MIT Technology Review Insights

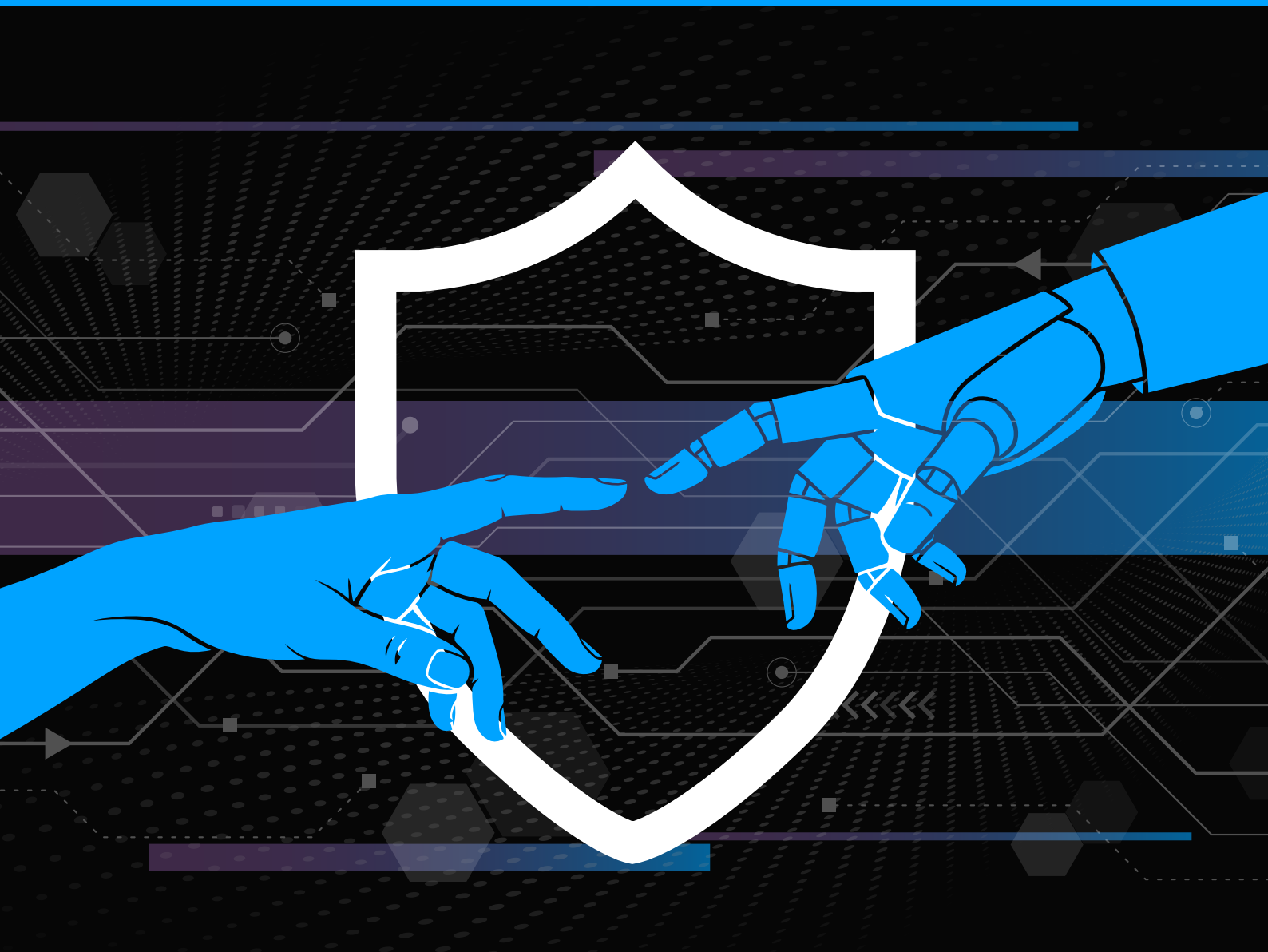
In Zusammenarbeit mit hergestellt

USERCENTRICS

Cookiebot by Usercentrics

Dateneinwilligung neu gedacht: Vom einmaligen Compliance-Akt zur nachhaltigen Kundenbeziehung.

Vertrauen im KI-Zeitalter: Wie Privacy-Led UX den Unterschied macht



Vorwort

„Vertrauen im KI-Zeitalter: Wie Privacy-Led UX den Unterschied macht" ist ein Bericht von MIT Technology Review Insights, gesponsert von Usercentrics, dem Mutterunternehmen von Cookiebot. Die vorgestellten Erkenntnisse und Perspektiven basieren auf Forschung sowie ausführlichen Interviews mit Branchenexpert:innen und Praktiker:innen, die an der Schnittstelle von Datenschutztechnologie, digitalem Marketing, Consumer Analytics und Vertrauen arbeiten. Autorin des Berichts ist Stephanie Walden, Redakteurin Laurel Ruma und Publisher Nicola Crepaldi. Die Recherche erfolgte redaktionell unabhängig. Die geäußerten Ansichten spiegeln die Perspektive von MIT Technology Review Insights wider.

Wir danken den folgenden Mitwirkenden für ihre Zeit und ihre Einblicke:

- **Tilman Harmeling,** Strategy and Market Intelligence, Usercentrics
- **Enza Iannopollo,** Vice President and Principal Analyst, Forrester
- **Max Lucas,** Senior Consultant and Managing Director, DWC Consult
- **Adelina Peltea,** Chief Marketing Officer, Usercentrics
- **Jeff Sauer,** Co-founder and CEO, MeasureU

Inhalte

Vorwort 3

01 Zusammenfassung 4

02 Digitales Vertrauen und KI 5

Das TRUST-Framework 5
Vertrauen und Chancen im Zeitalter agentischer KI 7
Die Technologie hinter Privacy-Led UX verstehen 7
Die Trust-Persona-Matrix (und warum sie wichtig ist) 8
Das Datenschutz-Paradox 9

03 Privacy-Led UX als Katalysator für digitales Vertrauen ... 10

Wie gute Privacy-Led UX aussieht 11
Interne Abstimmung vorantreiben 11
Erfolg bewerten und die richtigen Kennzahlen messen 12

04 Der ROI von Privacy-Led UX 13

Ein regulatorisches Umfeld im Wandel 14
Governance als Hebel für KI-Wachstum 15
Von der Offenlegung zur Architektur 15

Geleitwort

Der Moment, in dem Sie Kund:innen um ihre Daten bitten, ist einer der folgenreichsten Momente in der gesamten Markenbeziehung. Wer ihn richtig gestaltet, gewinnt Vertrauen, Einwilligung und die hochwertigen First-Party-Daten, die Personalisierung und verantwortungsvolle KI erst möglich machen. Wer ihn falsch angeht, verliert Kund:innen – die selten zurückkommen.

Genau diese Erkenntnis steht hinter unserem Bericht „Vertrauen im KI-Zeitalter: Wie Privacy-Led UX den Unterschied macht", den wir gemeinsam mit MIT Technology Review Insights erstellt haben. Grundlage sind Forschungsergebnisse von Usercentrics sowie Interviews mit Expert:innen aus den Bereichen Datenschutztechnologie, digitales Marketing und Consumer Analytics. Die zentrale Aussage ist klar: Datenschutz ist keine Bremse für Wachstum. Er ist eine Voraussetzung dafür.

Die Dringlichkeit ist real. Unsere Forschung zeigt, dass 77 % der Verbraucher:innen nicht vollständig verstehen, wie ihre Daten erhoben und genutzt werden. KI verschärft die Situation weiter. Mehr als die Hälfte der Nutzer:innen (59 %) fühlt sich unwohl dabei, dass ihre Daten zum Trainieren von KI-Modellen verwendet werden. Und anders als Browserdaten, die sich löschen lassen, oder eine Einstellung, die man später anpassen kann, hat KI-Training eine Dauerhaftigkeit, die Verbraucher:innen intuitiv spüren. Gleichzeitig setzen inzwischen mehr als 20 US-Bundesstaaten jeweils eigene Datenschutzregelungen um und die zuständigen Behörden zeigen, dass sie diese auch aktiv durchsetzen werden. Für Unternehmen lässt sich diese komplexe Compliance-Landschaft längst nicht mehr mit isolierten Einzellösungen bewältigen.

Organisationen, die jetzt transparente Consent-Infrastrukturen aufbauen, sind am besten aufgestellt, um KI künftig verantwortungsvoll und skalierbar einzusetzen. Datenschutz entwickelt sich zudem von einem einmaligen Einwilligungsmoment zu einer aktiv gesteuerten Datenbeziehung. Art, Zeitpunkt und Kontext der Datennachfrage wirken sich dabei direkt auf messbare Geschäftsergebnisse aus, beispielsweise auf Opt-in-Raten, Datenqualität und die Qualität der Signale, die Personalisierung und KI-Anwendungen überhaupt erst ermöglichen. Deshalb investiert Usercentrics in die Verbindungsebene zwischen Consent-Infrastruktur und den KI-Tools, die Unternehmen heute bereits einsetzen. So begleiten Datenschutzentscheidungen den gesamten Datenlebenszyklus und fließen auch in KI-Systeme ein.

Dieser Bericht gibt Ihnen eine praktische Roadmap für diesen Wandel. Er basiert auf dem TRUST-Framework mit fünf Prinzipien, um Privacy-Led UX entlang der gesamten Customer Journey umzusetzen:

- **Translate (Verständlich machen):** Klare Sprache, abgestimmt auf den Moment
- **Reduce (Reduzieren):** Weniger Consent-Hürden, höhere Opt-in-Raten
- **Unify (Vereinheitlichen):** Konsistenz über alle Touchpoints hinweg
- **Secure (Absichern):** Transparente Datenflüsse, von Anfang bis Ende
- **Track (Messen):** Vertrauen messen, etwa über Opt-in-Raten, Datenqualität und die Performance nachgelagerter Modelle

Organisationen, die diese Infrastruktur jetzt über Consent, KI-Governance und First-Party-Datenqualität hinweg aufbauen, werden deutlich besser vorbereitet sein, wenn sich das regulatorische und wettbewerbliche Umfeld weiter verschärft. Dieser Bericht zeigt, wie Sie dazu gehören können.

Adelina Peltea
Chief Marketing Officer, Usercentrics

01 Zusammenfassung

Privacy-Led User Experience (UX) (datenschutzfreundliche Nutzererfahrung) ist ein Designansatz, der Transparenz bei Datenerhebung und -nutzung als festen Bestandteil der Beziehung zu Kund:innen versteht. Im digitalen Marketing wird dieses Potenzial noch immer zu wenig genutzt. Privacy-Led UX behandelt Einwilligung nicht als bloße Checkbox für Compliance, sondern als bewussten ersten Schritt in einer fortlaufenden Kundenbeziehung. Unternehmen, die das richtig umsetzen, gewinnen etwas, das weit über reine Consent-Raten hinausgeht: das Vertrauen der Verbraucher:innen

Die Chancen von Privacy-Led UX sind erst kürzlich deutlicher geworden. Adelina Peltea, Chief Marketing Officer bei Usercentrics, beobachtet einen klaren Wandel in der Haltung vieler Unternehmen: „Noch vor wenigen Jahren wurde dieser Bereich eher als Spannungsfeld zwischen Wachstum und Compliance gesehen. Mit der Reifung des Marktes rückt jetzt stärker in den Fokus, wie sich gut gestaltete Datenschutzerlebnisse mit Geschäftswachstum verbinden lassen."

Zu den typischen Touchpoints von Privacy-Led UX gehören Consent-Management-Plattformen, Nutzungsbedingungen, Datenschutzerklärungen, Tools für Data Subject Access Requests (DSAR) sowie zunehmend auch Offenlegungen zur Nutzung von Daten in KI-Systemen.

Dieser Bericht untersucht, wie Datentransparenz Vertrauen bei Kund:innen schafft, wie sich dieses Vertrauen wiederum positiv auf die Unternehmensperformance auswirken kann und wie Unternehmen dieses Vertrauen auch dann aufrechterhalten können, wenn KI-Systeme Consent-Prozesse komplexer machen. Zu den wichtigsten Erkenntnissen gehören:

- **Datenschutz entwickelt sich von einer einmaligen Einwilligung zu einer fortlaufenden Datenbeziehung.** Führende Organisationen fragen nicht mehr zu Beginn pauschal nach weitreichenden Genehmigungen, sondern führen Datenentscheidungen schrittweise ein und passen die Tiefe der Anfrage an die jeweilige Phase der Kundenbeziehung an. Unternehmen, die so vorgehen, sammeln oft mehr und zugleich hochwertigere Daten von Verbraucher:innen, deren Wert mit der Zeit weiter steigt.

- **Privacy-Led UX ist eine Voraussetzung für den Einsatz und das Wachstum von KI.** Die Daten von Verbraucher:innen, die Organisationen erfassen, werden zunehmend zur Grundlage KI-gestützter Personalisierung. Wer jetzt klare und durchsetzbare Regeln für Datenschutz und Datentransparenz etabliert, ist besser in der Lage, KI künftig verantwortungsvoll und skalierbar einzusetzen. Das beginnt mit korrekt konfigurierten Consent-Mode-Setups auf Werbeplattformen.

- **KI-Agenten bringen ein neues Maß an Komplexität und neue Chancen.** Wenn KI-Systeme im Namen von Nutzer:innen handeln, kann der klassische Consent-Moment ganz entfallen. Die Steuerung agentisch generierter Datenflüsse erfordert eine Datenschutzinfrastruktur, die weit über das Cookie-Banner hinausgeht.

- **Privacy-Led UX erfordert funktionsübergreifende** Zusammenarbeit und klare Verantwortlichkeiten. Privacy-Led UX betrifft Marketing, Produkt, Rechtsabteilung und Datenteams. Trotzdem muss jemand die Strategie verantworten und die Fäden zusammenführen. Chief Marketing Officers (CMOs) sind dafür oft besonders gut positioniert, weil sie Marke, Daten und Customer Experience übergreifend im Blick haben.

- **Ein praxisnahes Framework hilft Unternehmen, Privacy-Led UX systematisch umzusetzen.** Organisationen müssen ihre Strategien für Datenerhebung und Datennutzung definieren und sicherstellen, dass ihre UX auch die Einwilligung integriert, einschließlich eines klaren Fokus auf Bannerdesign. Ein strukturierter Ansatz zur Bewertung und Verbesserung von Privacy-Led UX sorgt für Konsistenz an jedem Consent-Touchpoint.

02 Digitales Vertrauen und KI

Die meisten Internetnutzer:innen wissen heute, dass online nichts wirklich kostenlos ist. Jede heruntergeladene App, jeder abonnierte Service und jede Suchanfrage beruht auf einem Tausch. Immer mehr Verbraucher:innen verstehen, dass sie dabei an einem „Wertaustausch" teilnehmen, sagt Tilman Harmeling, Head of Strategy and Market Intelligence bei Usercentrics. „Selbst Apps oder Services, die kostenlos erscheinen, sind in Bezug auf die zugrunde liegenden Daten nie neutral", erklärt er.

Gleichzeitig wissen die meisten Menschen nicht genau, was sie dabei eigentlich eintauschen. Ein Usercentrics-Report zeigt, dass mehr als zwei Drittel der Verbraucher:innen, nämlich 77 %, nicht vollständig verstehen, wie Marken ihre Daten erheben und nutzen.[1]

Das TRUST-Framework

Usercentrics hat das TRUST-Framework entwickelt, einen Leitfaden zur Bewertung und Verbesserung von Privacy-Led UX an allen Kundentouchpoints. Es bildet die Grundlage für die praktischen Empfehlungen in diesem Bericht:

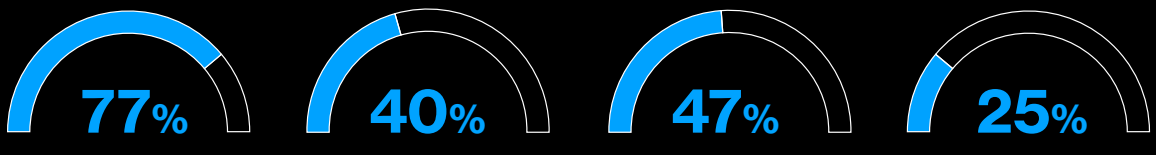
- **Translate** Formulieren Sie Datenschutzhinweise und -informationen in klarer, verständlicher Sprache. Passen Sie die Kommunikation an den jeweiligen Moment an. Kontextbezogene Hinweise entlang der Customer Journey sind deutlich wirksamer als umfangreiche Informationsblöcke auf einmal.
- **Reduce** Reduzieren Sie Reibung, ohne Auswahlmöglichkeiten einzuschränken. Gestalten Sie Consent-Oberflächen so, dass alle Optionen gleichwertig angeboten werden (akzeptieren, ablehnen oder anpassen). Die Steuerung sollte mit ein bis zwei Klicks erreichbar sein.
- **Unify** Sorgen Sie für ein konsistentes Datenschutzerlebnis über alle Touchpoints hinweg. Das Consent-Banner ist nur ein Teil eines größeren Ökosystems, zu dem auch DSAR-Tools, Preference Center, Produktberechtigungen und Hinweise bei KI-Interaktionen gehören. Inkonsistenzen zwischen diesen Elementen untergraben Vertrauen. Design und Sprache sollten daher über alle Berührungspunkte hinweg einheitlich sein.
- **Secure** Sichern Sie Datenflüsse durchgängig ab – einschließlich Drittanbieterintegrationen und KI-Tools. Machen Sie transparent, wohin Einwilligungssignale fließen, und verhindern Sie, dass KI-Tools zu intransparenten Datenverarbeitern werden, die außerhalb der Sicht von Nutzer:innen oder internen Governance-Teams agieren.
- **Track** Erfassen Sie Vertrauenssignale und optimieren Sie kontinuierlich. Etablieren Sie klare Verantwortlichkeiten auf Führungsebene und definieren Sie einheitliche KPIs über alle Teams hinweg. Messen Sie nicht nur Opt-in-Raten, sondern auch Kundenabwanderung, Kundenbindung, Engagement, Beschwerdequoten, DSAR-Anfragen und Klicks auf „Mehr erfahren". Testen Sie relevante Änderungen systematisch mit A/B-Tests.

Diese Wissenslücke führt zu präventiven und reaktiven Verhaltensweisen bei Verbraucher:innen, die versuchen, wieder mehr Kontrolle zu gewinnen. Präventiv bedeutet das zum Beispiel die Nutzung von Adblockern oder VPNs. Laut einer Studie von Forrester nutzten im Jahr 2025 mehr als 90 % der Verbraucher:innen mindestens ein Tool, um ihre digitale Privatsphäre zu schützen.[2] Reaktiv zeigt sich das in kleinen, aber aussagekräftigen Verhaltensänderungen, etwa wenn mehr Nutzer:innen Cookies ablehnen oder ihre Datenschutzeinstellungen restriktiver setzen.

“Die meisten Menschen denken sich: Ja, ich weiß, dass sie mich tracken, ich mache nur das Nötigste oder ich akzeptiere es einfach. Ich will einfach schnell zu dem, was ich eigentlich tun wollte“, sagt Jeff Sauer, Co-Founder und CEO des Marketing-Data-Unternehmens MeasureU. Das kann jedoch zu Frustration führen, etwa bei Cookie-Bannern, die Nutzer:innen am liebsten ignorieren würden. „Viele fragen sich: ‚Warum gibt es diese Banner überhaupt?‘ Obwohl sie eigentlich schützen sollen, fühlen sie sich oft wie ein Hindernis an“, ergänzt Sauer.

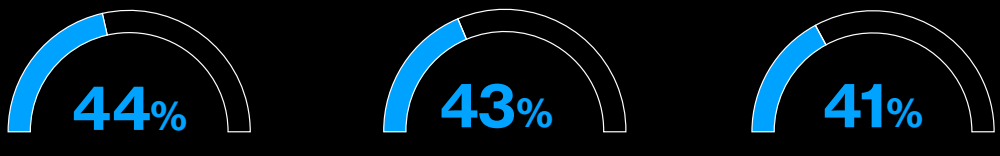
Weitere Reaktionen von Verbraucher:innen können noch folgenreicher sein. Laut der Cisco Data and Privacy Benchmark Study 2026 ist Transparenz der wichtigste Treiber für Kundenvertrauen.[3] Fällt Transparenz vollständig weg, kann auch die Beziehung zur Marke zerbrechen. Besonders deutlich zeigt sich das nach öffentlichen Vertrauensbrüchen, erklärt Enza Iannopollo, Vice President und Principal Analyst bei Forrester. „Wenn ein Unternehmen wegen einer Datenschutzverletzung in den Nachrichten ist, gehört zu den ersten Reaktionen vieler Verbraucher:innen: ‚Ich möchte vergessen werden. Ich möchte nicht, dass ihr meine Daten habt.‘“

Abbildung 1: Die Datenschutzlücke: Verbraucher:innen sind unsicher, wie ihre Daten verwendet werden, welche Rechte sie haben und wem sie vertrauen können.



Quelle: Zusammengestellt von MIT Technology Review Insights auf Basis von Daten aus „The State of Digital Trust in 2025“, Usercentrics, 2026[6]

Abbildung 2: Transparenz, Sicherheitsgarantien und die Möglichkeit, Datenfreigaben zu steuern, sind entscheidend, um Vertrauen bei Verbraucher:innen aufzubauen.



Quelle: Zusammengestellt von MIT Technology Review Insights auf Basis von Daten aus „The State of Digital Trust in 2025“, Usercentrics, 2026[7]

Sind datenbasierte Beziehungen einmal verloren, kehren sie nur selten zurück. Laut dem Thales Digital Trust Index 2025 haben 82 % der Kund:innen im vergangenen Jahr eine Marke aufgrund von Datenschutzbedenken verlassen.[4] Eine YouGov-Umfrage aus dem Jahr 2025 zeigt zudem: Zwei Drittel der Erwachsenen im Vereinigten Königreich kaufen nicht mehr bei Unternehmen, die ihr Vertrauen verloren haben. 21 % geben sogar an, dieser Marke nie wieder vertrauen zu wollen[5].

Vertrauen und Chancen im Zeitalter agentischer KI

Künstliche Intelligenz erweitert die Möglichkeiten der Datenerhebung schneller, als die Datenschutzrichtlinien der meisten Organisationen Schritt halten können. Agentische KI – also Systeme, die im Namen von Nutzer:innen handeln – entwickelt sich von einer theoretischen Möglichkeit zu einem realen Einsatzszenario und bringt besonders komplexe Fragen mit sich. Während generative KI Nutzer:innen noch bewusst entscheiden lässt, welche Informationen sie einem Chatbot oder Copilot preisgeben, handeln agentische Systeme stellvertretend. Sie können buchen, kaufen, kommunizieren und Daten weitergeben, ohne dass bei jedem Schritt eine explizite Einwilligung erfolgt.

Für datenschutzbewusste Unternehmen bedeutet das einen grundlegenden Wandel. In einem agentischen Umfeld verschiebt sich die zentrale Frage von „Versteht die Person, worin sie einwilligt?“ hin zu „Wer gibt die Einwilligung im Namen der Person, wofür und zu welchem Zeitpunkt?“

Die Technologie hinter Privacy-Led UX verstehen

Privacy-led UX erfordert eine Infrastruktur, die Nutzerentscheidungen über alle Datenflüsse hinweg konsequent durchsetzen kann. Eine neue Generation technischer Lösungen ermöglicht es Organisationen zunehmend, zu steuern, welche Daten ihre Systeme verlassen, wie sie weitergegeben werden und wie sichergestellt wird, dass Einwilligungssignale durchgängig respektiert werden.

Eine wichtige Entwicklung in diesem Bereich ist Server-Side Tagging. Anstatt Tracking-Skripte direkt im Browser der Nutzer:innen auszuführen, wo Daten unkontrolliert an Dritte abfließen können, werden sie zunächst über die eigenen Server des Unternehmens geleitet. So lässt sich nur das notwendige Minimum an Daten an nachgelagerte Partner weitergeben. Gleichzeitig können Datenübertragungen ohne Einwilligung blockiert oder gefiltert, unkontrollierte Weitergaben reduziert und ein klarer Audit-Trail darüber geschaffen werden, welche Daten wann, an wen und auf welcher Grundlage übermittelt wurden.

Sauer beschreibt den praktischen Vorteil so: „Wenn Sie auf Server-Side Tagging umstellen, können Sie beispielsweise Conversions an Meta senden, ohne die Privatsphäre dieser Person in gleicher Weise zu beeinträchtigen, weil die Daten nicht identifizierbar sind. Sie beseitigen damit die Schwächen der bisherigen Vorgehensweise und gewinnen gleichzeitig mehr Kontrolle über Ihre Daten.“

Eine schwierigere und womöglich dringendere Frage ist jedoch, was passiert, wenn Datenflüsse gar nicht mehr von Nutzer:innen selbst ausgelöst werden. Agentische KI-Systeme handeln zunehmend eigenständig und tauschen Daten mit externen Plattformen und Diensten aus, ohne dass ein klar erkennbarer Consent-Touchpoint entsteht. Die meisten Organisationen haben dafür bislang keine Governance etabliert. Ihnen fehlt oft die Transparenz darüber, auf welche Daten ihre Agenten zugreifen, geschweige denn die Kontrolle, um Nutzerpräferenzen über diese Interaktionen hinweg durchzusetzen.

Das Model Context Protocol (MCP) ist ein neuer Ansatz, um genau dieses Problem anzugehen. Es bietet einen standardisierten Rahmen, um zu steuern, wie KI-Systeme Informationen mit externen Plattformen austauschen. Darauf aufbauend kann eine Policy-Schicht festlegen, auf welche Daten ein Agent zugreifen und welche er weitergeben darf. Gleichzeitig schafft sie die Grundlage für eine revisionssichere Protokollierung und ermöglicht es Organisationen, Nutzerpräferenzen auch in automatisierten Systemen konsequent umzusetzen.

Allerdings steht diese Entwicklung noch am Anfang. Die Technologie existiert zwar bereits, doch das Bewusstsein dafür ist noch gering. „MCP ist weniger als ein Jahr alt“, sagt Adelina Peltea. „Die Verbreitung nimmt zu, aber die meisten Unternehmen wissen noch gar nicht, dass dieses Problem existiert, geschweige denn, dass es dafür erste Lösungen gibt.“

Das Zeitfenster, um der Governance-Lücke bei agentischen KI-Systemen zuvorzukommen, ist geöffnet, wird jedoch kleiner. Die notwendige Architektur rechtzeitig aufzubauen, bevor sie akut benötigt wird, gehört zu den folgenreichsten Datenschutzentscheidungen, die eine Organisation treffen kann.

In vielen Fällen entfällt der klassische Einwilligungsmoment ganz. Das hat weitreichende Folgen für Daten-Governance und unternehmerische Verantwortung. Unternehmen brauchen Infrastrukturen, die klar definieren, auf welche Daten Agenten zugreifen dürfen und wie Nutzerpräferenzen in automatisierten Prozessen berücksichtigt werden. Bislang haben sich nur wenige Organisationen mit dieser Realität auseinandergesetzt.

Die Herausforderung zeigt sich auch dort, wo KI-Agenten im Namen von Unternehmen handeln. Sie erfassen, verarbeiten und nutzen personenbezogene Daten, ohne dass ein sichtbarer Einwilligungsmoment stattfindet. Entscheidend ist hier nicht mehr, ob Nutzer:innen verstehen, worin sie einwilligen, sondern ob Organisationen in der Lage sind, Einwilligungspräferenzen in Echtzeit über alle Systeme hinweg durchzusetzen. Genau darin liegt die unmittelbare Herausforderung für Unternehmen: Consent-Architektur muss direkt in Systeme und Integrationen eingebettet sein, nicht erst nachträglich ergänzt werden.

Gleichzeitig bietet das wachsende Ökosystem der

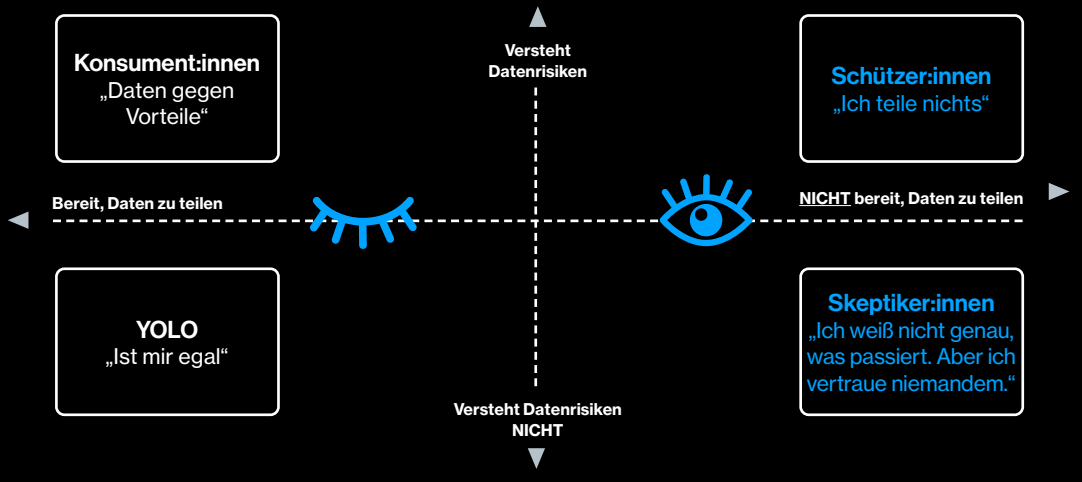
Die Trust-Persona-Matrix (und warum sie wichtig ist)

Nicht alle Nutzer:innen gehen gleich mit Datenschutz um. Usercentrics hat vier grundlegende Vertrauens-Personas identifiziert, die beeinflussen, wie Menschen Privacy-Erlebnisse wahrnehmen und darauf reagieren:

- **Konsument:innen** sind bereit, Daten im Austausch für konkrete Vorteile und ein besseres Erlebnis zu teilen.
- **Schützer:innen** sind sehr vorsichtig und stark auf Datenschutz fokussiert. Sie benötigen ein hohes Maß an Sicherheit und Vertrauen, bevor sie einer Interaktion zustimmen..
- **Skeptiker:innen** misstrauen den meisten Datenpraktiken und sind unsicher, ob Datenteilung überhaupt in ihrem Interesse liegt.
- Das **„Man lebt nur einmal"-Profil (YOLO)** ist gegenüber Datenschutzrisiken weitgehend gleichgültig und setzt sich, unabhängig vom Design, nur wenig mit Datenschutzentscheidungen auseinander.

Diese Personas zu verstehen, hilft Organisationen, Consent-Erlebnisse gezielt an die Bedürfnisse ihrer Nutzer:innen anzupassen.

Tilman Harmeling veranschaulicht das mit zwei Beispielen aus dem Bankensektor. Die Deutsche Bank, deren Markenbild stark auf Verlässlichkeit und Vertrauen beruht, verwendet eine formale und bewusste Consent-Sprache, die gut zu den Erwartungen ihrer Kundschaft passt. Revolut hingegen, eine Challenger-Bank, setzt auf eine leichtere, schnellere Ansprache, die sich an jüngere Nutzer:innen richtet, für die Geschwindigkeit und Einfachheit wichtiger sind als institutionelle Förmlichkeit.



Quelle: Zusammengestellt von MIT Technology Review Insights auf Basis von Daten von Usercentrics, 2026

Datenerhebung auch Chancen. Jede Interaktion mit einem Chatbot, jede Copilot-Anfrage und jede personalisierte Empfehlung liefert wertvolle Signale über Präferenzen und das Verhalten von Kund:innen. Damit entsteht auch die Möglichkeit, zu zeigen, dass Marken verantwortungsvoll mit diesen Daten umgehen.
Dieses Potenzial lässt sich jedoch nur ausschöpfen, wenn die Datenbeziehung von Anfang an richtig gestaltet ist. Die Vielzahl neuer Datenmomente, die KI mit sich bringt, erhöhen die Anforderungen an Consent-Kommunikation zusätzlich. Verbraucher:innen, die mit einem KI-Assistenten interagieren, haben andere Erwartungen und Bedenken als Nutzer:innen, die auf ein Cookie-Banner reagieren. Um diesen gerecht zu werden, müssen Datenschutzerlebnisse daher genauso durchdacht sein wie die KI-Funktionen selbst.

In seiner Rolle als Managing Director bei DWC Consult unterstützt Max Lucas Unternehmen bei der Einführung von Consent-Management-Plattformen – also Technologien, mit denen Marken Daten erfassen und auf Basis von Nutzerentscheidungen verarbeiten. Zu Beginn einer neuen Kundenbeziehung stellt er eine zentrale Frage: Mit welcher Consent-Adoption-Rate rechnet das Unternehmen? Bei US-Kund:innen liegt die Erwartung häufig bei rund 30 %. Wenn die tatsächlichen Daten eintreffen, sind viele überrascht, dass die Zahlen höher ausfallen.
Für Marken, die solche Touchpoints gestalten und mit Privacy-Led UX experimentieren möchten, skizziert Lucas einen dreiteiligen Ansatz: „Erstens Transparenz: Das bedeutet, Sie erklären in einer Sprache, die Nutzer:innen verstehen, was Sie tun möchten. Zweitens Mehrwert: Sie erklären, was Nutzer:innen im Gegenzug für ihre Einwilligung erhalten. Drittens Konsistenz: Das heißt, Sie bauen das Consent-Modell als natürlichen Bestandteil der User Journey auf."

Organisationen, die jetzt klare und durchsetzbare Datenschutzpraktiken etablieren, bevor KI zu tief in ihre Kundenerlebnisse integriert ist, sind künftig besser aufgestellt, um die Technologie verantwortungsvoll und in großem Maßstab einzusetzen. Privacy-led UX ist keine Einschränkung für den Einsatz von KI, sondern eine Voraussetzung dafür. Sie schafft die Grundlage dafür, dass Empfehlungen und Automatisierung überhaupt möglich sind und zuverlässig funktionieren.

Das Datenschutz-Paradox

Harmeling beschreibt eine zentrale Spannung im Umgang von Nutzer:innen mit Einwilligungen. Einerseits zeigt eine Usercentrics-Studie aus dem Jahr 2025, dass fast die Hälfte der Nutzer:innen heute seltener auf „Alle akzeptieren" klickt als noch vor drei Jahren. In vielen Märkten weltweit sinken die Opt-in-Raten. Andererseits führen die Vielzahl und Wiederholung von Datenschutzabfragen zu einer gewissen Abstumpfung. Nutzer:innen klicken sich reflexartig durch Banner, einfach weil sie ständig unterbrochen werden.
„Wir beobachten zwei Entwicklungen. Zum einen eine Art Consent-Müdigkeit: Menschen sind es leid, ständig Consent-Banner zu sehen. Gleichzeitig sehen wir aber auch das, was ich als ‚Privacy Awakening' bezeichne", sagt Harmeling. „Nutzer:innen klicken häufiger auf ‚Mehr Informationen', um besser zu verstehen, was tatsächlich mit ihren Daten passiert."

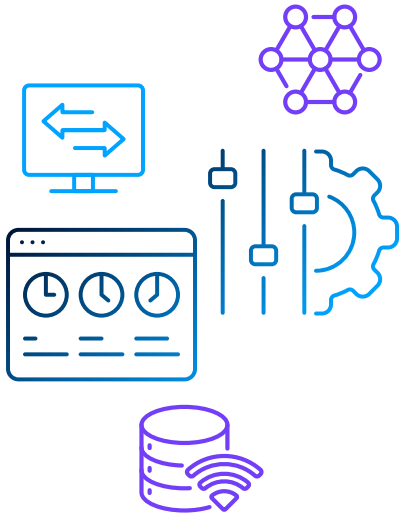
Eine ähnliche Dynamik zeigt sich auch im Umgang mit KI. Die Nutzung von KI-gestützten Tools wächst rasant, gleichzeitig steigt das Unbehagen darüber, wie Daten für Training und Personalisierung verwendet werden. Dieses Spannungsfeld wird häufig als AI Trust Gap bezeichnet (auf Deutsch KI-Vertrauenslücke).

Iannopollo hat diese Entwicklungen intensiv untersucht und sieht die Ursache weniger in der Gleichgültigkeit als vielmehr in den Rahmenbedingungen, unter denen Entscheidungen getroffen werden. „Wenn mir in den ersten zwei Sekunden auf einer Website 25 Dinge abgefragt werden, überspringe ich das wahrscheinlich", sagt sie. „Nicht, weil mir Datenschutz egal ist, sondern weil ich ein konkretes Ziel habe. Eine ausführliche Richtlinie zu lesen hilft mir in diesem Moment nicht weiter." Mit anderen Worten: Kognitive Überlastung lässt Datenschutzentscheidungen eher wie Hindernisse erscheinen als wie echte Wahlmöglichkeiten.
Dieser Druck verstärkt sich im Kontext von KI zusätzlich. Die hohe Dynamik und der Innovationsdruck führen zu einer gewissen Rationalisierung. Peltea verweist auf einen weiteren psychologischen Faktor: die Angst, den Anschluss zu verlieren, während Kolleg:innen und Wettbewerber die wohl revolutionärste Technologie unserer Zeit in rasantem Tempo einsetzen. „Viele Menschen und Unternehmen empfinden einen starken Druck: Wenn ich jetzt nicht auf KI setze, falle ich zurück. Und letztlich stimmt das auch. Es ist ein äußerst leistungsfähiges Werkzeug." Wenn Technologien unmittelbare Produktivitätsgewinne versprechen, wird der Nutzen häufig priorisiert, während Datenschutzbedenken in den Hintergrund treten.

Letztlich zeigt das Datenschutz-Paradox weniger ein Desinteresse der Nutzer:innen als vielmehr ein überlastetes System. Wenn Menschen unter Zeitdruck stehen, überfordert sind oder nicht ausreichend informiert werden, reagieren sie vor allem auf schlecht gestaltete Nutzererlebnisse.

Die zentrale Erkenntnis für Unternehmen: Sinkende Einwilligungsraten oder geringe Interaktion sind kein Zeichen von Gleichgültigkeit, sondern ein Hinweis darauf, dass das Nutzererlebnis nicht funktioniert.

03 Privacy-Led UX als Katalysator für digitales Vertrauen



Ein Consent-Banner ist oft der erste Berührungspunkt von Nutzer:innen mit den Datenpraktiken einer Marke. Und wie so oft zählt der erste Eindruck. Dennoch verfehlen viele Unternehmen dieses Ziel. Manchmal unbeabsichtigt, manchmal bewusst.

Im TRUST-Framework steht „Translate“ nicht ohne Grund an erster Stelle. Einer der häufigsten Fehler besteht darin, Nutzer:innen mit schwer verständlichen und überladenen Texten zu konfrontieren. Eine Studie von NordVPN zeigt, dass durchschnittliche Internetnutzer:innen eine ganze Arbeitswoche benötigen würden, um alle Datenschutzerklärungen der rund 96 Websites zu lesen, die sie in einem Monat besuchen.[9]

Manche Unternehmen machen sich genau das zunutze und setzen sogenannte Dark Patterns ein, also Gestaltungsmuster, die bewusst intransparent sind. Dazu gehören kognitive Überlastung durch zu viele Auswahlmöglichkeiten oder technischen Jargon, ungünstiges Timing, wenn Datenschutzentscheidungen in emotional aufgeladenen Situationen abgefragt werden, sowie unnötige Komplexität, die es erschwert, Einstellungen tatsächlich anzupassen.

Kurzfristig können solche Maßnahmen die Einwilligungsraten erhöhen. Langfristig entstehen jedoch Kosten – etwa durch höhere Absprungraten, mehr Löschanfragen oder Reputationsschäden, wenn manipulative Designs öffentlich werden. Das gilt besonders dann, wenn Marken Daten erfassen, ohne den erwarteten Mehrwert zu liefern. Sauer formuliert es deutlich: „Für mich galt im Internet schon immer eine unausgesprochene Regel: Wer Nutzer:innen mit falschen Versprechen lockt und dann enttäuscht, wird nicht lange bestehen.“

> „Sie können eine sehr schlechte oder nicht konforme Einwilligungsabfrage haben und trotzdem hohe Einwilligungsraten erzielen. Das allein sagt jedoch wenig aus. Entscheidend ist vielmehr, ob Sie Kund:innen halten oder gewinnen – und zwar als messbares Ergebnis von Privacy Design oder gezielt gestalteten Consent-Momenten. Genau daran lässt sich der Erfolg ablesen.“
>
> **Enza Iannopollo**, Vice President and Principal Analyst, Forrester

Andere UX-Fehler sind weniger offensichtlich, aber nicht weniger relevant. Dazu gehören Cookie-Banner, die visuell nicht zum Rest der Website passen, oder Datenschutztexte in einer generischen Sprache, die im Widerspruch zur Markenpersönlichkeit stehen. Solche Inkonsistenzen signalisieren subtil, dass Datenschutz eher nachträglich ergänzt wurde, statt ein bewusst gestalteter Teil der Kundenbeziehung zu sein.

Adelina Peltea weist darauf hin, dass das Problem häufig weniger im Bannerdesign selbst liegt als in einer fehlerhaften Gesamtstrategie. „Das Banner ist nur die Spitze des Eisbergs. Die Komplexität liegt nicht in der Lösung selbst, sondern darin, die gesamte Datenbeziehung zu definieren und eine UX-Strategie zu entwickeln, die auch Consent und Daten mit einschließt."

Wie gute Privacy-Led UX aussieht

Wirksame Privacy-Led UX sorgt dafür, dass Datenrichtlinien leicht verständlich sind und Datenschutzeinstellungen über die gesamte Customer Journey hinweg intuitiv genutzt werden können.
Damit zurück zum Prinzip „Translate" im TRUST-Framework von Usercentrics. Die wichtigste Best Practice ist eine klare, einfache Sprache zum richtigen Zeitpunkt. „Die Idee ist, Verbraucher:innen genau das mitzuteilen, was sie wissen müssen, genau dann, wenn sie es wissen müssen, und zwar so, dass sie kein Wörterbuch brauchen, um es zu verstehen", sagt Iannopollo.

„Unify" ist ein weiterer zentraler Grundsatz. Wenn ein Consent-Erlebnis dieselbe visuelle Sprache und denselben Wortschatz verwendet wie die übrige Markenkommunikation, vermittelt das Sorgfalt und Absicht. Tilman Harmeling nennt den Modehändler Zalando als Beispiel für gelungene Markenkonsistenz. Das Unternehmen verwendet Formulierungen wie „Wir schneiden hier alles auf dich zu" und knüpft damit sprachlich direkt an seine Markenwelt an. Porsche spricht wiederum von „voller Kontrolle" und greift damit das Fahrgefühl und die Markenidentität auf. „Diese Art von markengerechter Sprache gibt Nutzer:innen das Gefühl, willkommen zu sein", sagt Harmeling.

> „Die Unternehmen, die am weitesten sind, vermeiden die Weitergabe identifizierbarer Informationen aus zwei Gründen: Sie respektieren die Privatsphäre der Nutzer:innen und erzielen gleichzeitig bessere Ergebnisse. Genau so können Unternehmen Dateneinwilligungen zu ihrem Vorteil gestalten."
>
> **Jeff Sauer**, Co-founder and CEO, MeasureU

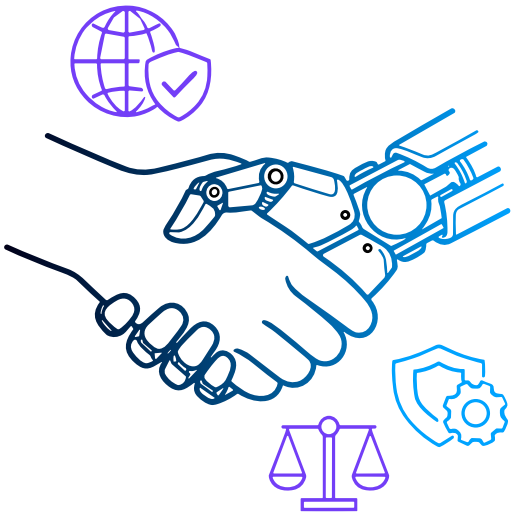
Interne Abstimmung vorantreiben

Eine zentrale Herausforderung bei der Bewertung des ROI von Datenschutz ist die interne Fragmentierung. Tilman Harmeling beobachtet hier häufig eine Lücke in funktionsübergreifenden Gesprächen über Privacy-Led UX. „Die Rechtsabteilung und das Marketing möchten beide ein vertrauenswürdigeres Umfeld schaffen. Im Kern verfolgen sie dasselbe Ziel. Aber ihre Definition von Vertrauen ist völlig unterschiedlich." Gemeinsame KPIs können helfen, hier Konsens zu schaffen und zu verhindern, dass Teams gegeneinander optimieren.

Diese Abstimmung wird zunehmend zu einer Aufgabe auf CMO-Ebene. Die Rolle bietet einen ganzheitlichen Blick auf Marke, Daten und Customer Experience und ist damit besonders gut geeignet, Datenschutzpraxis in strategisches Handeln zu übersetzen.

Die folgenden Fragen helfen, Lücken in Strategie und Verantwortlichkeiten frühzeitig sichtbar zu machen, bevor daraus hohe Kosten entstehen:

- Welche fünf Dinge sollten wir in diesem Quartal ändern, und wem gehört jeweils die Verantwortung, Marketing oder Legal?
- Woran erkennen wir in 90 Tagen, ob unsere Strategie funktioniert? Welche konkreten Signale messen wir?
- Wo liegt das Umsatzpotenzial? Welcher glaubwürdige Pfad führt von Datenschutzinvestitionen zu messbaren Geschäftsergebnissen?
- Welches Risiko entsteht, wenn wir nichts tun? Haben wir Compliance-, Reputations- und Datenqualitätsrisiken im Status quo sauber erfasst?



„Das Banner ist nur die Spitze des Eisbergs. Die Komplexität liegt nicht in der Lösung selbst, sondern darin, die gesamte Datenbeziehung zu definieren und eine UX-Strategie zu entwickeln, die auch Consent und Daten mit einschließt."

Adelina Peltea, Chief Marketing Officer, Usercentrics

Zur Säule „Unify" gehört auch die interne Abstimmung von Markenbotschaften und Governance. Privacy-Led UX liegt selten vollständig in einem einzigen Team. Sie betrifft Marketing, Rechtsabteilung, Produkt, IT und Datenverarbeitung. Eine funktionierende Umsetzung erfordert daher bereichsübergreifende Zusammenarbeit und klare Verantwortlichkeiten.

Timing ist der Punkt, an dem „Reduce" und „Translate" aus dem TRUST-Framework zusammenkommen. Iannopollo hat Customer Journeys im Finanzsektor analysiert und festgestellt, dass Datenschutzkommunikation in den meisten Fällen genau dann erscheint, wenn sie am wenigsten hilfreich ist. Oft geschieht das in besonders friktionsreichen Situationen, wenn Nutzer:innen ohnehin schon frustriert sind, etwa bei der Klärung eines Kontofehlers. Die Lösung liegt in der Struktur: Datenschutz-Hinweise sollten kontextbezogen in ruhigeren, weniger kritischen Momenten eingebunden werden, in denen Nutzer:innen eher bereit sind, sich bewusst damit auseinanderzusetzen, zum Beispiel wenn sie zum ersten Mal eine Zahlungsmethode speichern.

Führende Organisationen vermeiden es außerdem, alle Einwilligungen direkt zu Beginn gesammelt abzufragen. Peltea plädiert für das, was sie „kontextuellen Consent" nennt. „Je mehr Vertrauen Verbraucher:innen im Laufe ihrer Interaktion mit einer Marke aufbauen, desto eher können Unternehmen schrittweise weitere Informationen anfragen", erklärt sie.

Erfolg bewerten und die richtigen Kennzahlen messen

Die letzte Säule des TRUST-Frameworks, „Track", zeigt, ob Maßnahmen zur Datentransparenz tatsächlich wirken. Iannopollo betont, dass sich Investitionen in Datenschutz nur dann auszahlen, wenn mehr gemessen wird als bloße Einwilligungsraten. „Sie können eine sehr schlechte oder nicht konforme Einwilligungsabfrage haben und trotzdem hohe Einwilligungsraten erzielen. Das allein sagt jedoch wenig aus. Entscheidend ist vielmehr, ob Sie Kund:innen halten oder gewinnen – und zwar als messbares Ergebnis von Privacy Design oder gezielt gestalteten Consent-Momenten. Genau daran lässt sich der Erfolg ablesen."

Neben klassischen Kennzahlen wie Kundengewinnung und Kundenbindung empfiehlt Iannopollo, Datenschutz direkt in bestehende Feedbackschleifen zum Kundenerlebnis einzubetten. „Stellen Sie Fragen wie: ‚Haben Sie den Eindruck, dass wir transparent erklären, was wir tun? Wissen Sie, wie wir Ihre Daten verwenden?'"

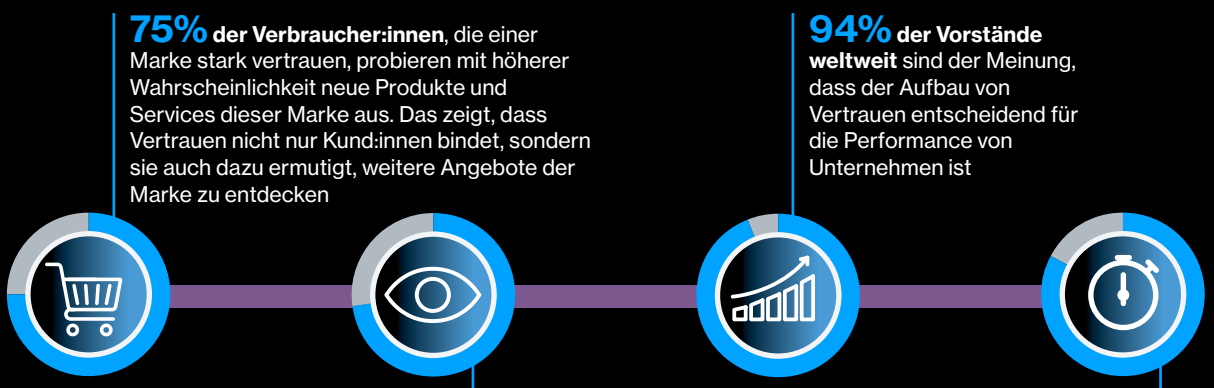
Auch A/B-Tests – also randomisierte Vergleiche zwischen zwei Varianten einer Seite oder eines Banners – sind ein bislang zu wenig genutztes Instrument. Statt sich an den Consent-Hinweisen von Wettbewerbern zu orientieren, empfiehlt Iannopollo, die eigene Version systematisch mit bisherigen Ergebnissen zu vergleichen. „Ich empfehle Unternehmen, bei jeder relevanten Änderung an Datenschutztexten oder -seiten A/B-Tests durchzuführen, weil sich so erkennen lässt, was tatsächlich funktioniert", sagt sie. „Wichtige Kennzahlen sind dabei Kundengewinnung, Kundenbindung und die erfolgreiche Einführung neuer Technologien."

04 Der ROI von Privacy-Led UX

Der direkteste Business Case für Privacy-Led UX liegt in First-Party-Daten. Sie kann sowohl die Menge als auch die Qualität von Kundendaten verbessern, weil Nutzer:innen stärker mit den Ökosystemen einer Marke interagieren. Max Lucas sagt dazu: „Wenn mehr Unternehmen Consent-Banner als Chance behandeln würden und nicht als Hindernis, könnten wir erhebliche Fortschritte beim Markenvertrauen sehen."

Iannopollo beschreibt den kumulativen Effekt von Vertrauensaufbau so: „Verbraucher:innen fühlen sich wohler dabei, Daten mit einem Unternehmen zu teilen, und genau diese Daten sind der eigentliche Wert. Wir wissen außerdem, dass Kund:innen, die einer Marke vertrauen,

Abbildung 3: Führungskräfte sehen einen starken Zusammenhang zwischen Verbrauchervertrauen und Geschäftserfolg



Quelle: Zusammengestellt von MIT Technology Review Insights, basierend auf Daten aus „Navigating Trust", Deloitte, 2026[10]

„Transparenz bedeutet, dass Sie in einer Sprache erklären, die Nutzer:innen verstehen, was Sie tun möchten. Dann kommt der Mehrwert hinzu, also die Erklärung, was Nutzer:innen im Gegenzug für ihre Einwilligung bekommen. Und schließlich die Konsistenz, also der Versuch, das Consent-Modell als natürlichen Teil der User Journey zu gestalten."

Max Lucas, Senior Consultant and Managing Director, DWC Consult

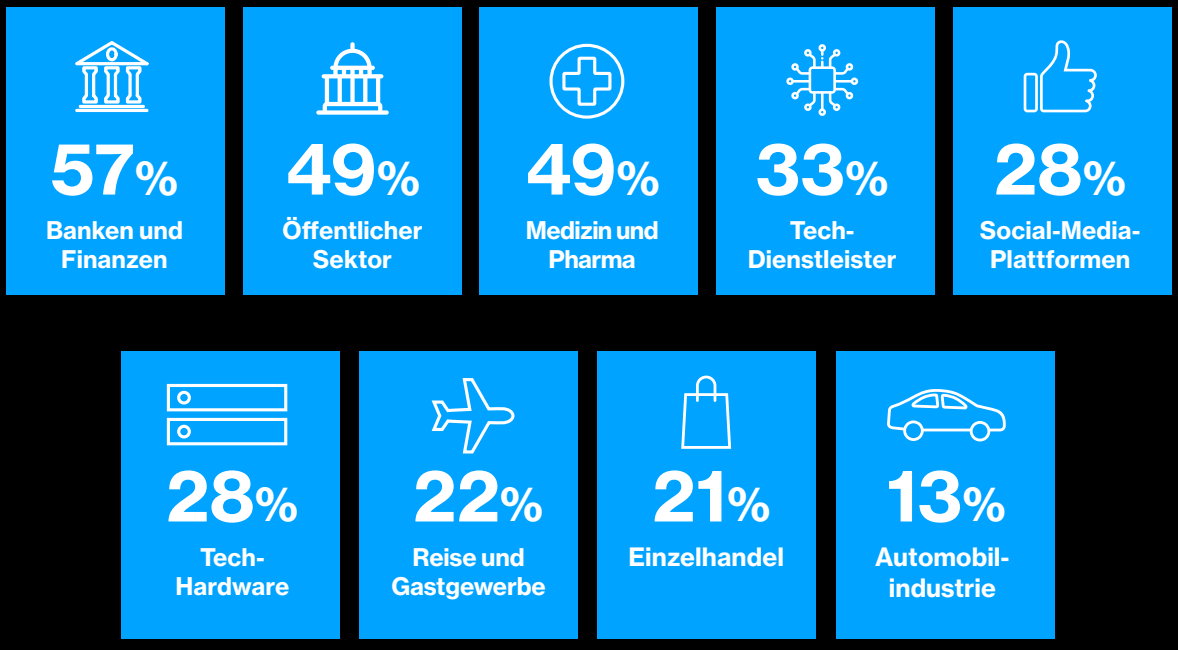
mehr kaufen und sie eher weiterempfehlen. Interessant ist auch, dass Menschen oft auch Unternehmen vertrauen, die mit einer Marke verbunden sind. Es gibt also einen Effekt auf Dritte." Für Organisationen, die KI-gestützte Personalisierung aufbauen, sind Daten mit vorheriger Einwilligung die Grundlage. Ohne sie lassen sich Modelle nicht sinnvoll trainieren.

Umgekehrt summieren sich die Kosten schlechter Privacy UX über die Zeit. Tilman Harmeling formuliert es klar: „Wenn Sie es als Unternehmen versäumen, von Anfang an ein gutes Datenschutz-Erlebnis zu schaffen, haben Sie im Kern bereits verloren. Sie verlieren Kund:innen, Vertrauen und am Ende auch Umsatz."

Ein regulatorisches Umfeld im Wandel

Das geschäftliche Argument für Privacy-Led UX wird durch ein regulatorisches Umfeld verstärkt, das zunehmend an Umfang gewinnt. In der EU hat die Datenschutz-Grundverordnung (DSGVO) die Grundlage geschaffen. Der EU AI Act ergänzt nun weitere

Abbildung 4: Verbraucher:innen teilen ihre personenbezogenen Daten am ehesten mit stark regulierten Branchen wie Banken, Behörden und dem Gesundheitswesen



Quelle: Zusammengestellt von MIT Technology Review Insights auf Basis von Daten aus „The State of Digital Trust in 2025", Usercentrics, 2026[12]

Anforderungen. In den USA haben inzwischen 20 Bundesstaaten umfassende Datenschutzgesetze verabschiedet und auch ohne einheitlichen Bundesstandard nehmen Rechtsstreitigkeiten deutlich zu.

„Viele Unternehmen in den USA haben Datenschutz lange ignoriert, weil sie dachten: Das ist eben die USA, wir haben hier keine entsprechenden Gesetze“, sagt Sauer. „Inzwischen erhalten Unternehmen jedoch Schreiben mit Klageandrohungen. Das ist am Ende der Auslöser, der sie zum Handeln bringt, nicht die abstrakte Gefahr eines Bußgelds auf einem anderen Kontinent.“

Regulierung wirkt dabei nicht nur als Compliance-Treiber, sondern auch als Vertrauenssignal. „Was wir aus den Daten zu sehen beginnen, ist, dass hochregulierte Unternehmen im Bereich KI am meisten vertraut werden. Offenbar besteht die Wahrnehmung, dass stark regulierte Organisationen wissen, was sie tun. Verbraucher:innen bringen ihnen daher automatisch mehr Vertrauen entgegen. Weniger regulierte Unternehmen schneiden in diesem Vergleich deutlich schlechter ab“, sagt Iannopollo.

Jahre nachweisbarer Compliance haben einen Vertrauensvorrat geschaffen, den Unternehmen auf ihre KI-Initiativen übertragen können. Iannopollo weist jedoch darauf hin, dass dieser Vorrat endlich ist und ein einzelner KI-Fehler in stark regulierten Branchen entsprechend besonders hohe Reputationsschäden verursachen kann.

Governance als Hebel für KI-Wachstum

Ein verantwortungsvoller KI-Einsatz basiert auf funktionierender Governance. Dazu gehören Systeme zur Nachverfolgung von Datenflüssen und Mechanismen, die sicherstellen, dass Datenschutzversprechen auch tatsächlich eingehalten werden. Ohne diese Grundlage bleibt Privacy-Led UX oberflächlich.
Es zeichnet sich zunehmend ab, dass die Einführung von KI auf denselben Governance-Strukturen aufbaut. Iannopollo berichtet, dass Forrester Datenschutzverantwortliche nach dem Return on Investment ihrer Privacy-Programme befragt hat. Die zweithäufigste Antwort im vergangenen Jahr war – nach regulatorischer Compliance – die Unterstützung bei der Einführung von KI. „Ein großer Teil dieser Arbeit unterstützt in Wirklichkeit Innovation“, sagt sie.
Gerade agentische KI macht die Notwendigkeit proaktiver Governance besonders deutlich. Automatisierte Systeme können Daten weitergeben, bevor Nutzer:innen überhaupt davon erfahren. Es gibt keinen späteren Zeitpunkt, an dem sich solche Prozesse noch korrigieren lassen. Die Berechtigungsarchitektur muss vorhanden sein, bevor der Agent handelt.

> „Wenn Sie es als Unternehmen versäumen, von Anfang an ein gutes Datenschutz-Erlebnis zu schaffen, haben Sie im Kern bereits verloren. Sie verlieren Kund:innen, Vertrauen und am Ende auch Umsatz.“
>
> **Tilman Harmeling**, Strategy and Market Intelligence, Usercentrics

Von der Offenlegung zur Architektur

Architektur wird zum zentralen Konzept in der Diskussion über Datenschutz, Datentransparenz und verantwortungsvollen KI-Einsatz. Lange Zeit spielte Datenschutz in der User Experience nur eine Nebenrolle und erschien vor allem in Richtlinien und Offenlegungen. Zunehmend wird Datenschutz jedoch selbst Teil des Produkts. Wie Unternehmen Momente von Wahl und Kontrolle gestalten, wird entscheidend dafür sein, wie Kund:innen digitale Dienste und die dahinterstehenden Organisationen bewerten.

Anders gesagt: Das letzte Jahrzehnt hat Unternehmen dazu gebracht, Datenschutz ernst zu nehmen. Das nächste wird verlangen, dass Produkte von Grund auf danach gestaltet werden.

Letztlich hängt dieser Wandel von einer Frage ab, die kein Framework und kein technischer Standard vollständig beantworten kann: Ist eine Organisation wirklich bereit, Vertrauen zu verdienen, oder versucht sie nur, den Eindruck davon zu erzeugen? Enza Iannopollo ist überzeugt, dass Verbraucher:innen diesen Unterschied besser erkennen, als viele Marken annehmen. „Die Wahrnehmung einer Marke ist ihr Goodwill. Verantwortlichkeit ist die erste Dynamik in jedem Vertrauensaufbau. Unternehmen müssen verstehen, dass genau diese Verantwortlichkeit die Grundlage für Vertrauen ist. Ich glaube, das ist heute wichtiger denn je.“

Fußnoten

1. “The State of Digital Trust in 2025,” Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
2. Stephanie Liu and Anna Hoskins, “Consumers are Privacy-Savvy and AI-Wary: Insights from the US Consumer Privacy Segmentation Report,” Forrester, October 15, 2025, https://www.forrester.com/blogs/consumers-are-privacy-savvy-and-ai-wary-insights-from-the-us-consumer-privacy-segmentation/.
3. “Cisco 2026 Data and Privacy Benchmark Study,” Cisco, https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html.
4. “Global Trust in Digital Services Declines, finds Thales,” Thales, March 18, 2025, https://cpl.thalesgroup.com/about-us/newsroom/digital-trust-index-2025.
5. Janice Fernandes, “How Brands Can Rebuild Trust with UK Consumers After Losing It,” YouGov, September 19, 2025, https://yougov.com/en-gb/articles/53019-how-brands-can-rebuild-trust-with-uk-consumers-after-losing-it.
6. “The State of Digital Trust in 2025,” Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
7. “The State of Digital Trust in 2025,” Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
8. “The State of Digital Trust in 2025,” Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.
9. Irma Šlekyt, “NordVPN Study Shows: Nine Hours to Read the Privacy Policies of the 20 Most Visited Websites in the US,” NordVPN, October 23, 2023, https://nordvpn.com/blog/privacy-policy-study-us/.
10. “Navigating Trust: An Advertiser’s and Marketer’s Guide to Data, Privacy, and Trust,” Deloitte, 2024, https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/risk-advisory/2024/us-advisory-navigating-trust.pdf.
11. F. Paul Pittman, Hope Anderson, and Abdul M. Hafiz, “US Data Privacy Guide,” White & Case, January 20, 2026, https://www.whitecase.com/insight-our-thinking/us-data-privacy-guide.
12. “The State of Digital Trust in 2025,” Usercentrics, July 1, 2025, https://usercentrics.com/resources/state-of-digital-trust-report/.

Über MIT Technology Review Insights

MIT Technology Review Insights ist die Custom-Publishing-Sparte der MIT Technology Review – des weltweit ältesten Technologiemagazins, herausgegeben unter dem Dach des Massachusetts Institute of Technology. Der Bereich konzipiert Live-Events und erstellt Analysen zu den drängendsten technologischen und wirtschaftlichen Fragestellungen unserer Zeit. Insights führt qualitative und quantitative Studien in den USA und international durch und veröffentlicht ein breites Spektrum an Formaten: Fachartikel, Reports, Infografiken, Videos und Podcasts. Sämtliche Inhalte wurden von Autorinnen und Autoren, Redakteurinnen und Redakteuren, Analystinnen und Analysten sowie Illustratorinnen und Illustratoren recherchiert, gestaltet und verfasst – einschließlich der Konzeption von Umfragen und der zugehörigen Datenerhebung. KI-gestützte Werkzeuge kamen ausschließlich in nachgelagerten Produktionsschritten zum Einsatz und unterlagen dabei einer umfassenden redaktionellen Qualitätskontrolle.

Über Usercentrics

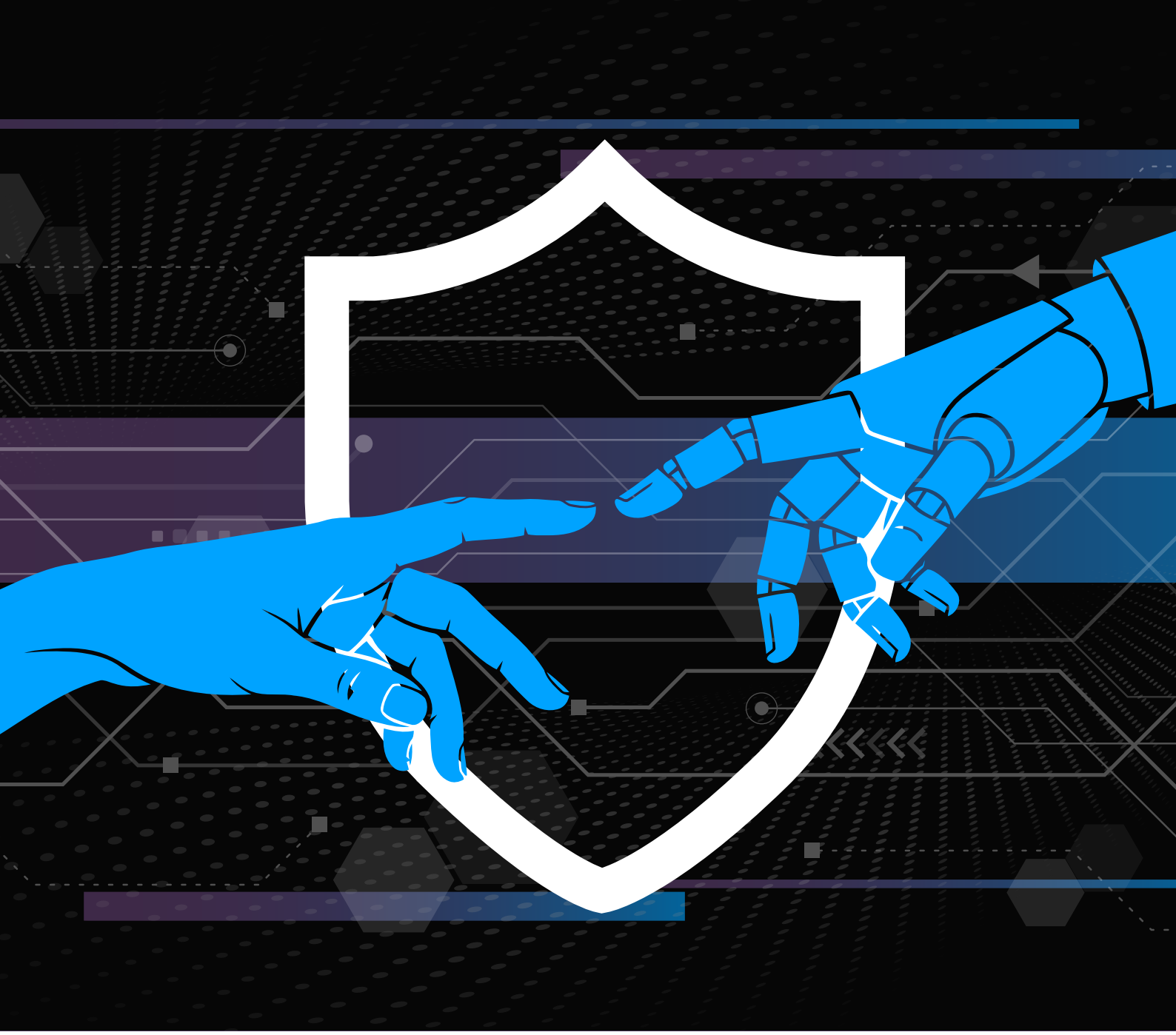
Usercentrics gehört zu den weltweit führenden Anbietern im Bereich Privacy-Technologie und unterstützt Unternehmen dabei, einwilligungsbasierte Daten in messbaren Geschäftserfolg zu verwandeln. Die Plattform ermöglicht es Organisationen, Nutzerdaten über Websites, Apps und KI-gestützte Anwendungen hinweg gesetzeskonform zu erheben, zu aktivieren und auszuwerten. Datenschutz ist dabei von Grund auf in sämtliche Datenflüsse integriert – so entsteht eine belastbare Infrastruktur für reibungslose Abläufe und nachhaltiges Wachstum. Usercentrics ist in 195 Ländern aktiv, verarbeitet monatlich über 8,8 Milliarden Nutzereinwilligungen und versetzt Marken in die Lage, besseres Marketing zu betreiben – gestützt auf die bewussten Entscheidungen ihrer Nutzerinnen und Nutzer und aufgebaut auf skalierbarem Vertrauen. Mehr unter usercentrics.com.

USERCENTRICS

Cookiebot by Usercentrics

Gestaltung von Shultz Design Collaborative, LLC. Illustrationen bereitgestellt von Adobe Stock.

Zum Zitieren dieses Berichts verwenden Sie bitte: „Building trust in the AI era with privacy-led UX“, MIT Technology Review Insights und Usercentrics, April 2026.



MIT Technology Review Insights

www.technologyreview.com

insights@technologyreview.com