Deine eigenen KI-Helfer: Wie du datensicher Assistenten baust

Themen:

1. Vorwort
2. Funktionsweisen
3. Promptbibliothek
4. Assistenten
5. Formulare
6. Compliance-Kompass

Vorwort

Stell dir vor: Du hast einen digitalen Assistenten, der dir und deinem Team rund um die Uhr bei allen Aufgaben hilft –ganz ohne Datenschutzsorgen. Aufgaben werden automatisch erledigt, Informationen blitzschnell gefunden und alles läuft nach den aktuellen Datenschutzregeln. So wird euer Arbeitsalltag einfacher, sicherer und ihr habt mehr Zeit für die wirklich wichtigen Projekte.

In der digitalen Wirtschaft ist der Einsatz von Künstlicher Intelligenz zu einem entscheidenden Wettbewerbsfaktor geworden. Mit Inkrafttreten des EU AI Act stehen Unternehmen vor der Herausforderung, KI-Technologien nicht nur effektiv, sondern auch rechtskonform einzusetzen.

In diesem Video stellt dir meine Kollegin die Secure-Suite vor. Damit kannst du Kundendaten und interne Informationen datenschutzkonform nutzen. Du wirst ohne Vorkenntnisse und ganz einfach eigene Assistenten für wiederkehrende Aufgaben bauen. Und gleichzeitig auf die leistungsfähigsten KI-Modelle zugreifen – alles strukturiert und leicht bedienbar.

Lass mich dir nun einen kurzen Einblick in die Funktionsweise geben.

Funktionsweisen

Wir starten links oben und klicken auf den Pfeil, wodurch wir zu den Account-Einstellungen gelangen. Unter ‚Profil' kannst du deinen Namen sowie deine E-Mail-Adresse und dein Passwort bearbeiten.

Unter den Präferenzen kannst du dein Standardmodell auswählen. Genaueres zu diesen Modellen findest du im PDF im Anhang. Du kannst hier die Chatfunktionen vordefinieren sowie die Sprache auswählen.

Außerdem ist es möglich, zwischen hellem und dunklem Modus zu wechseln.

Die individuellen Anweisungen sind für dich sehr wichtig, da du hier der KI Informationen über dich geben kannst, was deine Ergebnisse maßgeblich verbessern wird. Zuerst entscheidest du, ob diese Informationen für jeden neuen Chat angewendet werden sollen oder nur, wenn du sie aktivierst.

Ich würde dir hierbei empfehlen, sie zu aktivieren. Du solltest hier relevante Infos zu deinem Hintergrund, deinen Zielen und deinem bevorzugten Kommunikationsstil eingeben. Zum Beispiel in meinem Fall:

Ich erstelle Online-Kurse zum Thema KI und interessiere mich für den AI Act. Ich schätze klare, praxisnahe Antworten und möchte, dass das Modell mir bei technischen Fragen, Kursinhalten und strategischen Entscheidungen hilft.'

Damit bekommt die KI einen guten Rahmen für präzisere und relevantere Antworten. Diese können aber auch noch ausführlicher ausfallen.

Gruppen könnten beispielsweise ein Team sein oder eine Arbeitsgruppe zu einem bestimmten Thema oder Fall.

Auf die Wissensordner komme ich später noch genauer zu sprechen. Du benötigst sie zum Beispiel für die Agenten, die ich dir gleich noch zeigen werde.

In den geteilten Chats kannst du von dir versendete beziehungsweise geteilte Chats einsehen und verwalten. Die Erinnerungen sind ähnlich zu den zuvor besprochenen individuellen Anweisungen und können dem Programm helfen, nach und nach über dich zu lernen.

Kommen wir zu den weiteren Funktionen. Mithilfe dieses Symbols kannst du die Seitenleiste ausblenden, und durch die Lupe deine Chats durchsuchen. Die Lupe ist aber auch ein Weg, alle Funktionen zu öffnen, umso schneller zu navigieren. Wenn du nämlich daraufklickst, öffnet sich ein Fenster, in dem du beinahe alle Punkte und Einstellungsmöglichkeiten, die wir bisher besprochen haben, finden kannst.

Das Besondere an der KIRA Secure Suite ist, dass du nicht nur Zugriff auf ein Modell hast, sondern eine Vielzahl an unterschiedlichen Sprachmodellen nutzen kannst, um für jeden Use Case das beste Modell und den besten Anbieter auszuwählen – und das noch dazu DSGVO-konform.

Neben dem jeweiligen Modell erhältst du eine kurze Erklärung, und ausführlichere Informationen findest du in den Dokumenten im Anhang.

Das ist aber noch nicht alles. Wie du es vielleicht von ChatGPT oder anderen Anbietern kennst, kannst du durch die Klammer Dateien hochladen. Das ist sogar mit Videos und Audiodateien bis zweihundert Megabyte möglich.

Anhand des Kugel-Symbols stellst du die Internetsuche ein oder aus. Diese kann nützlich sein, wenn du aktuelle Daten und Quellen benötigst.

Eine besonders hilfreiche Funktion beim Verfassen von Berichten stellt das Canvas-Modell dar. Am Beispiel eines Auftrags, aktiviere ich in der unteren Prompt-Leiste das Canvas-Modell. Dadurch erscheint ein Fenster, das es mir äußerst unkompliziert ermöglicht, meine Texte genau auf die jeweilige Zielgruppe oder Zielperson zuzuschneiden.

Rechts unten sind drei Symbole sichtbar: Die ersten beiden dienen dazu, die Textlänge individuell einzustellen. In unserem Beispiel möchte ich den Bericht etwas kürzer gestalten. Mit der dritten Funktion lässt sich die Sprachvereinfachung mit nur einem Klick anpassen, wodurch der Text den letzten Feinschliff erhält – diese Funktion überarbeitet zudem Rechtschreibung, Stil und Struktur. Wenn du mit dem Ergebnis zufrieden bist, kannst du es oben rechts als PDF- oder Word-Datei exportieren. Möchtest du hingegen

noch weitere Aspekte ergänzen, nutzt du das Prompt-Fenster unten links und führst den Dialog fort.

Unter Integrationen kannst du deine Microsoft oder Google-Umgebung oder auch andere Plattformen mit der Secure Suite verbinden. Du kannst hier aber auch die interne Wissensdatenbank mit Daten füttern. Dazu klickst du auf Wissensordner hinzufügen gibst ihm einen Namen und eine kurze Beschreibung und kannst anschließend deine Dateien hochladen.

Unter den Wissensordnern findest du außerdem, wie zuvor schon angesprochen, eine Vielzahl an weiteren Plattformen, die du mit der Secure Suite verknüpfen kannst.

Du kannst anschließend im Chat Fenster mit deinen hochgeladenen Dateien arbeiten. Dazu klickst du auf die Büroklammer. Dadurch hast du Zugriff auf alle hochgeladenen Dateien und Dokumente und kannst mit ihnen arbeiten.

Promptbibliothek

Der nächste Punkt, den ich dir zeigen möchte, ist die Promptbibliothek. Hier kannst du entweder für dich selbst oder auch für deine Kollegen Prompts speichern, die entweder sehr gut gelungen sind oder häufig genutzt werden. Dadurch musst du sie nicht immer wieder neu verfassen, sondern hast sie immer sofort bei der Hand.

In meinem Fall wäre das die Rechtschreibprüfung. Ich gebe dem Prompt einen Namen und kopiere den Prompt ein. Außerdem kann ich, wie schon erwähnt, einstellen, wer Zugriff auf den Prompt haben soll. Ich muss nur noch auf ‚Speichern' klicken, und schon ist der Prompt in meiner Bibliothek im Ordner ‚Privat' hinterlegt.

Assistenten

Der Reiter ‚Assistenten' kann für dich und deine Produktivität sehr wichtig sein. Hier baust du dir eigene, kleine KI-Modelle, die nach bestimmten Abläufen funktionieren und dich so bei wiederkehrenden Tätigkeiten unterstützen können. Die fertigen Assistenten findest du anschließend übrigens hier.

Um zu starten, gebe ich meinem Assistenten den Namen, E-Mail-Assistent. Ich möchte nämlich, dass er mich beim schreiben von Emails unterstützt.

Anschließend haben wir zwei Möglichkeiten, den Assistenten aufzubauen: als Formular oder als Chatbot.

Da ich zum Beispiel bei Stellenausschreibungen fast immer nach demselben Muster arbeite, würde ich hierbei das Formular wählen, da ich mir einzelne Kategorien erstellen kann, die der Nutzer dann ausfüllt. Was ich damit genau meine, zeige ich dir im Anschluss. Da wir für die Emails aber flexibler sein möchten, bleiben wir beim Prompt.

In den Anweisungen kannst du dem Assistenten genau sagen, wie er sich verhalten soll, was also seine Aufgabe ist, in welchem Stil er schreiben soll und so weiter. sei hier ruhig ausführlicher als ich es war.

Als nächsten Schritt kannst du deinem Assistenten sein Wissen übermitteln. Dazu kannst du entweder schon von dir in die Wissensdatenbank hochgeladene Daten nutzen, oder neue Dokumente hochladen. Dadurch kann der Assistent über spezifisches Wissen verfügen und es in die Antworten einbauen.

Die Aktionen sind ein extrem mächtiges und praktisches Tool, das du unbedingt in deinen Arbeitsablauf integrieren solltest. Du kannst sie dir als eine Art mini Automatisierungen vorstellen. Als Beispiel werden wir nun, wie schon angekündigt mein office postfach verknüpfen.

Das geht ganz einfach und ist in wenigen Sekunden erledigt. es gibt aber noch viele weitere Anwendungen, die du unbedingt testen solltest. Wie du siehst, benötigt es nur wenige Klicks, und mein Email Postfach ist verknüpft. Nnun wähle ich noch akzeptieren und auf der nächsten Seite, Aktion hinzufügen aus, so dass wir den Assistenten gleich testen können.

Bevor wir den Assistenten aber testen, zeige ich dir noch, wie du hier ganz einfach unter den verschiedenen Modellen wählen kannst. Welches Modell wofür geeignet ist, haben wir schon besprochen. Außerdem ist es hier möglich, die Kreativität einzustellen. Für freiere Texte solltest du die Kreativität höher stellen, bei Themen wie Datenverarbeitung oder E-Mails, wo es auf Genauigkeit ankommt, eventuell etwas niedriger

Probieren wir das Ganze jetzt einmal aus.

Wir öffnen den Assistenten und geben ihm den Auftrag, Jakob eine E-Mail zu senden mit der Bitte, uns eine Übersicht der neuesten KI-Tools zukommen zu lassen.

Der Assistent beginnt sofort mit der Erstellung der Nachricht und liefert uns einen Entwurf, den wir selbstverständlich noch nach unseren Wünschen anpassen können. Anschließend haben wir die Möglichkeit, die E-Mail über unseren Outlook-Account zu öffnen, um gegebenenfalls Anhänge hinzuzufügen oder kleinere Änderungen vorzunehmen. In meinem Fall gebe ich der KI sogar direkt den Befehl, die Mail sofort zu verschicken. Da ich mehrere Accounts verknüpft habe, werde ich gefragt, mit welchem Konto ich die Nachricht versenden möchte. Nach meiner Bestätigung wird die E-Mail umgehend an Jakob gesendet. Wenn wir anschließend im Ordner „Gesendete Mails" nachsehen, finden wir dort die versendete Nachricht.

Natürlich kannst du auch abfragen, wann die letzte E-Mail von einem Kunden eingegangen ist oder Termine abrufen beziehungsweise direkt in den Kalender eintragen lassen. Wie du siehst, erleichtern und vereinfachen solche Integrationen erheblich die Art und Weise, wie man sich organisiert und effizient arbeitet.

Als nächstes möchte ich dir einen weiteren Assistenten vorstellen, der all unserer Meetings organisiert. Mithilfe einer konkreten Anweisung kann ich dadurch schnell auf die benötigten Informationen zugreifen. Dieser Assistent analysiert die vorherigen Besprechungen und erstellt eine Logik, um festzustellen, ob noch offene Aufgaben bestehen. Durch einen Klick auf die Quelle habe ich sogar die Möglichkeit, direkt in das transkribierte Dokument einzusehen und mir die detaillierte Aufnahme durchzulesen.

Alternativ kann ich auch den Prompt formulieren, dass die KI mir eine priorisierte Liste der ausstehenden Aufgaben erstellt. Wie du bereits erkennen kannst, wird hier übersichtlich nach Personen aufgeschlüsselt, bei wem Handlungsbedarf besteht und welcher Status jeweils vorliegt. Das Resultat, das du gleich vollständig sehen wirst, ist äußerst beeindruckend und ermöglicht nicht nur eine erhebliche Zeitersparnis, sondern sorgt zudem für eine klare und strukturierte Übersicht.

Formulare

Nun möchte ich dir zum Abschluss wie versprochen, noch die Formular Funktion erklären.

Um zu starten, gebe ich meinem Assistenten den Namen ‚Stellenausschreibung'. Ich möchte nämlich, dass er mich beim Erstellen von Stellenausschreibungen unterstützt.

Anschließend wählen wir diesmal Formular aus.

Um das Formular zu erstellen, füge ich nun Felder mit den wichtigsten Punkten ein, die in meiner Stellenausschreibung vorkommen sollen. Dabei habe ich die Möglichkeit, unterschiedliche Eingabetypen wie Text, Zahlen oder auch Datum zu wählen.

Das mache ich für alle benötigten Felder, was am Ende dann so aussieht.

Als Nächstes gebe ich dem Agenten Anweisungen – also was er machen soll und wie er sich verhalten soll. Ich blende dir meinen Prompt kurz ein, damit du ihn dir ansehen kannst.

Wir können den Agenten, wie zuvor erklärt, mit neuem Wissen füllen, es hochladen oder aus der Wissensdatenbank nutzen. Außerdem können wir erneut das Modell ändern und auch die Kreativität einstellen.

Testen können wir den Assistenten rechts oben unter ‚Assistent verwenden'.

Hier finde ich dann das zuvor erstellte Formular, in das ich nur noch die Grunddaten der Stellenausschreibung eingeben muss. Bin ich mit den Eingaben fertig, klicke ich auf Senden und die KI erstellt mir eine fertige Stellenausschreibung. Sie verpackt also alle

von mir in das Formular eingegebenen Daten in einen Text, ohne das ich mir über Formulierungen den Kopf zerbrechen muss, wenn ich das nicht möchte.

Das war nun ein kurzer Überblick über einige der Funktionen, die diese Plattform bietet. Wie du feststellen konntest, verändert und vereinfacht sich die Arbeitsweise erheblich, wenn man eine derart leistungsstarke Plattform nutzt. Möchtest du im beruflichen Umfeld mit KI arbeiten, ist es unerlässlich, wie bei der Secure-Suite, DSGVO-konform vorzugehen und gleichzeitig die Möglichkeit zu haben, schnell auf franchiseinternes Wissen zuzugreifen.

Nur so kann die KI dich wirklich verstehen und dich qualitativ hochwertig unterstützen. Du kannst diese Suite gerne selbst testen, indem du unsere Website besuchst. Und dich dort unter „Login" für die KIRA Secure-Suite anmeldest. Verwende dabei als Zugangsdaten die E-Mail-Adresse: office@kira.at sowie das Passwort: SecureSuite25 – Achte darauf, dass beide „S" großgeschrieben sind. Falls du Interesse an dieser Plattform hast, zögere nicht, uns zu kontaktieren.

Ich wünsche dir viele erfolgreiche Momente auf der Plattform.

Compliance Kompass

Für den richtigen KI-Einsatz brauchst du klare Grundprinzipien.

Transparenz bedeutet bei der KIRA SecureSuite: Du behältst jederzeit die Kontrolle über deine eigenen Daten. Du siehst genau, welche Inhalte du hochgeladen hast, wie sie verarbeitet werden und welche Ergebnisse daraus entstehen. Keine Blackbox – sondern maximale Nachvollziehbarkeit in deinem System.

Datenschutz steht bei uns an erster Stelle. Alle Daten werden DSGVO-konform in EU-Rechenzentren verarbeitet. Du entscheidest selbst, welche Informationen eingebunden werden – und kannst sicher sein, dass sie vertraulich und geschützt bleiben.

Sicherheit ist mehr als Technik – es ist ein Prinzip. Dank moderner Verschlüsselung, klarer Zugriffsbeschränkungen und regelmäßiger Sicherheitsupdates bist du mit der SecureSuite auf einem hohen Schutzniveau unterwegs – ganz gleich, ob Basis- oder Pro-Version.

Ethik gehört bei Künstlicher Intelligenz unbedingt dazu. Du trägst Verantwortung für den Einsatz der Technologie. Die SecureSuite unterstützt dich dabei, fair, respektvoll und diskriminierungsfrei zu arbeiten – und die Ergebnisse kritisch zu hinterfragen.

Pflicht meint: Du handelst rechtskonform. Mit der SecureSuite erfüllst du die Vorgaben des AI Act, beachtest Datenschutzregeln und interne Richtlinien – ohne dabei den Überblick zu verlieren. Die Plattform hilft dir, deinen gesetzlichen Verpflichtungen gerecht zu werden.