer Portale, um staatliche Leistungen abzurufen. Das Ziel ist ein reibungsloser, barrierefreier Zugang für alle. Der Anspruch ist richtig, wenngleich die Umsetzung schwierig ist.

Um das Ziel zu erreichen, müssen Verwaltungen immense Herausforderungen meistern wie den Fachkräftemangel, die steigende Aufgabenkomplexität und den Personalabbau. Zudem erwarten Bürgerinnen und Bürger Nutzererlebnisse auf Amazon-, Netflix- und PayPal-Niveau - Standards, die traditionelle Verwaltungsstrukturen kaum leisten können. Veralterte IT-Landschaften und langwierige Beschaffungsprozesse bremsen Innovationen, während die technologische Entwicklung außerhalb der Verwaltung rasant voranschreitet.

REDUKTION DER „TIME TAX“

Agentische KI bietet die Chance, einen großen Sprung zu machen. Der entscheidende Unterschied zu bisherigen Automatisierungsansätzen ist die regelbasierte Autonomie. KI-Agenten übernehmen komplette Prozessketten statt punktueller Aufgaben. Sie treffen Entscheidungen innerhalb definierter Rahmen und orchestrieren Aktivitäten eigenständig.

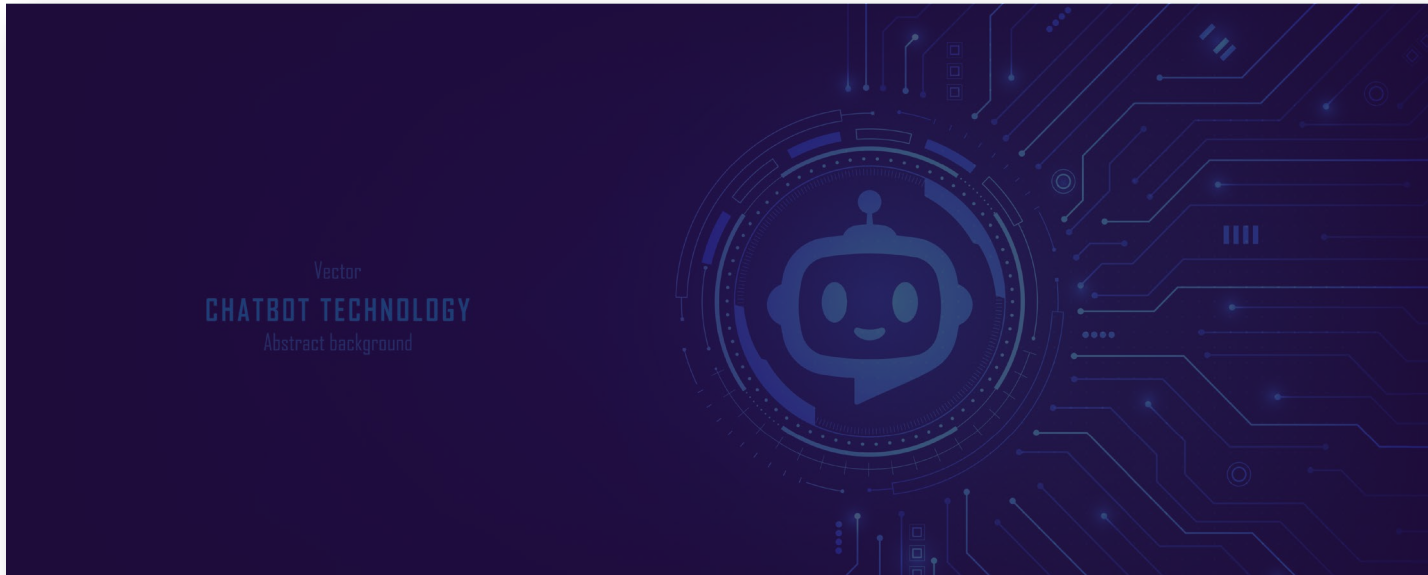
Regelbasierte Autonomie beginnt bei der Priorisierung von Anfragen und endet beim Auslösen von Folgeprozessen. Das Ergebnis ist eine End-to-End-Abwicklung der Abläufe bei 24/7-Verfügbarkeit - etwas, was klassische Bots und auch generative KI bislang nicht geleistet haben und auch nicht leisten können.

Im Zentrum der Transformation steht die Reduktion der „Time Tax“: der Zeitverlust durch bürokratische Hürden. Agentische Systeme eliminieren diese Steuer auf Lebenszeit durch nahtlose Erlebnisse in natürlicher Sprache statt Formularschlachten. Der Rückgriff auf vorhandene Daten aus digitalen Identitätslösungen wie der BundID (und künftig auch EUDI-Wallet¹) verhindert redundante Mehrfacheingaben.

Die Verwaltung zieht sich somit nicht zurück. Sie kommuniziert proaktiv und wirkt im Hintergrund im Sinne der Bürgerinnen und Bürger - und nur so weit, wie diese es zulassen.

¹ Ab 2027 können sich Bürgerinnen und Bürger EU-weit mit dem EUDI-Wallet (European Digital Identity Wallet) authentifizieren. Die BundID fungiert als Schnittstelle, sodass alle angeschlossenen Dienste automatisch EUDI-Wallet-kompatibel werden.

DREI STUFEN DER AGENTISCHEN BÜRGERINTERAKTION



Die Einführung agentischer KI-Systeme in der Verwaltung erfolgt nicht als disruptiver Bruch, sondern in Entwicklungsstufen entlang definierter Reifegrade: die assistierende 24/7-Verwaltung, die souveräne Bürgerinteraktion und die autonome Agent-zu-Agent-Verhandlung. Die drei Stufen bringen jeweils Vorteile für Bürgerinnen und Bürger und sind unterschiedlich komplex in der Umsetzung.

Um diese Stufen greifbar zu machen, begleiten wir exemplarisch die fiktive Bürgerin Sandra Müller, eine alleinerziehende Mutter, die Wohngeld beantragen möchte, durch die drei Entwicklungsstufen. Sandra Müller ist 38 Jahre alt, arbeitet in Teilzeit als Verkäuferin in einem Baumarkt und zieht ihre beiden Kinder – sieben und zehn Jahre alt – allein groß. Seit der Trennung vor zwei Jahren jongliert

sie zwischen Arbeit, Kinderbetreuung und Haushalt. Kürzlich musste sie ihre Arbeitszeit weiter reduzieren, weil die Betreuungssituation schwieriger wurde. Ihr Einkommen sank dadurch spürbar.

Zeit für Behördengänge hat Sandra praktisch nur abends, wenn die Kinder schlafen. Sie nutzt das Internet für Online-Shopping und Social Media. Komplexe Verwaltungsportale mit Fachbegriffen wie „§ 3 WoGG“ überfordern sie allerdings. Die Absicht, einen Wohngeldantrag auszufüllen – mit all den Nachweisen, Formularen und der Angst, etwas falsch zu machen – hat sie monatelang vor sich hergeschoben. Dabei wäre die finanzielle Entlastung dringend nötig.

STUFE 1: DIE ASSISTIERENDE 24/7-VERWALTUNG

SANDRAS ERFAHRUNG

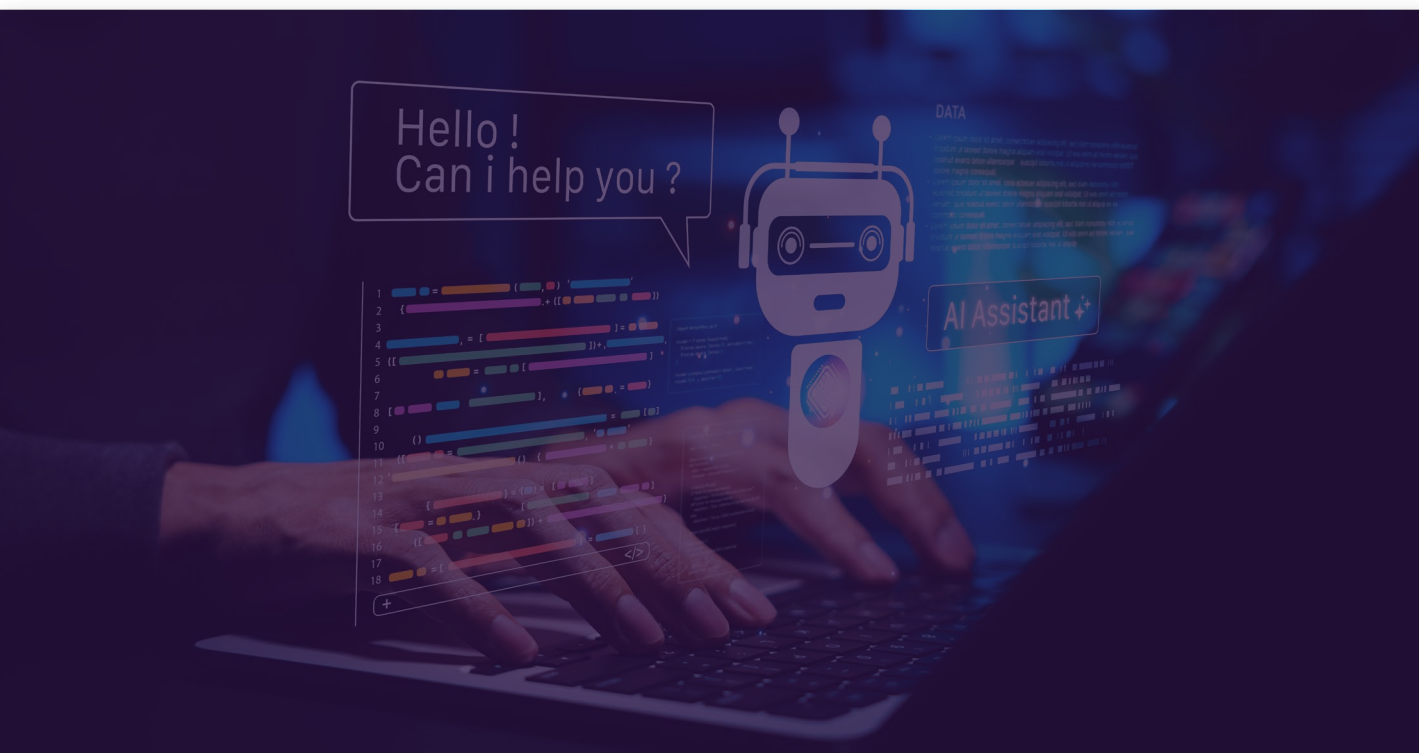
Es ist 21:30 Uhr, die Kinder schlafen endlich. Sandra öffnet die Website ihrer Stadt und klickt auf den Chat-Button. Statt der üblichen „Sie melden sich außerhalb der Öffnungszeiten“-Meldung begrüßt sie ein KI-Avatar in natürlicher Sprache: „Guten Abend, ich bin hier, um Ihnen zu helfen. Was kann ich für Sie tun?“

Sandra tippt: „Ich brauche finanzielle Unterstützung für meine Miete. Mein Einkommen hat sich verändert, und ich weiß nicht, ob ich Anspruch auf etwas habe.“

Der Avatar reagiert sofort: „Ich verstehe. Es klingt, als könnten Sie für Wohngeld infrage kommen. Darf ich Ihnen ein paar Fragen stellen, um das zu prüfen?“ Sandra bejaht und wird durch einen kurzen Dialog geführt: Haushaltsgröße, ungefähres Einkommen, Miethöhe.

Nach zwei Minuten erhält sie die Rückmeldung: „Basierend auf Ihren Angaben, haben Sie voraussichtlich Anspruch auf Wohngeld. Sie können Ihren Antrag online stellen. Ich zeige Ihnen, welche Unterlagen Sie benötigen und wie das Antragsverfahren abläuft.“

Der Avatar erklärt Sandra Schritt für Schritt, was zu tun ist. Er listet benötigte Dokumente auf und bietet an, eine E-Mail mit sämtlichen Informationen zu senden. Sandra kann zudem wählen, ob sie am Tag darauf einen Rückruf von der Wohngeldstelle erhalten möchte – der Avatar trägt sie direkt in die Terminliste ein.



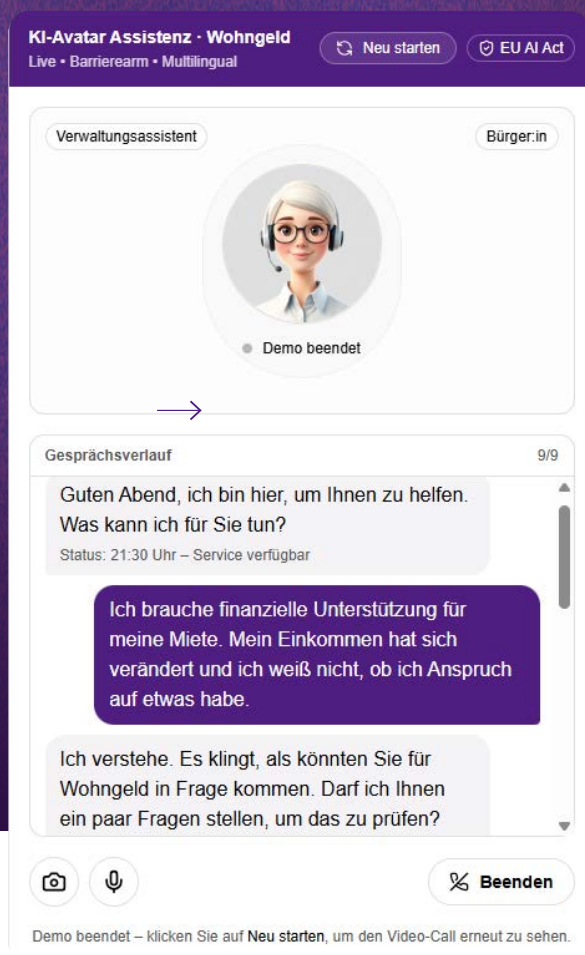
WAS AUS SANDRAS PERSPEKTIVE GESCHIEHT

- Sofortige Orientierung: keine Wartezeiten, 24/7-Verfügbarkeit
- Barrierefreie Kommunikation: Alltagssprache genügt, Fachkenntnisse (z. B. „§ 3 WoGG“) sind nicht erforderlich
- Empathische Interaktion: Die KI erkennt emotionale Signale („Einkommen verändert“) und reagiert angemessen
- Ergebnis: kein Frust, Sandra fühlt sich sofort informiert und handlungsfähig

WAS AUS SICHT DER WOHNGELDSTELLE GESCHIEHT

- Effizienzgewinn: 23 Anfragen über Nacht bearbeitet, davon zwölf vollständig gelöst
- Qualifizierte Arbeitsvorbereitung: Sachbearbeiter Thomas erhält eine priorisierte Rückrufliste mit konkreten Fallinformationen (z. B. „Potenzieller Anspruch, Erstinformation erfolgt“)
- Fokus auf Wertschöpfung: Routinefragen (Öffnungszeiten, Zuständigkeit) entfallen, Konzentration auf komplexe Beratungsfälle
- Proaktive Beratung: Thomas erkennt Zusatzbedarfe (z. B. Kinderzuschlag) bereits vor dem Gespräch
- Qualitätssteigerung: Verbleibende Kontakte sind hochwertige Beratungsgespräche, die menschliches Ermessen erfordern

24/7-VERWALTUNGSSISTENZ



STUFE 2: DIE SOUVERÄNE BÜRGERINTERAKTION

Die zweite Stufe markiert den Übergang von der assistierenden zur befähigenden KI. Hier agiert eine persönliche Bürger-Agentin als Vermittlerin zwischen Individuum und Verwaltung – eine digitale Sachverwalterin, die im Interesse der Bürgerin oder des Bürgers handelt.

SANDRAS ERFAHRUNG

Eine Woche später sitzt Sandra wieder am Laptop. Dieses Mal nutzt sie die neue „Mein Bürger-Assistent“-App, für die sie sich mit ihrer BundID (künftig auch via EUDI-Wallet möglich) angemeldet hat.

Sie spricht direkt in ihr Smartphone: „Ich möchte jetzt den Wohngeldantrag stellen. Ich habe meine Gehaltsabrechnungen und den Mietvertrag hier.“

Ihre persönliche Bürger-Agentin antwortet: „Perfekt, Sandra. Ich führe Sie durch den Prozess. Zunächst hole ich Ihre bereits gespeicherten Daten aus Ihrer BundID – Adresse, Familienstand und Bankverbindung. Ist das in Ordnung?“

Sandra bestätigt. Die Agentin zeigt transparent an, welche Daten sie abrufen. Dann erklärt sie: „Für Ihren Haushalt mit zwei Kindern benötige ich noch: Ihr aktuelles Monatseinkommen, die Höhe Ihrer Miete und Nebenkosten sowie Angaben zu Ihrem Vermögen.“

Sandra fotografiert ihre aktuelle Gehaltsabrechnung mit dem Smartphone. Die Agentin extrahiert automatisch die relevanten Zahlen: „Ich sehe hier ein Nettoeinkommen von 1.850 Euro im letzten Monat. Stimmt das?“ Sandra bestätigt.

Sie tippt die Mietdaten ein, und die Agentin überprüft in Echtzeit die Plausibilität: „Ihre Miete von 920 Euro liegt innerhalb der zulässigen Höchstbeträge für Ihre Stadt und Haushaltsgröße.“

Nach zehn Minuten zeigt die Agentin eine Zusammenfassung: „Ihr Antrag ist vollständig. Basierend auf Ihren Angaben, beträgt Ihr voraussichtlicher Wohngeldanspruch etwa 370 Euro monatlich. Möchten Sie den Antrag jetzt verbindlich einreichen?“

Sandra scrollt durch die Vorschau. Alle Daten sind korrekt in die amtlichen Formulare übertragen. Mit einem Fingertipp und ihrer BundID-PIN reicht sie den Antrag rechtsverbindlich ein. Sie erhält sofort eine Bestätigung und einen Link zum Statusmonitor: „Sie können hier jederzeit sehen, wie weit die Bearbeitung ist. Die durchschnittliche Bearbeitungszeit beträgt aktuell zwölf Tage.“

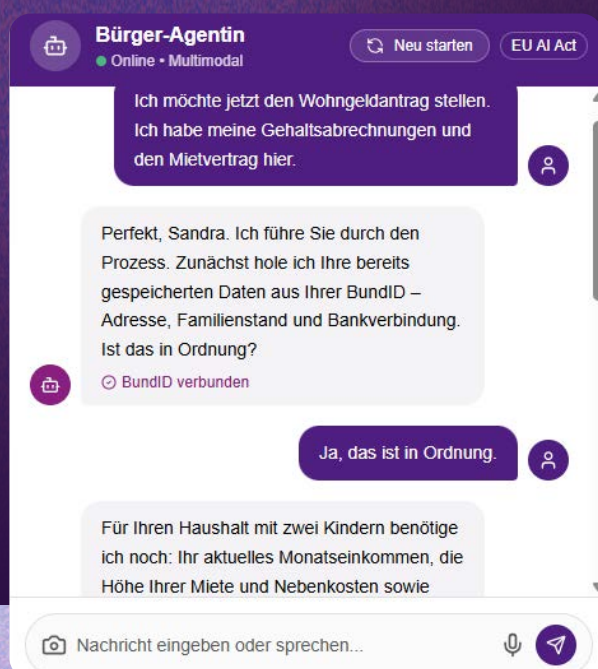
WAS AUS SANDRAS PERSPEKTIVE GESCHIEHT

- Automatisierung: kein manuelles Ausfüllen von Formularen, Kommunikation in natürlicher Sprache und einfacher Dokumenten-Upload per Foto
- Sicherheit und Qualität: Echtzeit-Prüfung auf Vollständigkeit und Plausibilität eliminiert Fehlerangst
- Transparenz: volle Kontrolle über verwendete Daten mit jederzeitiger Korrekturmöglichkeit
- Massive Zeitersparnis: Reduktion des Aufwands von mehreren Stunden auf Minuten reiner Interaktionszeit

WAS AUS SICHT DER WOHNGELDSTELLE GESCHIEHT

- Datenqualität: Antrag liegt vollständig, strukturiert und maschinenlesbar vor, inklusive gültiger BundID-Signatur
- Prozessoptimierung: Wegfall von Rückfragen zu fehlenden Unterlagen oder unleserlichen Angaben
- Fokusverschiebung: sofortiger Einstieg in die inhaltliche Prüfung (Einkommen, Vermögen, Besonderheiten)
- Messbare Erfolge: Die Ablehnungsquote wegen Formfehlern sinkt deutlich. Die Bearbeitungszeit reduziert sich signifikant. Die Bearbeitungskapazität steigt bei gleicher Personalstärke

DIE SOUVERÄNE BÜRGERINTERAKTION



STUFE 3: DIE AUTONOME AGENT-ZU-AGENT-VERHANDLUNG

In der dritten Stufe übernehmen Bürger- und Government-Agenten Aufgaben eigenständig: Sie erkennen relevante Veränderungen, prüfen Ansprüche proaktiv und verhandeln automatisiert miteinander. Der Mensch greift nur noch bei Ausnahmen oder Entscheidungen mit Ermessensspielraum ein.

SANDRAS ERFAHRUNG

Zwei Jahre später hat Sandra die Mein-Bürger-Assistent-App weiterhin installiert. Dieses Mal meldet sich ein Agent bei ihr proaktiv:

„Guten Morgen, Sandra. Ich habe im Einkommensregister eine Veränderung bemerkt: Ihr Arbeitgeber hat für den letzten Monat ein geringeres Einkommen gemeldet. Das könnte Ihren Wohngeldanspruch erhöhen. Möchten Sie, dass ich das für Sie prüfe?“

Sandra ist überrascht. Sie hatte vergessen, dass ihr Teilzeitanteil gesunken war. „Ja, bitte prüf das.“

Ihr Bürger-Agent kommuniziert nun im Hintergrund mit dem Government-Agenten der Wohngeldstelle: Bürger-Agent an Government-Agent: „Antrag auf Wohngeldneuberechnung für Sandra Müller, BundID [verschlüsselte ID]. Einkommensveränderung liegt vor. Benötigte Nachweise?“

Government-Agent an Bürger-Agent: „Einkommensveränderung im Register erkannt. Zusätzlich erforderlich: aktuelle Nebenkostenabrechnung, da letzte vor 13 Monaten eingereicht.“

Bürger-Agent an Sandra (Push-Nachricht): „Ich benötige noch Ihre aktuelle Nebenkostenabrechnung. Bitte fotografieren Sie diese, wenn Sie Zeit haben.“

Sandra fotografiert das Dokument abends. Ihr Agent sendet es automatisch weiter.

Government-Agent (intern): Prüfung durchgeführt. Einkommensrückgang: 230 Euro. Nebenkosten unverändert. Berechnung: neuer Anspruch 485 Euro monatlich (bisher 370 Euro). Erhöhung: 115 Euro. Rückwirkende Nachzahlung: 345 Euro. --> Regelfall, keine Ermessensentscheidung erforderlich. --> Eskalation an Sachbearbeitung für finale Freigabe.

Sachbearbeiterin Lisa Hoffmann erhält eine Benachrichtigung: „Wohngeldneuberechnung Sandra Müller – automatische Prüfung abgeschlossen, Freigabe erforderlich.“ Sie sieht einen vollständig vorbereiteten Bescheid mit Berechnungsdetails, vergleicht stichprobenartig die Werte und gibt den Bescheid frei. Zeitaufwand: zwei bis fünf Minuten. Government-Agent an Bürger-Agent: Bescheid genehmigt. Neuer Wohngeldanspruch: 485, Euro/Monat, rückwirkend ab [Datum]. Nachzahlung: 345, Euro. Auszahlung erfolgt in 3 Werktagen.

Sandra erhält eine Benachrichtigung: „Gute Nachrichten! Ihr Wohngeldanspruch wurde neu berechnet. Sie erhalten ab sofort 485 Euro monatlich und eine Nachzahlung von 345 Euro. Der vollständige Bescheid ist in Ihrem digitalen Postfach abrufbar.“

Die gesamte Interaktion, von der proaktiven Erkennung bis zum genehmigten Bescheid, dauerte vier Tage, davon 90 Prozent reine Systemlaufzeit. Sandras aktiver Zeitaufwand: drei Minuten (Foto machen, Benachrichtigungen lesen).

WAS AUS SANDRAS PERSPEKTIVE GESCHIEHT

- Proaktivität: Das System erkennt Ansprüche automatisch; kein eigener Impuls nötig
- Minimale Interaktion: Einbindung nur bei zwingender Mitwirkung (z. B. Dokumenten-Upload) oder Entscheidungspunkten
- Unsichtbare Verwaltung: maximale Effizienz im Hintergrund statt Belastung mit bürokratischen Details
- Kontrolle ohne Aufwand: Transparenz via Dashboard („Set and Forget“) ohne Notwendigkeit einer aktiven Überwachung
- Entlastung: Wegfall der typischen emotionalen Hürden und des Stresses bei Behördenkontakten

WAS AUS SICHT DER WOHNGELDSTELLE GESCHIEHT

Der Government-Agent handelt autonom. Er ...

- überwacht das Einkommensregister und erkennt Veränderungen
- führt Registerabfragen durch (Melderegister, Einkommensregister)
- nimmt die Neuberechnung nach § 27 WoGG vor

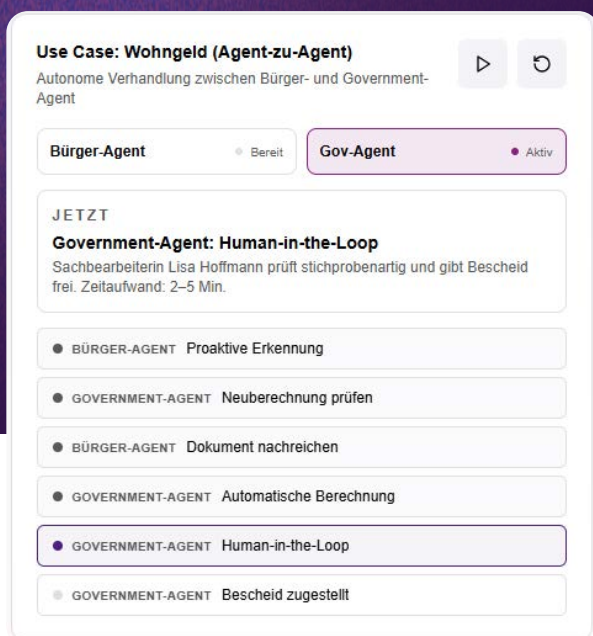
- prüft, ob es sich um einen Regelfall handelt
- bereitet den Bescheid vor und eskaliert ihn zur Freigabe durch einen Menschen

Sachbearbeiterin Lisa fungiert als Qualitätsprüferin und finale Entscheiderin, nicht als administrative Bearbeiterin. Ihr Arbeitsalltag hat sich grundlegend verändert: Eingehende Wohngeldanträge durchlaufen nun den automatisierten Pfad. Sie übernimmt hauptsächlich:

- komplexe Einzelfälle: Selbstständige mit schwankendem Einkommen, Sondervermögen, Härtefälle
- Widersprüche und Beschwerden: Fälle, in denen Bürgerinnen und Bürger mit einer Entscheidung nicht einverstanden sind
- Stichprobenkontrollen: regelmäßige Überprüfung automatisierter Entscheidungen
- die proaktive Beratung: aufsuchende Sozialarbeit für Personen, die digitale Kanäle nicht nutzen können

Die Arbeit ist anspruchsvoller geworden, aber auch befriedigender. Statt endloser Excel-Tabellen und Formularprüfungen ist sie Problemlöserin für Menschen in schwierigen Lebenslagen.

DIE AUTONOME VERHANDLUNG



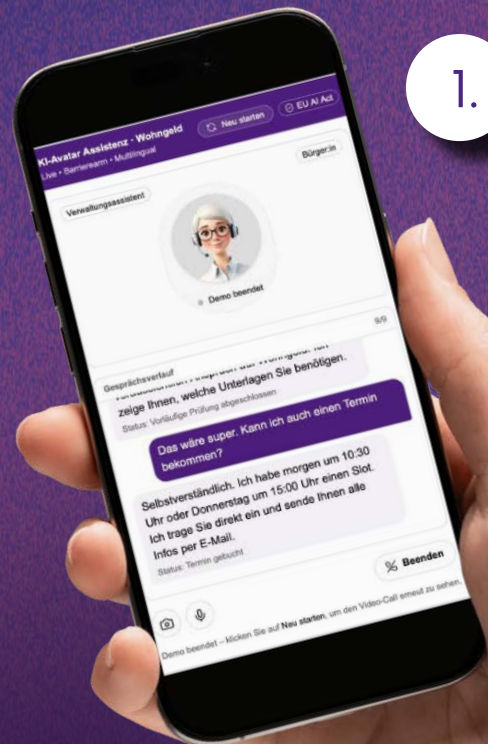
AGENTISCHE BÜRGERINTERAKTION – DIE DREI STUFEN IM ÜBERBLICK

	STUFE 1: 24/7-ASSISTENZ	STUFE 2: SOVERÄNE INTERAKTION	STUFE 3: AUTONOME VERHANDLUNG
CHARAKTERISIERUNG	KI-Avatar beantwortet Anfragen 24/7, bietet Orientierung – Bürger führt Antrag selbst durch	Persönlicher Agent führt durch Antragsprozess, füllt Formulare automatisch aus – Bürger behält Kontrolle	Agenten kommunizieren autonom, erkennen Ansprüche proaktiv – Menschen greifen nur nach Ermessen ein
AUTONOMIE-GRAD	Niedrig – Agent informiert, Mensch handelt vollständig selbst	Mittel – Agent befähigt und strukturiert, Mensch entscheidet und genehmigt	Hoch – Agent handelt eigenständig, Mensch genehmigt oder greift nach Ermessen ein
BÜRGERNUTZEN	- Sofortige Antworten 24/7 - Abbau von Frustration - Verständnis für Ansprüche	- Keine Formularfehler - Medienbruchfreie Antragstellung - Volle Transparenz und Kontrolle	- Proaktive Anspruchserkennung - Nahezu unsichtbare Verwaltung - Minimaler Aufwand (außer bei Mitwirkung)
VERWALTUNGS-NUTZEN	- Entlastung bei Routinefragen - Qualitativ hochwertigere Beratungsgespräche - Bearbeitungszeit unverändert	- Weniger formale Ablehnungen - Strukturierte, vollständige Anträge - Fokus auf inhaltlicher Prüfung - Reduzierte Bearbeitungszeit	- Höhere Bearbeitungskapazität - Fokus auf komplexen Fälle - Ausschließlich Ausnahme- und Ermessensfälle - Qualitätsprüfer statt Formularprüfer - Deutlich reduzierte Bearbeitungszeit
CHANGE-ANFORDERUNGEN	Gering – KI als unterstützende Ergänzung, bestehende Arbeitsweise bleibt weitgehend erhalten	Mittel – neue Arbeitsabläufe mit strukturierten Anträgen, Zusammenarbeit mit Agenten erforderlich	Hoch – fundamentale Transformation der Rollen, Kulturwandel von Vollbearbeitung zu Ausnahmesteuerung
PROZESS-REDESIGN	Minimal – bestehende Prozesse bleiben unverändert, Agent ergänzt bestehende Kanäle	Moderat – Antragsprozesse digitalisieren, Medienbrüche eliminieren, BundID-Integration	Umfassend – Trennung von regelbasierten und ermessensbasierten Schritten, Eskalationslogik definieren, Qualitätskorridore festlegen
GOVERNANCE-KOMPLEXITÄT	Niedrig – begrenzte Entscheidungsbefugnis, Standard-Guardrails ausreichend	Mittel – Human-in-the-Loop bei finaler Einreichung, Consent-Management	Hoch – verpflichtende Human-Überprüfung bei negativen Bescheiden, nach Ermessen, bei Widersprüchen; Stichprobenkontrollen (mind. 10 %)
NEUE ROLLEN	- Prompt Engineer - Chat-Moderator	- Citizen Experience Designer - Data Steward - BundID-Administrator	- Agent Orchestrator - AI Governance Manager - Exception Handler - Quality Assurance Specialist

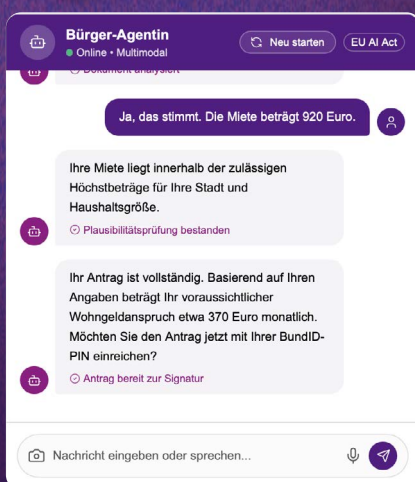
DIE DREI INTERAKTIONS-STUFEN IN AKTION

Eine verlinkte Demo veranschaulicht die drei Stufen agentischer Bürgerinteraktion. Sie vermittelt einen schnellen Eindruck davon, wie die beschriebenen Abläufe praktisch umgesetzt werden können.

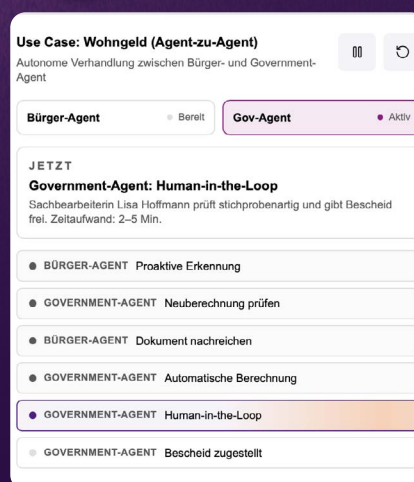
1.



2.



3.


[LINK ZUR DEMO](#)

DIE WEGBEREITER DES AGENTISCHEN KI-ZEITALTERS

Die Entscheidung über den Einsatz von KI-Agenten in der Verwaltung setzt ein klares Verständnis der technologischen und organisatorischen Voraussetzungen voraus. Die folgenden Abschnitte skizzieren die relevanten Bereiche, die den Rahmen für den Einsatz von KI-Agenten in der Praxis spannen: Worin unterscheiden sich agentische Systeme von bisherigen KI-Ansätzen? Wie verändert sich die Mensch-Maschine-Kommunikation vom Klick zum Prompt? Welche Schnittstellen erleichtern die Integration in bestehende Fachverfahren? Welche hybride Architektur aus Sprachmodellen, Regellogik, Trust-Mechanismen und Governance ist erforderlich? Und welche Infrastruktur bildet dafür das Fundament?

Diese Bausteine greifen ineinander: Ohne digitale Identität können Agenten nicht im Namen von Bürgern handeln. Ohne Register fehlen verlässliche Datenquellen. Ohne Standards bleibt Integration proprietär und teuer. Diese zentralen Wegbereiter sollten Verwaltungen verstehen und gezielt gestalten.

VON SCHWACHER ZU STARKER KI: EINORDNUNG AGENTISCHER SYSTEME

Die KI-Forschung unterscheidet zwischen schwacher KI (Narrow AI), die spezifische Aufgaben löst, und starker KI (Artificial General Intelligence), die menschenähnliche kognitive Fähigkeiten besitzt.

Agentische KI bewegt sich in einer Zwischenzone: Sie besitzt nicht die universelle Problemlösungsfähigkeit starker KI, geht aber durch ihr proaktives, zielorientiertes Handeln weit über schwache KI hinaus.

Der Übergang von assistierender zu agentischer KI ist aktuell die zentrale technologische Entwicklung. Der fundamentale Unterschied zeigt sich im Handlungsmodus: Assistierende Chatbots reagieren auf direkte Eingaben mit Textbausteinen. KI-Agenten verfolgen hingegen definierte Ziele, planen Schrit-

te, nutzen Tools wie Kalender und Register und passen Strategien dynamisch an. Diese Fähigkeiten entstehen durch die Kombination aus Large Language Models (LLMs) für Sprachverständnis, Reasoning-Fähigkeiten für mehrstufige Planung und standardisierten Schnittstellen für systemseitige Aktionen.

VOM KLIKK ZUM PROMPT: PARADIGMENWECHSEL BEIM NUTZERERLEBNIS

Die erweiterten Fähigkeiten agentischer Systeme erfordern einen grundlegenden Wandel in der Art und Weise, wie Bürgerinnen und Bürger mit öffentlicher Verwaltung interagieren. Wir erleben einen Paradigmenwechsel von grafischen Oberflächen wie Buttons und Menüs hin zu Sprach-Interfaces. Die kognitive Last sinkt drastisch: Bürgerinnen und Bürger formulieren Anliegen frei, ohne Portalstrukturen verstehen zu müssen. Sprachbasierte Zugänge demokratisieren den Zugang und senken Barrieren, insbesondere für Menschen mit geringer digitaler Kompetenz.

MODEL CONTEXT PROTOCOL (MCP): STANDARDISIERTE SCHNITTSTELLEN FÜR AGENTEN

Damit Agenten ihre Fähigkeiten in komplexen Verwaltungsstrukturen voll entfalten können, bedarf es jedoch mehr als nur besserer Interfaces. Es braucht technische Interoperabilität. Das Model Context Protocol fungiert als Standardisierungsschicht, vergleichbar mit dem USB-C-Standard in der Hardware-Welt. Statt für jede AI-Tool-Kombination eigene Integrationen zu bauen, implementieren Systeme einen MCP-Server, der ihre Fähigkeiten in standardisierter Form exponiert.

Funktionsweise und Nutzen

MCP ist der Schlüssel zur Interoperabilität: Ein Wohngeld-Fachverfahren, das auf einem MCP-Server betrieben werden würde, könnte von verschiedenen KI-Agenten genutzt werden – egal ob Bür-

ger-Agent, Government-Agent oder Analyse-Tool. Die Client-Server-Architektur ermöglicht es, dass Agenten Funktionen automatisch entdecken. Sessions sind langlebig und zustandsbehaftet – ideal für mehrstufige Workflows. Die Wertschöpfung verlagert sich damit von der Infrastruktur-Integration zur intelligenten Orchestrierung.

Sicherheit und Identitätsmanagement

Die Herausforderung liegt im Multi-Party-Ansatz: Eine KI-Agentin handelt im Auftrag eines Menschen, greift aber auf Systeme zu, die ihre eigenen Berechtigungsmodelle haben. Das MCP muss daher die ursprüngliche Nutzeridentität über die gesamte Aufrufkette hinweg übermitteln und sicherstellen, dass die Agentin nur auf Ressourcen zugreifen kann, für die der Nutzer autorisiert ist.

Zudem braucht es die explizite Zustimmung: Bevor ein Agent im Namen einer Bürgerin einen Termin bucht oder einen Antrag stellt, muss dies transparent kommuniziert und autorisiert werden.

DIE AGENTISCHE ARCHITEKTUR: KEIN REINES LLM-SYSTEM

Agentische Systeme in der Verwaltung lassen sich nicht auf Large Language Models reduzieren. Nach aktuellem Stand der Diskussion entstehen tragfähige Lösungen vielmehr aus einer Hybridarchitektur, in der unterschiedliche Komponenten zusammenspielen. Erfolgreiche Ansätze kombinieren insbesondere fünf Ebenen:

1. **LLM-Ebene:** natürlichsprachliche Verarbeitung und mehrstufiges Schlussfolgern
2. **regelbasierte Logik:** fachliche Berechnungen (z. B. Wohngeldformel nach § 19 WoGG), Plausibilitätsprüfungen und Fristenlogik
3. **Integration der Fachverfahren:** Anbindung bestehender Systeme, etwa über standardisierte Schnittstellen wie MCP – Fachver-

fahren bleiben führende Systeme und Single Source of Truth

4. **Trust Layer:** technische Leitplanken wie Guardrails, Input und Output Validierung, Boundary Enforcement sowie Audit Trails
5. **Governance Ebene:** klar definierte Human in the Loop Punkte, Qualitätskorridore, Eskalationsregeln und Stichprobenkontrollen

Dieser Architekturansatz ist deshalb relevant, weil die einzelnen Komponenten unterschiedliche Aufgaben erfüllen: LLMs ermöglichen eine flexible Sprachverarbeitung, sind jedoch nicht deterministisch. Die regelbasierte Logik stellt Präzision und Rechtskonformität sicher. Fachverfahren bleiben die autoritativen Datenquellen. Trust Mechanismen begrenzen Fehlverhalten und Fehlinterpretationen. Governance schafft Verantwortlichkeit und rechtssichere Nachvollziehbarkeit.

Agentische KI ist in diesem Verständnis keine Ablösung bestehender Systeme durch LLMs, sondern eine Orchestrierung vorhandener Bausteine. Der Agent fungiert als steuernde Schicht, die zwischen Bürgern, Regelwerk und Fachverfahren vermittelt. Diese Voraussetzungen sollten in die nationale Infrastrukturstrategie eingebettet werden: in den **Deutschland-Stack** - eine souveräne Technologie-Plattform für Digitalvorhaben in Deutschland. Der Deutschland-Stack definiert in seiner aktuellen Version sieben prioritäre Technologiefelder: agentische und generative KI, digitale Identitäten, souveräne Cloud, Verschlüsselung und Kryptographie, sicheres Arbeiten und Kommunizieren, Infrastruktur und Netze sowie IT-Sicherheit.

Dass **agentische und generative KI** dabei besonders hervorgehoben wird, unterstreicht ihre Rolle bei der Automatisierung komplexer Arbeitsabläufe. Zugleich gewinnen auch standardisierte Schnittstellen – etwa das beschriebene Model Con-

text Protocol (MCP) – an Bedeutung, weil sie Interoperabilität ermöglichen.

DIGITALE IDENTITÄT, REGISTER UND CLOUD-INFRASTRUKTUR

Die BundID ist das zentrale Identifikations- und Authentifikationsmittel für digitale Verwaltungsleistungen in Deutschland. Sie folgt den Vorgaben der eIDAS-Verordnung und bietet unterschiedliche Sicherheitsniveaus. Für agentische Systeme ist sie zentral, da sie sichere Authentifikation, strukturierte Datenbereitstellung, elektronische Signaturen sowie bidirektionale Kommunikation und Statusverfolgung ermöglicht.

Ab Ende 2026 ergänzt die European Digital Identity Wallet (EUDI-Wallet) diese Infrastruktur auf europäischer Ebene. Sie ermöglicht die EU-weite Authentifizierung, die sichere Speicherung von Nachweisen und eine datensouveräne Nutzung nach dem Prinzip Privacy by Design. Die BundID fungiert dabei als Schnittstelle: Alle angeschlossenen Verwaltungsdienste werden EUDI-Wallet-kompatibel.

Für agentische Systeme eröffnet diese Integration einen erweiterten Datenraum, grenzüberschreitende Nutzbarkeit und ein explizites Consent-Management. Verwaltungen, die heute auf offene Standards (OIDC, eIDAS) setzen, sind vorbereitet; proprietäre Identitätslösungen erfordern aufwendige Nachrüstungen.

Interoperables Register als Datendrehscheibe

Neben einer sicheren Identifikation benötigen agentische Systeme Zugriff auf authentische Datenquellen. Das Once-only-Prinzip - Daten nur einmal erheben und dann verwaltungsweit nutzen – erfordert interoperable Register für Personen-, Unternehmens- und Geodaten. Deutschland hat

mit dem Registermodernisierungsgesetz wichtige Grundlagen geschaffen. Eine Transformation in Richtung einer agentischen Bürgerinteraktion erfordert eine Analyse der NOOTS-Architektur mit Blick auf die Nutzung von KI-Agenten.

Souveräne Cloud-Infrastruktur als Skalierungsplattform

Die Bereitstellung von KI-Agenten erfordert skalierbare Rechenkapazität, insbesondere GPU-Ressourcen für Large Language Models. Viele Verwaltungen verfolgen Cloud-first-Strategien - nicht aus Überzeugung, sondern aus einer Notwendigkeit heraus. Die lokale Infrastruktur erfüllt die Anforderungen nicht.

Für sensible Verwaltungsprozesse sind jedoch souveräne Cloud-Lösungen oder ein On-Premises-Betrieb erforderlich. Initiativen wie GAIA-X und hoheitliche Cloud-Angebote zielen darauf ab, europäische Alternativen zu US-amerikanischen Hyper-scalern zu etablieren, um digital souverän agieren zu können.

PROZESS-REDESIGN: VON DER VOLLBEARBEITUNG ZUR AUSNAHMENSTEUERUNG

Agentische KI erfordert ein Umdenken in den Verwaltungsprozessen: von der klassischen Vollbearbeitung hin zum intelligenten Eingreifen bei Ausnahmen. KI-Agenten übernehmen klar definierte, regelbasierte Schritte. Dazu zählen unter anderem Registerabfragen, Vollständigkeitsprüfungen und Fristenberechnung. Verwaltungsfachkräfte greifen nur in Ermessensfällen, bei Härtefallprüfungen oder Widersprüchen ein. Dieser Paradigmenwechsel erfordert ein Prozess-Redesign in vier Schritten:

1. Prozessanalyse zur Identifikation regelbasierter Schritte versus ermessensbasierte Schritte
2. Nutzung des Automatisierungspotenzials, da zahlreiche Verwaltungsprozesse regelbasiert und damit automatisierbar sind

3. Definition klarer Trigger für Eskalationslogik, wann der Agent an Menschen übergibt
4. Stichproben zur Überprüfung automatisierter Entscheidungen als Qualitätssicherung

Trust Layer und Leitplanken

Ein neues Prozessmodell funktioniert nur mit robusten Sicherheitsmechanismen. KI-Agenten benötigen technische Sicherheitsmaßnahmen, die verhindern, dass sie aus der Spur laufen:

- Input-Validierung erkennt und wehrt Prompt-Injection-Angriffe ab
- Output-Filter verhindern toxische, diskriminierende oder rechtlich problematische Ausgaben
- Boundary Enforcement stellt sicher, dass Agenten nur auf freigegebene Tools und Datenquellen zugreifen
- Rate Limiting schützt vor übermäßiger Ressourcennutzung oder DoS-ähnlichem Verhalten
- Continuous Monitoring überwacht Agent-Aktivitäten in Echtzeit mit automatischen Alerts bei Anomalien

Diese Leitplanken sind nicht optional, sondern die technische Umsetzung der Prinzipien eines verantwortungsvollen KI-Einsatzes.

Wann Human-in-the-Loop Pflicht ist

Trotz aller Automatisierung gibt es klare Grenzen der Autonomie. Die dritte Stufe der Agent-zu-Agent-Verhandlung wirft fundamentale Fragen zur Balance zwischen Effizienz und Autonomie auf. Fünf Bereiche erfordern zwingend menschliche Intervention:

1. Negative Bescheide müssen von einem Menschen geprüft und verantwortet werden. Der Government-Agent kann begründete Ablehnungsempfehlungen vorbereiten, aber nicht autonom umsetzen.
2. Bei Sanktionen und Rückforderungen (z. B. wegen falscher Angaben) ist die Prüfung durch einen Menschen zwingend erforderlich.

3. Bei Ermessensentscheidungen, wenn das Gesetz der Behörde Spielraum lässt („kann“, „soll“), entscheidet ein Mensch – etwa bei Härtefallregelungen.
4. Bei Widersprüchen übernimmt ein Mensch die komplette Fallbearbeitung.
5. Mindestens zehn Prozent aller automatisiert genehmigten Bescheide werden nachträglich von Menschen geprüft, vergleichbar mit der Qualitätssicherung in der Industrie.

JOBPROFILE FÜR DAS AGENTISCHE ZEITALTER

Agent Orchestrators konfigurieren, überwachen und optimieren KI-Agenten und definieren Eskalationsregeln sowie Qualitätskorridore.

Prompt Engineers entwickeln und testen Prompts für verschiedene Verwaltungsszenarien und optimieren die Antwortqualität.

AI Governance Managers stellen Compliance mit regulatorischen Anforderungen sicher und koordinieren Risikobeurteilungen.

Data Stewards verantworten Datenqualität in Registern und definieren Metadaten sowie Zugriffsrechte.

Citizen Experience Designers gestalten agentische Interaktionen aus Nutzerperspektive und führen Usability-Tests durch.

Exception Handlers sind hochqualifizierte Sachbearbeitende für komplexe Fälle, die Agenten eskalieren.

Die beschriebenen Bereiche sind die Basics, die den Einsatz von KI-Agenten ermöglichen. Entscheidend für den Einsatz ist jedoch die Gestaltung der Governance und damit das Schaffen von Vertrauen in die Art der Interaktion.

RESPONSIBLE AI UND GOVERNANCE ALS VERTRAUENSSTIFTER

Der verantwortungsvolle Einsatz agentischer KI-Systeme in der Verwaltung erfordert ein klares Regelwerk (Governance), das Vertrauen, Sicherheit, Ethik und Transparenz als gleichwertige Ziele verankert. Nur wenn diese Dimensionen systematisch berücksichtigt werden, werden agentische Systeme in der Breite akzeptiert.

TRANSPARENZ UND ERKLÄRBARKEIT

Die Grundlage jedes vertrauenswürdigen Systems ist Transparenz. KI-gestützte Verwaltungsentscheidungen müssen nachvollziehbar sein. Das ist nicht nur eine ethische Anforderung, sondern eine rechtliche gemäß EU AI Act.

Agenten müssen Gründe für Entscheidungen, insbesondere bei Ablehnungen, verständlich darlegen und konkrete Handlungsoptionen aufzeigen. Mit der lückenlosen Aufzeichnung aller Aktionen durch Audit Trails erfüllen Verwaltungen ihre Rechenschaftspflicht und ermöglichen Ex-post-Prüfungen bei strittigen Fällen.

ETHIK UND BIAS-VERMEIDUNG

Über Transparenz hinaus müssen die Systeme selbst entlang ethischer Grundsätze agieren. KI-Systeme dürfen nicht bestehende gesellschaftliche Vorurteile verstärken, weil sie beispielsweise auf verzerrten Trainingsdaten basieren.

Verwaltungen sind dem Gleichheitsgrundsatz verpflichtet und müssen somit Schutzvorkehrungen treffen. Diese umfassen die sorgfältige Auswahl und Prüfung von Trainingsdaten, regelmäßige Bias-Audits der Systemausgaben, diverse Teams in Entwicklung und Evaluation sowie kontinuierliches Monitoring im Produktivbetrieb.

Menschliche Aufsicht bei Hochrisikoentscheidungen

Selbst bei technisch einwandfreien Systemen bleibt menschliche Aufsicht unverzichtbar. Das Human-in-the-Loop-Prinzip stellt sicher, dass kritische Entscheidungen menschlicher Prüfung unterliegen, insbesondere solche mit negativen Folgen für Bürgerinnen und Bürger.

KI bereitet vor, Menschen entscheiden. Dieses Prinzip wahrt rechtsstaatliche Standards und schafft eine klare Verantwortlichkeit.

SICHERHEIT DURCH PRIVACY BY DESIGN

Datenschutz von Anfang an

Ethische Algorithmen benötigen sichere Rahmenbedingungen. Privacy by Design bedeutet, Datenschutz als integralen Bestandteil der Systemarchitektur zu behandeln, nicht als nachträgliche Ergänzung.

Für agentische Systeme umfasst dies Datensparsamkeit durch die Erhebung ausschließlich notwendiger Daten, eine End-to-End-Verschlüsselung für sensible Kommunikation, wenn möglich eine Pseudonymisierung statt der Verwendung realer personenbezogener Daten sowie klare Regelungen für Aufbewahrungsfristen und Datenlöschung.

Hoheitliche Cloud-Lösungen

Die technische Umsetzung dieser Datenschutzprinzipien erfordert eine passende Infrastruktur. Für sensible Verwaltungsprozesse sind IT-Systeme und Geräte vorzuziehen, die unter nationaler oder europäischer Kontrolle stehen.

Verwaltungen reduzieren damit Abhängigkeiten von außereuropäischen Anbietern und minimieren Risiken durch Datenzugriffe ausländischer Behör-

den gemäß extraterritorialen Gesetzen wie dem US CLOUD Act.

Datensouveränität: Kontrolle in Bürgerhand

Der konsequenteste Datenschutz ist jener, der den Bürgerinnen und Bürgern das Steuer und die Kontrolle überlässt. Die BundID und künftige digitale Wallets verankern das Prinzip der Datensouveränität. Jede oder jeder entscheidet selbst, welche persönlichen Daten sie oder er für welchen Zweck freigibt. KI-Agenten, die in ihrem Auftrag handeln, müssen die explizite Zustimmung für jeden Datenzugriff einholen.

Diese Architektur kehrt das traditionelle Machtverhältnis um: Nicht die Verwaltung kontrolliert Bürgerdaten, sondern Bürgerinnen und Bürger gewähren der Verwaltung temporären Zugriff für spezifische Zwecke.

CO-KREATION: BÜRGERINNEN UND BÜRGER ALS MITGESTALTER

Datensouveränität ist ein wichtiger Schritt, doch ein noch tieferes Vertrauen entsteht durch aktive Beteiligung. Die Akzeptanz agentischer Systeme steigt erheblich, wenn Bürgerinnen und Bürger in

die Konzeption von Verwaltungsleistungen eingebunden werden.

Das Amarillo-Beispiel aus den USA zeigt, wie Co-Creation funktioniert: Die texanische Stadt entwickelt den KI-Assistenten Emma gemeinsam mit Einwohnern, beobachtet täglich gestellte Fragen und passt das System kontinuierlich an echte Bedürfnisse an.

Feedback-Schleifen und kontinuierliche Verbesserung

Ein solcher partizipativer Ansatz muss sich über den gesamten IT-Lebenszyklus erstrecken. KI-Agenten sollten nicht als abgeschlossene Produkte verstanden werden, sondern als lernende Systeme, die durch Nutzerfeedback besser werden.

Transparente Rückmeldeformate wie Bewertungen von Interaktionen oder Verbesserungsvorschläge stärken das Vertrauen und fördern die Weiterentwicklung. So entsteht ein kontinuierlicher Dialog zwischen der Verwaltung und ihren „Kunden“, der die Interaktion nicht nur technisch verbessert, sondern auch die gesellschaftliche Legitimation von KI in der Verwaltung stärkt.



AGENTISCHE KI UMSETZEN

Für den Einstieg in agentische KI sprechen drei Argumente. Sie rechtfertigen ein zügiges, zugleich aber bewusst strategisches Vorgehen.

- 1. Die technologische Reife ist erreicht.** Die grundlegenden Technologien – Sprachmodelle, Tool-Integration über standardisierte Schnittstellen und persistente Kontexte – sind verfügbar und erprobt. Verwaltungen, die jetzt starten, bauen Erfahrung und organisatorische Kompetenz auf, während andere noch beobachten.
- 2. Die Erwartungen der Bürger steigen schneller, als die Verwaltung nachziehen kann.** Digitale Angebote werden zunehmend an Maßstäben gemessen, die aus anderen Lebensbereichen bekannt sind: Verfügbarkeit, Verständlichkeit und Transparenz. Bleiben diese Erwartungen unerfüllt, leidet nicht nur die Nutzung, sondern auch Vertrauen und Legitimität staatlichen Handelns.

- 3. Der Fachkräftemangel macht Automatisierung unverzichtbar.** Steigende Aufgabenkomplexität trifft auf sinkende Personalressourcen. Ohne gezielte Automatisierung geraten Verwaltungen strukturell unter Druck. Agentische Systeme eröffnen hier neue Spielräume, indem sie regelbasierte Aufgaben zuverlässig übernehmen.

Diese Argumente sprechen für entschlossenes Handeln, jedoch nicht für hektische Schnellschüsse. Erfolgreich ist ein Einstieg dann, wenn er mit Stufe 1 beginnt und von Anfang an die richtigen architektonischen Weichen für die Stufen 2 und 3 stellt. Übereilte Pilotprojekte mit instabilen Lösungen erzeugen Frustration und sind langfristig schädlicher als ein späterer, dafür tragfähiger Einstieg.



KRITISCHE ARCHITEKTURENTSCHEIDUNGEN: HEUTE DIE WEICHEN STELLEN

Ein häufiger strategischer Fehler besteht darin, Stufe 1 als isoliertes Pilotprojekt zu behandeln. In diesen Fällen wird oft die schnellste und einfachste Lösung gewählt, und das ist nicht selten die Wahl eines proprietären Cloud-Anbieters mit hohem Vendor-Lock-in-Effekt. Die Folgen zeigen sich spätestens beim Übergang zu Stufe 2:

- Das eingesetzte Modell ist nicht mehr verfügbar oder wirtschaftlich tragfähig
- Die Anbindung von Fachverfahren erfordert proprietäre Zusatzmodule
- Zentrale Komponenten wie die BundID lassen sich nicht integrieren
- Governance-Anforderungen müssen nachträglich und aufwendig ergänzt werden
- Ein Strategiewechsel, etwa hin zu Open Source, bedeutet faktisch einen Neubau

Die Kosten solcher Fehlentscheidungen sind hoch - finanziell und zeitlich.

FÜNF ARCHITEKTURPRINZIPIEN FÜR EINEN TRAGFÄHIGEN EINSTIEG

Ein nachhaltiger Aufbau agentischer Systeme folgt daher fünf Grundprinzipien:

1. Modularität

Alle Komponenten müssen austauschbar sein. Offene Schnittstellen und klar getrennte Layer verhindern Abhängigkeiten.

2. offene Standards

Standardisierte Protokolle wie MCP sind proprietären APIs vorzuziehen. Die Architektur sollte von Beginn an Open-Source-fähig sein.

3. Trennung von Fachlogik und KI-Modellen

Verwaltungswissen und Sprachmodelle sind getrennte Ebenen. Fachlogik bleibt deterministisch und überprüfbar.



4. Governance Readiness

Audit Trails, Monitoring und Eskalationsmechanismen sind Pflichtbestandteile – nicht optionale Ergänzungen.

5. Skalierbarkeit

Die Architektur muss Wachstum ermöglichen – ohne grundlegendes Redesign.

Diese Prinzipien erfordern zu Beginn mehr Disziplin, reduzieren jedoch auf späteren Stufen den Zeit- und Budgetaufwand erheblich.

REIFEGRAD-EINORDNUNG: WANN IST WELCHES MODELL REALISTISCH?

Die Umsetzbarkeit agentischer Modelle hängt weniger von Zeitplänen ab als von organisatorischen und technischen Voraussetzungen. Die folgende Einordnung unterstützt eine realistische Bewertung:



STUFE	VORAUSSETZUNGEN FÜR ERFOLGREICHE UMSETZUNG	TYPISCHE STOLPERSTEINE	EINSTIEGSSCHWELLE
STUFE 1: 24/7-ASSISTENZ	TECHNISCH: • LLM-Zugang (Cloud oder On-Premises) • strukturierte Wissensdatenbank • Basis-Guardrails (Input-/Output-Validierung) ORGANISATORISCH: • Orchestrator, Prompt Engineer, Designer notwendig • Commitment der Fachbereiche für Wissenskuration • Pilotnutzer-Gruppe (100+ Personen)	• Unzureichende oder veraltete Wissensbasis • Fehlende Prompt-Engineering-Kompetenz • Unterschätzung des kontinuierlichen Pflegeaufwands • Unrealistische Erwartungen an Antwortqualität	Niedrig Grundlegende IT-Kompetenz und Bereitschaft zum Experimentieren genügen. Technologie ist verfügbar, Risiko überschaubar.
STUFE 2: SOVERÄNE INTERAKTION	TECHNISCH: • BundID-Integration mit eSignatur-Fähigkeit (ab 2027 EUDI-Wallet-Kompatibilität) • Dokumentenextraktion (OCR/Computer Vision) • MCP-Server für relevante Fachverfahren • Registerqualität (Konsistenz, Aktualität, Vollständigkeit) ORGANISATORISCH: • Prozess-Redesign: Trennung von regelbasiert und ermessensbasiert • Change Management für Sachbearbeitende • Data Steward für Registerqualität	• Mangelhafte Datenqualität in Registern • Fehlende MCP-Adapter für Legacy-Fachverfahren • Widerstand bei Sachbearbeitenden („Jobverlust-Angst“) • Unterschätzung des Prozess-Redesign-Aufwands • Rechtliche Unsicherheiten bei elektronischer Signatur	Mittel Erfordert ausgereifte digitale Basisinfrastruktur (BundID, Register) und organisatorische Veränderungsbereitschaft. Vorarbeit aus Stufe 1 essenziell.
STUFE 3: AUTONOME VERHANDLUNG	TECHNISCH: • föderierte Registeranbindung (Once-only-Prinzip) • Agent-zu-Agent-Protokolle (standardisiert) • proaktives Monitoring von Datenänderungen • hochentwickelter Trust Layer mit Audit Trails ORGANISATORISCH: • umfassende Governance (10 %+ Stichproben, klare Human-in-the-Loop-Punkte) • Kulturwandel: Ausnahme-steuerung statt Vollbearbeitung • Rechtsgutachten zur Verantwortlichkeit	• Föderale Fragmentierung (16 Länder, unterschiedliche Systeme) • Rechtliche Unsicherheiten bei autonomen Entscheidungen • Mangelnde Akzeptanz bei Sachbearbeitenden und Bürgern • Komplexität der behördenübergreifenden Orchestrierung • Fehlende Standards für Agent-zu-Agent-Kommunikation	Hoch Setzt vollständige Umsetzung von Stufe 2 voraus plus zusätzlicher rechtlicher, ethischer und technischer Klärungen. Pilotierung in kontrollierten Umgebungen empfohlen.

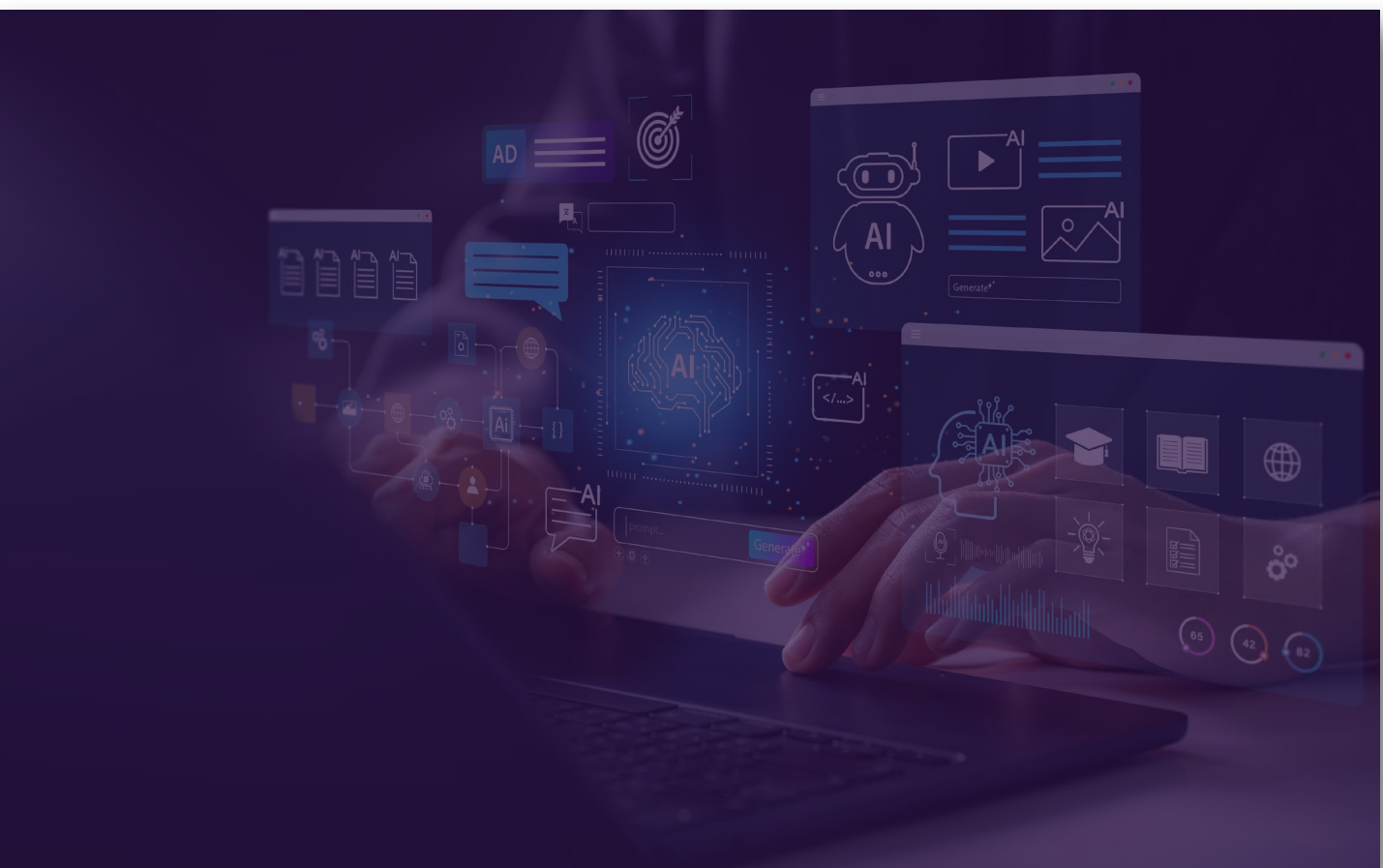
Die beschriebenen technischen und organisatorischen Voraussetzungen im Blick, braucht eine Realisierung von KI-Agenten ein klares Vorgehensmuster. Folgende drei wesentliche Elemente sind Voraussetzung für eine erfolgreiche Umsetzung:

Schrittweises Vorgehen: Stufe 1 dient als Einstieg und Lernphase. Darauf aufbauend werden systematisch die Voraussetzungen für Stufe 2 geschaffen. Stufe 3 ist eine langfristige Perspektive, kein kurzfristiges Ziel.

Parallelität zulassen: Stufe 1 kann produktiv betrieben werden, während parallel an Registern, Identitätsintegration und Prozessen für Stufe 2 gearbeitet wird. Die Stufen bauen aufeinander auf, schließen sich aber nicht aus.

Leapfrogging richtig verstehen: Veraltete Portale können übersprungen und sprachbasierte Zugänge direkt eingeführt werden. Organisatorische Lernprozesse lassen sich jedoch nicht abkürzen. Ein direkter Sprung zu Stufe 3 ohne Erfahrungen aus Stufe 1 und 2 ist nicht realistisch.

Agentische KI ist somit kein Technologieprojekt, sondern ein Transformationsvorhaben. Wer frühzeitig strukturiert einsteigt, verschafft sich Handlungsspielräume – nicht durch Tempo, sondern durch Weitsicht.



FAZIT

Agentische KI bietet der öffentlichen Verwaltung neue Möglichkeiten, Leistungen effizienter, zugänglicher und bürgernäher zu erbringen. Sie ermöglicht einen Übergang von reaktiver Kommunikation und Bearbeitung hin zu proaktiver Unterstützung, reduziert bürokratische Reibungsverluste und senkt die „Time Tax“ für Bürgerinnen und Bürger. Sprachbarrieren, begrenzte digitale Kompetenzen oder fehlende zeitliche Verfügbarkeit verlieren damit an Bedeutung - staatliche Leistungen werden breiter zugänglich.

Diese Entwicklung ist jedoch kein reines Technologieprojekt. Sie erfordert eine leistungsfähige, souveräne und interoperable IT-Architektur, verlässliche Datenquellen sowie klare Governance-Strukturen. Ebenso entscheidend ist der organisatorische Wandel: neue Kompetenzprofile, veränderte Rollenbilder und ein anderes Zusammenspiel von Mensch, Prozess und Technologie.

Der Einstieg muss dabei nicht revolutionär erfolgen. Verwaltungen sind nicht gezwungen, jede Stufe der bisherigen Digitalisierung vollständig zu durchlaufen. Ein stufenweiser Ansatz ermöglicht es, früh Nutzen zu stiften, Erfahrungen aufzubauen und gleichzeitig die Voraussetzungen für weitergehende Modelle zu schaffen. Die drei beschriebenen Entwicklungsstufen zeigen einen realistischen Pfad

- von assistierender Unterstützung über befähigende Bürger-Agenten bis hin zu weitgehend automatisierten Agent-zu-Agent-Prozessen.

Die technologischen Grundlagen für diesen Weg sind bereits vorhanden. Entscheidend ist nicht die Wahl einzelner KI-Modelle, sondern deren rechtskonforme, transparente und fachlich fundierte Einbettung in bestehende Strukturen. Unterschiede zwischen Consumer- und Government-Agenten entstehen vor allem durch Governance, Vertrauensmechanismen, Domänenwissen und den Zugriff auf föderale Register. Diese gilt es, nunmehr aktiv zu gestalten.

Vor diesem Hintergrund sollte agentische KI in aktuellen strategischen Debatten zur künftigen IT-Architektur des Staates von Beginn an mitgedacht werden. Der Deutschland-Stack bietet dafür den strategischen Rahmen, in dem zentrale Bausteine wie Identität, souveräne Cloud, Standards und Sicherheit zusammengeführt und für die Umsetzung nutzbar gemacht werden. Der aktuelle Stand zeigt, dass grundlegende Bausteine mit Blick auf eine agentische Bürgerinteraktion bereits mitgedacht werden. Das ist wichtig und richtig. Die Frage ist nicht, ob agentische Systeme Teil der Verwaltungsrealität werden, sondern wie vorausschauend und strukturiert dieser Wandel gestaltet wird.

ANSPRECHPARTNER



DR. BERND PEPER

Leiter Sopra Steria Next

E. bernd.peper@soprasteria.com

T. +49 151 40625244



MAXIMILIAN FINGER

KI-Berater Sopra Steria Next

E. maximilian.finger@soprasteria.com

T. +49 151 40625570



Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg

T. 040 22703-0
E. info.de@soprasteria.com
W. www.soprasteria.com