

KI-4-Everyone · Daily News

19. August 2026



SAFE

OpenAI verspricht API-Kunden: Keine Datenspeicherung

OpenAI bestätigt Zero Data Retention für API-Kunden und kündigt Private Safety Processing an – Sicherheitsprüfungen ohne Einblick in Nutzerdaten.

PROD

GitHub Copilot: Neue Übersicht für laufende KI-Aufgaben

Wer mehrere Copilot-Sitzungen gleichzeitig nutzt, behält mit dem neuen "My work"-Bereich den Überblick über offene und erledigte Aufgaben.

OpenAI verspricht Datenschutz auf Hardware-Ebene: Zero Data Retention plus Private Safety Processing

Der ChatGPT-Anbieter will fortgeschrittene Sicherheitspruefungen auch dann ermoeeglichen, wenn Kundendaten das eigene Unternehmen nicht dauerhaft erreichen sollen.

Wer als Firma mit sensiblen Daten arbeitet, steht bei KI vor einem Dilemma: Man will die besten Modelle nutzen, aber die eigenen Vertraege, Patientenakten oder Konstruktionsplaene sollen nicht auf fremden Servern landen. OpenAI reagiert nun mit einem Versprechen, das genau an dieser Stelle ansetzt. Der Anbieter bekraeftigt seine Zusage, fuer berechnete API-Kunden keine Daten dauerhaft zu speichern, und kuendigt zusaetzlich eine Technik an, die selbst Sicherheitspruefungen ohne Datenzugriff moeglich machen soll.

Konkret geht es um zwei Bausteine. Zum einen bestaetigt OpenAI die bereits bestehende Option Zero Data Retention, kurz ZDR, fuer Kunden der Programmierschnittstelle (API, die technische Verbindung, ueber die andere Firmen OpenAIs Modelle in ihre eigenen Produkte einbauen). ZDR bedeutet, dass Anfragen und Antworten nicht auf den Servern des Anbieters zurueckbleiben. Zum anderen kuendigt das Unternehmen einen neuen Ansatz namens Private Safety Processing an. Damit sollen Sicherheitspruefungen an den fortgeschrittensten Modellen laufen koennen, ohne dass OpenAI die Kundendaten dabei einsehen kann. Die Ankuendigung stammt aus einem Blogbeitrag des Unternehmens.

Der Hintergrund ist eine wachsende Spannung in der Branche. Auf der einen Seite fordern Aufsichtsbehoerden und Sicherheitsforscher, dass KI-Anbieter genau hinschauen, wofuer ihre Modelle genutzt werden - etwa um Missbrauch oder gefaehrliche Ausgaben zu erkennen. Auf der anderen Seite verlangen Grosskunden in Branchen wie Recht, Gesundheit oder Finanzen, dass ihre Eingaben das Unternehmen gar nicht erst dauerhaft erreichen.

Private Safety Processing ist der Versuch, beides zugleich zu bedienen: Sicherheit ueberpruefen, ohne den Inhalt zu lesen. Fuer Unternehmenskunden, die bislang wegen Datenschutzbedenken zoeigern, koennte das ein Argument fuer den Einstieg sein - und Konkurrenten wie Anthropic oder Google unter Zugzwang setzen, aehnliche Zusicherungen zu machen.

Was im Material offen bleibt, ist der technische Kern. Wie genau Private Safety Processing funktioniert, welche kryptografischen Verfahren dahinterstecken und ob unabhaengige Pruefer die Zusicherungen verifizieren koennen, geht aus der vorliegenden Ankuendigung nicht hervor. Auch der Zeitpunkt der Verfuegbarkeit ist unklar - der Blogbeitrag spricht von einer Vorschau (preview), was in der Branche oft heisst, dass Details und Ausrollung noch folgen. Ebenso offen: Fuer welche Modelle genau die Funktion gelten wird und ob sie Aufpreise kostet. Ohne diese Angaben laesst sich schwer beurteilen, ob es sich um eine echte technische Neuerung oder vor allem um eine vertragliche Zusage handelt.

In den kommenden Wochen lohnt der Blick auf zwei Dinge: erstens auf technische Whitepapers oder Erklaerungen, die OpenAI zu Private Safety Processing nachliefert - ohne die bleibt das Versprechen abstrakt. Zweitens darauf, ob Wettbewerber nachziehen und ob Regulierer, etwa in der Europaeischen Union, solche Datenschutz-Zusicherungen als ausreichend anerkennen oder ob sie zusaetzliche Nachweise verlangen. Fuer aufgeklärte Laien lohnt sich hier vor allem eine gesunde Skepsis: Die Frage ist nicht, was ein Anbieter verspricht, sondern was er nachpruefbar belegt.

PROD

Replit bringt kostenlosen KI-Coding-Zugang mit GPT-5.6 Luna

Replit führt einen Free Mode ein, der auf GPT-5.6 Luna läuft. Nutzer können damit Ideen direkt in funktionierende Software umwandeln – ohne Token-Kosten. Der Zugang ist für alle offen.

PROD

ChatGPT Ads startet in 31 europäischen Märkten

OpenAI weitet Werbung in ChatGPT auf 31 europäische Märkte aus. Werbetreibende erreichen Nutzer gezielt beim Vergleichen und Entscheiden. Wie genau das Targeting funktioniert, bleibt im Material unklar.

REG

OpenAI startet Initiative für demokratische KI-Aufsicht bei nationaler Sicherheit

OpenAI startet ein Programm zur Stärkung demokratischer Kontrolle von KI im Bereich nationale Sicherheit. Regierungsbehörden sollen Werkzeuge, Training und Expertise erhalten. Details zur Umsetzung nennt das Material nicht.

OS

OneCLI: Open-Source-Agenten-Plattform für Teams aus YC S26

Jonathan und Guy stellen OneCLI vor – ein quelloffenes Agenten-System für Teams. Jeder Mitarbeiter bekommt einen eigenen, abgesicherten Agenten mit Sandbox. GitHub, Gmail, Notion und Dropbox lassen sich direkt per Chat verbinden.

OS

LFM2.5: Quantisierungs-optimierte Checkpoints jetzt verfügbar

Neue Q4_0-Checkpoints für LFM2.5 entstehen per Quantization-Aware Distillation. Damit werden Modelle kleiner und effizienter, ohne stark an Qualität zu verlieren. Weitere Details nennt das Material nicht.

RES

Studie untersucht KI-Nutzungsmuster in Software-Teams

Eine Untersuchung analysiert, wie Software-Teams KI tatsächlich einsetzen. Welche Muster dabei auftreten und was die Ergebnisse konkret zeigen, ist im vorliegenden Material nicht ausgeführt.

RES

Mathematik im KI-Zeitalter: Was ändert sich für Forschende?

Ein Beitrag beleuchtet, wie KI die Mathematik verändert. Konkrete Befunde oder Zahlen enthält das Material nicht. Das Thema betrifft Forschende, die KI als Werkzeug für mathematische Arbeit nutzen.

PROD

Air Theremin: Musik machen per Handgeste vor der Webcam

Air Theremin ist ein Browser-Instrument, das Handbewegungen vor der Webcam in Töne umwandelt. Es braucht keine Installation – der Browser reicht. Technische Details zur genutzten KI-Methode nennt das Material nicht.

OS

Google veröffentlicht Bildklassifizierungs-Modell tipsv2-b14

Das Modell erkennt Bildinhalte ohne vorheriges Training auf bestimmte Kategorien. Es wurde fast 182.000-mal heruntergeladen und ist auf Hugging Face frei verfügbar.

Keine Termine gemeldet.

PROD

Privacy Gateway: Deutsches Tool filtert sensible Daten vor ChatGPT heraus

Bevor Texte an ChatGPT gehen, entfernt das Tool personenbezogene Informationen automatisch. Das soll Unternehmen vor Datenschutzrisiken schützen.

PROD

Calendly bringt KI-Mitschriften und Planungsassistenten namens Callie

Der Terminplaner Calendly steigt ins Meeting-Protokoll-Geschäft ein. Zusätzlich erscheint ein Planungsassistent namens Callie, der Termine koordinieren soll.

PROD

KI-Update kompakt: Trainingsdaten, OpenAI Astra und Fotografie im Fokus

Das KI-Update fasst dreimal pro Woche die wichtigsten KI-Entwicklungen zusammen. Aktuelle Themen sind Trainingsdaten, OpenAI Astra, Fotografie und Sonnenstürme.

PROD

Smarthome-Küche: WLAN-Dunstabzug klingt gut, nervt im Alltag

Ein Erfahrungsbericht zeigt: Vernetzte Küchengeräte machen den Alltag oft komplizierter statt einfacher. Laut dem Bericht kann das sogar gefährlich werden.

PROD

Makita-kompatibler Akku-Kompressor bei Amazon für rund 36 Euro

Ein viel gekaufter Kompressor ist mit Makita-18V-Akkus kompatibel und kostet bei Amazon knapp unter 36 Euro.