doo SMART EVENT AUTOMATION

KI und Datenschutz im Eventmanagement

Was ist erlaubt, was ist möglich?

Künstliche Intelligenz bietet enorme Chancen für personalisierte Kommunikation und Automatisierung im Eventmanagement – aber was genau ist rechtlich zulässig? Darf KI die E-Mails von Teilnehmenden beantworten? Dürfen KI-basierte Chatbots eingesetzt werden oder personalisierte Einladungen mit KI basierend z.B. auf dem LinkedIn-Profil einer potenziellen Teilnehmerin generiert werden?

In diesem Whitepaper finden Sie alle wichtigen Informationen rund um KI und Datenschutz. Mehr über den generellen Einsatz von KI im Event-Management finden Sie in diesem Whitepaper.

Einleitung

Events werden immer automatisierter organisiert – und der Einsatz von Künstlicher Intelligenz (KI) spielt dabei eine wesentliche Rolle.

KI-gestützte Tools beantworten z. B. Supportanfragen, steuern Ticketing- und Check-in-Prozesse, personalisieren Inhalte und liefern Prognosen zur Auslastung.

Parallel dazu ist mit der EU-KI-Verordnung ein neuer Rechtsrahmen entstanden, der ab 2025/2026 schrittweise verbindlich wird und den Einsatz von KI-Systemen reguliert. Auch KI-Projekte müssen also immer zugleich datenschutzkonform nach DSGVO und konform nach der KI-Verordnung ausgestaltet sein. Hinzu kommen branchenspezifische Vorgaben und – bei internationalen oder hybriden Formaten – weitere Spezialregelungen.

Dieses White Paper beleuchtet, wie künstliche Intelligenz (KI) und Datenschutz im Eventmanagement zusammenspielen, und übersetzt abstrakte Rechtsvorgaben in konkrete Handlungsempfehlungen für die Praxis.

Ziel ist es, Verantwortlichen in Eventbereich einen pragmatischen Leitfaden an die Hand zu geben, mit denen sie KI-Potenziale nutzen können, ohne dabei datenschutztechnische Regeln zu brechen oder in unnötige Haftungsrisiken zu geraten.

Agenda

KI und Datenschutz: Rechtliche Grundlagen

Nicht personenbezogene Daten sind datenschutzrechtlich unbedenklich

Die erste und zentrale Frage bei jedem Einsatz von künstlicher Intelligenz (KI) dreht sich um den Datenschutz und die Verwendung von personenbezogenen Daten, also z B. Name, Adresse, Geburtsdatum oder auch die E-Mail-Adresse.

Werden von der KI keine solche personenbezogenen Daten verarbeitet, bedarf es hier keiner weiteren datenschutzrechtlichen Prüfung.

Beispiel: Return on Invest eines Events analysieren

Das KI-System erhält alle Transaktionen und Teilnehmendenzahlen, um den Erfolg des Events zu analysieren. Hierfür braucht es keine individuellen Daten der Teilnehmenden. Stattdessen es kann mit aggregierten, anonymisierten Daten gearbeitet werden. Der Anwendungsbereich der DSGVO wird somit nicht eröffnet.

Wer KI im Eventbereich wirklich effektiv und gewinnbringend verwenden will, muss dazu aber auch personenbezogene Daten verwenden. Dazu braucht es eine maximal verlässliche und gleichzeitig möglichst pragmatische Rechtsgrundlage.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Im Veranstaltungsbereich werden als Rechtsgrundlage die Einwilligung, die Vertragserfüllung oder auch das sogenannte berechtige Interesse relevant sein.

Eine Einwilligung ist die **freiwillige**, für den **bestimmten Fall**, in **informierter Weise** und **unmissverständlich abgegebene Willensbekundung**, dass man mit einer bestimmten Verwendung seiner Daten einverstanden ist.

Durch die Erteilung der Einwilligung erklärt die betroffene Person ihr Einverständnis zur Verarbeitung personenbezogener Daten. Die Einwilligung kann jederzeit widerrufen werden.

Einwilligung in die Veröffentlichung von Fotos

Die Teilnehmenden bestätigen vor Ort eindeutig und freiwillig, dass sie mit der Veröffentlichung von Fotos einverstanden sind. Alternativ kann diese Einwilligung vorab bei Anmeldung mittels Opt-In abgefragt werden, was aber keinen Einfluss auf die Anmeldung an sich haben darf.

KI und Datenschutz: Rechtliche Grundlagen

Die Rechtsgrundlage der Vertragserfüllung erlaubt die Verarbeitung personenbezogener Daten, wenn diese zwingend erforderlich ist, um einen Vertrag mit der betroffenen Person zu erfüllen oder vorvertragliche Maßnahmen auf deren Anfrage durchzuführen. Die Verarbeitung muss für den Vertragszweck notwendig sein.

Beispiel: Die Veranstaltung findet hybrid statt. Die Verarbeitung der E-Mail-Adresse ist somit erforderlich, um dem Teilnehmenden den Zugangslink für die Online-Plattform zuschicken zu können.

DIe dritte relevante Rechtsgrundlage ist das **berechtigte Interesse**. Hiernach ist eine Datenverarbeitung erlaubt, wenn sie zur Wahrung der Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Das ist aber nur soweit zulässig, sofern keine überwiegenden Grundrechte oder Interessen der betroffenen Person entgegenstehen.

Beispiel: KI-gestützte Betrugserkennung bei Event-Ticketkäufen

Es wird ein KI-System genutzt, um Ticketkäufe automatisch auf Betrug oder massenhafte Bot-Bestellungen zu prüfen. Dabei werden z.B. auffällige Kaufmuster, IP-Adressen oder ungewöhnlich große Bestellmengen analysiert. Grundlage hierfür ist das „berechtigte Interesse“, da der Veranstalter sein Event vor Betrug schützen und eine faire Ticketverteilung sicherstellen möchte.

Grundsätze der Datenverarbeitung

Liegt eine der drei oben genannten Rechtsgrundlagen vor, ist im nächsten Schritt die Datenverarbeitung an sich zu prüfen. Zur Vermeidung von Datenschutzverstößen gibt es vier Grundsätze: Datensparsamkeit, Zweckbindung, Transparenz und Vertraulichkeit.

Datensparsamkeit – weniger ist mehr

Der Grundsatz der Datensparsamkeit – auch als Datenminimierung oder Datenvermeidung bezeichnet – besagt, dass bei der Verarbeitung von personenbezogenen Daten nur die Daten erhoben und verwendet werden dürfen, die für den jeweiligen Verarbeitungszweck erforderlich sind.

Gerade KI-Projekte verleiten dazu, die Datensätze ungefiltert zu verwenden. Der Mehrwert ist dabei in der Regel überschaubar.

Auch und insbesondere bei mit KI generierten Datensätzen dürfen nur Daten erhoben werden, die wirklich notwendig sind. Für die Anmeldung zu einem Konzert ist es somit **nicht relevant, welchen Beruf die Teilnehmenden haben. Relevant sind dagegen Name und Adresse**, um die Eintrittskarten zu personalisieren und zuschicken zu können.

KI und Datenschutz: Rechtliche Grundlagen

Als Merkhilfe zur Datensparsamkeit gilt **„NO SPORTS“:**

S

Sensitive Data
Besonders sensible personenbezogene Daten wie Gesundheit, Ethnie, politische Meinungen

P

Personal Data
Personenbezogene Daten – nur nutzen, wenn nötig und erlaubt

O

Outdated Data
Veraltete Informationen, die nicht mehr stimmen

R

Redundant Data
Doppelte oder überschüssige Daten

T

Trivial Data
Belangloses, für den jeweiligen Zweck nicht relevante Daten

S

Secret Data
Vertrauliche Infos und/oder Geschäftsgeheimnisse

Zweckbindung

Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Wurde eine E-Mail-Adresse abgefragt, um den Zugangslink oder das Ticket zu schicken, darf diese E-Mail-Adresse grundsätzlich nicht für weitere, andere Zwecke verwendet werden, wie zum Beispiel das Zusenden eines Newsletters mit Terminankündigungen.

Mit Blick auf die Nutzung von KI sind hier vor allem Bestandsdaten problematisch. Daten, die bereits erhoben wurden, wurden zwangsläufig (noch) nicht mit dem Zweck „KI-Training“ oder allgemein im KI-Kontext erhoben. Hier ist also ganz genau zu prüfen, welche Bestandsdaten in die KI einfließen oder eben nicht.

Transparenz

Das Datenschutzrecht setzt zudem voraus, dass über die Verwendung der erhobenen Daten transparent informiert wird. Betroffene, deren personenbezogene Daten verwendet werden, müssen darüber informiert sein, wie und vor allem zu welchen Zwecken die Daten verarbeitet werden.

Wenn KI zur Anwendung kommt, ist den Betroffenen transparent zu kommunizieren, dass KI eingesetzt wird – und zu welchen Zwecken. Das schafft Vertrauen und auch Akzeptanz für die Verwendung.

KI und Datenschutz: Rechtliche Grundlagen

Soll bei einer Veranstaltung KI eingesetzt werden, sei es als Chatbot oder für die Nachbereitung, muss dies von vornherein klar ersichtlich sein. Das Event braucht daher eine wasserdichte Datenschutzerklärung.

Vertraulichkeit

Personenbezogene Daten und auch sonstige vertrauliche Informationen und Geschäftsgeheimnisse müssen vertraulich behandelt werden. In KI-Kontext geht es dabei vor allem darum, dass Daten nicht ungeprüft in externe, öffentliche KI-Tools, wie ChatGPT & Co eingespeist werden dürfen.

Es ist daher immer zu prüfen, was die KI mit den Daten macht, wie der Datenschutz ausgestaltet ist und ob die Datenverarbeitung innerhalb oder außerhalb der EU stattfindet.

Zudem sollte geprüft sein, ob das externe KI-Tool die eingespeisten Daten verwendet, um das KI-Modell weiter zu trainieren. Insbesondere Letzteres muss auf jeden Fall ausgeschlossen werden – sonst besteht das Risiko, dass sich die eingegebenen Daten plötzlich in den Antworten an andere Nutzer wiederfinden.

EU AI-Act: Das Gesetz zur künstlichen Intelligenz

Der Gesetzgeber hat den Umgang mit KI-Tools in der sogenannten KI-Verordnung (EU-AI-Act) geregelt. Die Verordnung ist im August 2024 in Kraft getreten und in Teilen seit Februar 2025 innerhalb der EU anwendbar.

Ziel der KI-Verordnung ist es, einen einheitlichen Rechtsrahmen für die Entwicklung, das Inverkehrbringen und die Nutzung von künstlicher Intelligenz in der EU zu schaffen. Zudem soll sichergestellt werden, dass KI sicher, transparent und ethisch vertretbar eingesetzt wird und keine Grundrechte verletzt werden. Es soll Vertrauen geschaffen werden und gleichzeitig Innovation vorangebracht werden.

Was ist KI?

KI ist eine Technologie, die Computer dazu befähigt, Aufgaben zu erledigen, für die normalerweise menschliche Intelligenz nötig ist – zum Beispiel Texte verstehen, Bilder erkennen, Entscheidungen treffen oder Fragen beantworten.

KI kann zur Unterstützung bei Routinetätigkeiten eingesetzt werden. Sie hilft, die Produktivität zu steigern und bessere Entscheidungen zu treffen.

KI birgt jedoch auch einige Risiken. KI kann falsche oder frei erfundene Informationen liefern. Dies ist auch unter dem Phänomen der “halluzinierenden KI” bekannt. Die Antworten wirken oft überzeugend, sind aber nicht immer korrekt. KI-generierte Ergebnisse müssen immer von einem Menschen geprüft werden.

KI kann unbewusst bestimmte Gruppen oder Meinungen bevorzugen oder benachteiligen. Dieses Phänomen wird auch “Bias” genannt. Das passiert, wenn die Trainingsdaten nicht ausgewogen sind. Darum ist ein kritischer Umgang mit Ergebnissen wichtig, was auch die menschliche Kontrolle mit einschließt.

Problematisch sind zudem automatisierte Entscheidungsfindungen. Dabei trifft eine KI vollkommen autark und ohne „Human in the Loop“ rechtlich relevante Entscheidungen. Dies wird oft mit dem HR-Bereich in Verbindung gebracht: Hier werden mitunter Bewerbungen komplett ohne menschliches Mitwirken oder Sichten aussortiert.

Mehr über den Einsatz von KI im Event-Bereich sowie über den gezielten Einsatz von KI-Agenten erfahren Sie in einem weiteren, ausführlichen doo Whitepaper. Dieses finden Sie unter https://www.doo.net/learning-center-single/ki-eventmanagement

EU AI-Act: Das Gesetz zur künstlichen Intelligenz

Regulierung durch KI-VO
Die KI-Verordnung stuft KI-Systeme in vier Risikokategorien ein. Je höher das Risiko ist, desto mehr Regularien sind bei der Verwendung von KI zu beachten.

verboten

Grundsätzlich verboten sind laut EU-AI-Act KI-Systeme bei manipulativen Systemen oder Social Scoring, weil das damit verbundene Schadenspotenzial zu hoch ist. Hierunter fallen zum Beispiel Social Scoring nach chinesischem Vorbild, die biometrische Echtzeit-Identifizierung im öffentlichen Raum sowie KI zur bewussten Manipulation von Menschen.

hohes Risiko

Unter Hochrisiko-KI-Systeme fallen Anwendungen wie Recruiting-Auswahlverfahren, Leistungsbewertungen, Kredit/Scoring, medizinische Anwendungen, sicherheitskritische Infrastruktur und das autonome Fahren.

Hochrisiko-KI-Systeme unterliegen strengen Anforderungen, darunter Risikoanalysen, Transparenzverpflichtungen und menschlicher Überwachung. Bei der Verwendung solcher Hochrisiko-KI ist eine detaillierte technische Dokumentation zu erstellen und kontinuierliche Risikoüberprüfungen durchzuführen.

begrenztes Risiko

Unter KI-Systeme mit begrenztem Risiko fallen Chatbots, KI-generierte Inhalte (Social Media Posts) oder einfache Empfehlungssysteme. Diese Risikokategorie unterliegt Transparenzpflichten. Nutzer müssen darüber informiert werden, dass sie mit einer KI interagieren bzw. das die Inhalte von einer KI generiert wurden. Dies ist für die Eventbranche besonders interessant und wird bereits in der Praxis eingesetzt.

Dabei werden Chatbots für die schnelle und einfache Kommunikation mit den Teilnehmenden eingesetzt. Die KI erstellt und personalisiert die Einladungen.

EU AI-Act: Das Gesetz zur künstlichen Intelligenz

Der Chatbot auf der Event-Website braucht somit einen Hinweis á la „Powered by AI“. KI-generierte Texte und Bilder müssen gekennzeichnet werden. Hier lässt sich auch eine direkte Verknüpfung zum Datenschutz herstellen, der ebenfalls Transparenzpflichten vorschreibt.

minimales Risiko

Als vierte Kategorie gibt es KI-Systeme mit einem minimalen Risiko, die keinen speziellen Regulierungen unterliegen und an die auch keine verpflichtenden Anforderungen hinsichtlich Transparenz, Dokumentation oder menschlicher Aufsicht gebunden sind.

Beispiele dafür sind Spam-Filter, KI-gestützte Schreibassistenten oder Assistenten für automatische Textvorschläge, die im Event- und Veranstaltungsbereich bereits Anwendung finden.

Checkliste Legal

Um KI-Systeme rechtskonform in der Praxis einzusetzen, sollten folgende Punkte abgefragt und geprüft werden:

- Werden **personenbezogene Daten** benötigt?
- **Rechtsgrundlage abklären –** Einwilligung, Vertrag oder berechtigtes Interesse? (letzteres mit Transparenz und Abwägung).
- **Datenminimierung** beachtet? Nur die nötigsten Daten verwenden. Kein “Datensammelrausch”.
- **Zweckbindung** gewahrt? Daten nur für legitime, vorher definierte Zwecke einsetzen – bei neuen Zwecken neu nachdenken.
- **Transparenz** hergestellt? Betroffene informieren (Privacy Notice, Hinweise im UI) über KI-Einsatz.
- **Automatisierte Entscheidungen?** Wenn ja, sicherstellen, dass sie niemanden ohne menschliche Prüfung benachteiligen.
- **Datensicherheit** gewährleistet? Keine unnötigen Datenlecks – nur vertrauenswürdige KI-Tools nutzen, keine geheimen/personenbezogenen Daten in unsichere Kanäle laden.
- **Ergebnisse überprüfen!** Menschlicher Qualitätscheck für ale Ergebnisse, vor allem, wenn Personen davon betroffen sind.

Use Cases Kommunikation und Interaktion mit Teilnehmenden

Use Case 1: KI beantwortet E-Mails von Teilnehmenden

Szenario

Das Postfach quillt über mit zig E-Mails von Teilnehmenden, wie z.B: “Wo finde ich mein Ticket?”, “Kann ich meinen Workshop-Slot wechseln?”, “Gibt es Parkplätze?”

Relevante Fragenstellung

Dürfen Inhalte einer E-Mail von Teilnehmenden kopiert und von einem KI-System beantwortet werden? Darf die KI komplett autonom auf E-Mails reagieren?

Datenschutz & KI Check

- **Rechtsgrundlage:** Als Rechtsgrundlage kommt der Vertrag oder auch das berechtige Interesse in Frage. Bei einer Supportanfrage durch einen Teilnehmenden, wird von diesem eine Antwort erwartet. Die Verarbeitung seiner Daten im Rahmen einer konkreten Frage zu dem Event dient der Vertragserfüllung.

  Zudem besteht ein berechtigtes Interesse, effizient Support zu leisten – das ist eindeutig auch im Sinne des Anfragenden, der effizienten Support erwartet. Eine zusätzliche Einwilligung ist daher weder erforderlich noch praktikabel.

- **Datentransfer an KI-Anbieter:** Bei der Nutzung von KI ist immer zu unterscheiden, ob es sich um eine “eigene KI” handelt oder ein externer Dienst herangezogen wird. Sobald personenbezogene Daten an einen Dienstleister als Auftragsverarbeiter übermittelt werden, wird ein Auftragsver-arbeitungsvertrag (AVV) benötigt.

  Findet die Datenverarbeitung außerhalb der EU statt, wird ein zusätzlicher “Transfermechanismus” benötigt, um sicherzustellen, dass die Datenverarbeitung europäischen Standards unterliegt. Bei internationalen Datentransfers muss exakt geprüft werden, ob der Anbieter tatsächlich unter dem EU-U.S. Data Privacy Framework zertifiziert ist oder ob auf Standardvertragsklauseln der EU-Kommission (Standard Contractual Clauses bzw. SCCs) zurückgegriffen werden muss.

  Die Daten dürfen zudem von dem System nicht zu KI-Trainingszwecken genutzt werden. Daten können zwar so aufbereiten werden, dass keine

Use Cases Kommunikation und Interaktion mit Teilnehmenden

personenbezogenen Inhalte übertragen werden. Dies steht jedoch im Widerspruch zu einen effektiven KI-Support.

- **Automatisierungsgrad:** Antwortet die KI komplett autonom und wird dadurch die betroffene Person erheblich beeinträchtigt, ist das eine automatisierte und damit rechtswidrige Entscheidung. Zudem gefährdet eine komplett autonome Entscheidung die Qualität eines effizienten Supports und es besteht die Gefahr von Halluzinationen. Die KI sollte also nicht ausschließlich autonom arbeiten, sondern immer durch einen Menschen kontrolliert werden (“human in the loop”). Dies gilt insbesondere, wenn es um sensible Daten, wie zum Beispiel Barrierefreiheit geht.

- **Transparenz:** Ausdrücklich muss nicht über den Einsatz von KI in diesem Szenario informiert werden, solange ein Mensch verantwortlich bleibt und die Antworten sinnvoll und korrekt sind. Hätte die KI mit dem oder der Teilnehmenden gechattet und es wäre kein Mensch involviert, gäbe es einen neuen Fall.

  Unabhängig davon ist es aus datenschutzrechtlicher Transparenz empfehlenswert, in der Datenschutzerklärung darauf hinzuweisen, dass mit KI-gestützten Systemen gearbeitet wird und diese zur Bearbeitung von Anfragen eingesetzt werden.

Fazit & Empfehlung

Ja, KI darf E-Mails von Teilnehmenden beantworten. Es ist datenschutzrechtlich zulässig, solange ein legitimer Zweck, wie z. B. der effiziente Support, vorliegt und verantwortungsvoll mit den Daten umgegangen wird.

- KI ist vorzugsweise **als Assistenz** einzusetzen, nicht als alleinige, automatische - Antwort. Ein menschlicher Mitarbeitender sollte, insbesondere bei heiklen Fällen, nachprüfen und die Qualität gewährleisten.

- Geeignete Tools sind in der eigenen Service-Plattform integrierte KIs oder ein EU-basierter Dienst mit Vertrag. Es sollten **keine sensiblen Rohdaten** an unbekannte Dritte gesendet werden, auch nicht zu Trainingszwecken.

- Keine besondere Kategorien von Daten, wie z.B. Gesundheitsdaten, verwenden.

- **Datenschutzinformation updaten:** Transparent kommunizieren, dass Supportanfragen mit Hilfe von KI bearbeitet werden.

Use Case 2: Chatbot statt Hotline Szenario

Szenario

Es wird ein Chatbot eingesetzt, der für die Kunden 24/7 erreichbar ist und das Team entlasten soll.

Relevante Fragenstellung

Darf ein Chatbot eingesetzt werden und direkt Teilnehmenden die Fragen beantworten?

Datenschutz & KI Check

- Ein Chatbot interagiert direkt mit Teilnehmenden. Bei einem vollständig anonymen Chat fehlt der Personenbezug. Ein Beispiel wäre die Frage “Wann ist die Mittagspause?”. Bei einer Eingabe von Fragen mit Namen oder Vertragsdaten werden dagegen auch personenbezogene Daten verarbeitet.

- **Rechtsgrundlage:** Die Beantwortung von Teilnehmendenfragen ist durch den Vertrag oder durch berechtigtes Interesse gedeckt.

  Es besteht ein Interesse, den Eventvertrag zu erfüllen und effizienten Support zu bieten und den Teilnehmenden einen reibungslosen Ablauf zu gewährleisten.

  Dabei sind die gegenseitigen Interessen abzuwägen. Werden einfache Fragen zu Location oder Organisation gestellt, greift der Chatbot nicht bzw. nur minimal in die Privatsphäre ein. Der Chatbot hat nur die Daten zu sammeln, die unbedingt benötigt werden und idealerweise geben Teilnehmenden auch nur diese ein. Solange Transparenz eingehalten wurde, wird die Abwägung in der Regel zugunsten des Einsatzes eines Chatbots ausfallen. Für die Frage „Wann geht das Event los?“ werden z. B. gar keine persönlichen Daten, benötigt.

- **Transparenz und Datensparsamkeit:** Der Nutzer muss wissen, dass er mit einer KI chattet, ansonsten beeinflusst dies das Vertrauensverhältnis und verstößt gleichzeitig gegen die Transparenzpflicht. Es ist daher klar kenntlich zu machen, dass der Chatbot KI-basiert arbeitet. Hierfür genügt ein schriftlicher Hinweis, wie z. B. „Sie chatten hier mit einem KI-Assistenten bzw. KI-Chatbot“. Auch ein Icon oder eine andere grafische Lösung kann diesen Zweck erfüllen.

Use Cases Kommunikation und Interaktion mit Teilnehmenden

Zudem sollte auch in der Datenschutz erklärung darauf hingewiesen werden, a) dass Daten gesammelt werden und b) welche Daten genau erfasst werden. Des Weiteren sollte ausdrücklich erwähnt sein, dass eine KI die Eingabe verarbeitet.

Der Chatbot sollte möglichst keine vertraulichen Informationen abfragen, es sei denn, diese sind zur Beantwortung der Frage unbedingt nötig. Je weniger Daten abgefragt werden, desto geringer ist das rechtliche Risiko. Auch die Trainingsdaten des Chatbots sollten sauber und ohne unnötige Altlasten sein.

Dies gilt auch für Fragen mit persönlichem Bezug: So kann der Chatbot z. B. zur Beantwortung einer Buchungsanfrage die Ticket-ID statt dem Namen abfragen.

- **Modell und Hosting:** Da bei der Nutzung eines Chatbots regelmäßig personenbezogene Daten verarbeitet werden, ist ein On-Premise-System oder eine EU-gehostete Lösung empfehlenswert. Wird der Chatbot über eine externe Plattform betrieben, ist sicherzustellen, dass die datenschutzrechtlichen Anforderungen eingehalten werden. Insbesondere ist – sofern der Anbieter als Auftragsverarbeiter tätig wird – ein entsprechender Auftragsverarbeitungsvertrag (AVV) abzuschließen.

Use Cases Kommunikation und Interaktion mit Teilnehmenden

Bei internationalen Datentransfers muss zudem geprüft werden, ob der Anbieter tatsächlich unter dem EU-U.S. Data Privacy Framework zertifiziert ist oder ob auf Standard Contractual Clauses (SCCs) zurückgegriffen werden muss.

- **Automatisierungsgrad:** Dem Chatbot sind Grenzen zu setzen. Wird eine Frage nicht verstanden, müssen Halluzinationen vermieden werden. Es sind daher feste Fallback-Antworten wie zum Beispiel „Da bin ich überfragt, ich leite Sie an einen Kollegen weiter“ zu konfigurieren.

Der Chatbot sollte bei sensiblen Themen immer einen Menschen ins Boot holen. Bei einer Anfrage zum Datenschutz oder bei komplexen Problemen sowie bei emotionalen Themen sollte die Anfrage immer an einen menschlichen Mitarbeitenden delegiert werden.

Fazit & Empfehlung

Ja, ein Chatbot darf eingesetzt werden, um Fragen von Teilnehmenden zu beantworten. Die Anwendung ist unter Beachtung der rechtlichen Grundlagen datenschutzkonform und verbessert den Service.

- **Offen kennzeichnen**, dass es ein KI-Chatbot ist, z. B. mit einem Icon und / oder einem kurzen schriftlicher Hinweis.
- In der **Datenschutzerklärung** erklären, welche Daten im Chat erfasst und wofür diese verwendet werden.
- **Datenbegrenzung:** Den Chat so gestalten, dass Nutzer möglichst keine sensiblen Daten eingeben müssen. Keine Speicherung von Chats länger als nötig.
- Zur **technischen Absicherung** sind die Nutzung eines EU-Servers oder eines eigenen Servers empfehlenswert. Bei Beauftragung von externen Dienstleistern ist ein Auftragsverarbeitungsvertrag (AVV) gesetzlich verpflichtend.
- **Halluzinationen ausschließen:** Der Bot sollte im Zweifel an einen menschlichen Support-Mitarbeitenden verwiesen („Ich verbinde Sie mit einem Kollegen…“)
- **Berechtigtes Interesse dokumentieren:** Interne Abwägung, warum der Bot zulässig ist (Entlastung, 24/7 Service vs. minimale Eingriffe in Datenschutz)

Use Cases Kommunikation und Interaktion mit Teilnehmenden

Use Case 3: Personalisierte Einladungen und individuelle Schreiben

Szenario

Eventeinladungen oder auch Dankesschreiben sollen personalisiert werden. Die Individualisierung geht dabei über eine persönliche Anrede hinaus und soll sich je nach Adressat auf frühere Teilnahmen stützen oder branchenspezifische Texte enthalten.

Relevante Fragenstellung

Kann KI dazu verwendet werden, um personalisierte Anschreiben zu generieren, ohne den Datenschutz zu verletzen?

Datenschutz & KI Check

Personalisierte Texte enthalten personenbezogene Daten (Namen, Firma, Teilnahme frühere Events). Auch der KI-generierte Output (Einladung, Schreiben) enthält wiederum personalisierte Daten. Der Anwendungsbereich des Datenschutzes ist eröffnet.

- **Rechtsgrundlage:** Beim Versand von Einladungen an ehemalige oder potenzielle Teilnehmende handelt es sich in der Regel um Direktwerbung. E-Mail-Werbung an Bestandskunden ohne ausdrückliche Einwilligung ist laut Gesetz gegen unlauteren Wettbewerb (UWG) erlaubt, wenn die gesetzlichen Voraussetzungen eingehalten werden. Die verwendeten Daten müssen im Zusammenhang mit einem vorherigen Verkauf oder der Bewerbung ähnlicher Leistungen stehen.

  Datenschutzrechtlich wird Direktwerbung auf die Rechtsgrundlage des berechtigten Interesses gestützt, wobei stets eine einfache Widerspruchsmöglichkeit bestehen muss. Bei Neukontakten ist E-Mail-Werbung grundsätzlich nur mit vorheriger Einwilligung zulässig; das berechtigte Interesse kann zwar hier je nach Kommunikationskanal (z. B. postalische Werbung) in Betracht kommen, dies gilt in der Regel aber nicht für E-Mail-Werbung.

  Für personalisierte Einladungen werden in der Regel Daten verwendet, die bereits rechtmäßig erhoben wurden. Eine maßvolle Personalisierung kann sowohl im Interesse des Veranstalters als auch der Empfänger liegen, weil zielgerichtete Informationen oft als relevanter wahrgenommen werden als generische Massenmails. Gleichwohl sollte der Inhalt sensibel gestaltet werden: Entsteht der Eindruck umfassender Nachverfolgung

Use Cases Kommunikation und Interaktion mit Teilnehmenden

oder Profilbildung, kann dies zu Akzeptanzproblemen und Vertrauensverlust führen.

KI-generierte Inhalte sollten zudem unbedingt vor Versand durch einen Menschen geprüft werden, um rechtliche und kommunikative Risiken zu minimieren.

- **Datentransfer an KI-Anbieter:** Bei der Nutzung externer KI-Diensteister ist genau zu prüfen, ob der Anbieter datenschutzkonform arbeitet. Mit Blick auf die Datenminimierung sollte die KI platzhalterbasiert arbeiten. Personendaten sollten erst im Nachgang per Serienmail-Tool eingefügt werden.

  Die KI sollte also keine echten Daten, sondern nur abstrakte Daten erhalten. Dadurch wird das Missbrauchsrisiko deutlich minimiert.

- **Transparenz:** Es muss klar kommuniziert sein, dass im Rahmen des Events personalisierte Informationen und Unterlagen versendet werden. Der Einsatz von KI ist dagegen nicht zwingend zu erwähnen, solange die Datennutzung an sich rechtlich abgedeckt ist.

- **Bewertungsschreiben/Zertifikate:** Sollen nach dem Event personalisierte Schreiben, Teilnahmebestätigungen mit tatsächlich besuchten Programmpunkten oder ein individuelles Dankesschreiben für Feedback mittels KI generiert werden, dürfen die bereits vorhanden Daten verarbeitet werden. Diese dürfen auch verwendet werden, um den Teilnehmenden ein Follow-up zu schicken.

  Beides ist auf das berechtigte Interesse an der Kundenpflege gestützt. Hinzu kommt, dass dieses Vorgehen von den Teilnehmenden erwartet werden darf.

Use Cases Kommunikation und Interaktion mit Teilnehmenden

Fazit & Empfehlung

Ja, KI kann Eventeinladungen und auch Dankesschreiben personalisieren.

- Bei externen KI-Tools Daten soweit wie möglich anonymisieren oder pseudonymisieren, z. B. Platzhalter statt Klarnamen verwenden und erst im finalen Schritt personalisieren. Verträge nach Auftragsverarbeitungvereinbarung prüfen.
- **Nur sinnvolle Personalisierung einsetzen:** Datenpunkte nutzen, die dem Empfänger einen Mehrwert oder persönliche Ansprache geben.
- **Qualitätskontrolle:** Generierte Schreiben von einem Menschen kurz gegenlesen lassen, zumindest stichprobenartig.
- **Transparenz nach außen:** Bekannt machen, dass personalisierte Inhalte erstellt werden.
- **Opt-out respektieren:** Falls jemand keine personalisierten Mails wünscht, Abbestellmöglichkeiten implementieren.

Use Case 4: Automatische Fachbesucher-Prüfung

Szenario

Es soll sichergestellt sein, dass nur qualifiziertes Fachpublikum Zutritt zu einer Fachtagung erhält. Oft werden zur Überprüfung Branchen-Nachweise bei Anmeldung hochgeladen.

Relevante Fragenstellung

Darf die KI diese Uploads automatisch auswerten und eine Entscheidung über die Qualifikation aussprechen?

Datenschutz & KI Check

Nachweise über fachliche Qualifikation enthalten personenbezogene Daten wie Name, Firma, Adresse und ggf. ein Foto und unterfallen damit dem Datenschutzrecht.

- **Rechtsgrundlage:** Die Überprüfung des Branchen-Nachweises kann als Teil der Vertragserfüllung angesehen werden: Wenn es sich um eine Fachtagung/-event handelt und die Vorlage eines Nachweises auch in den AGB verankert ist, dass ein Nachweis vorzulegen ist, ist die Verarbeitung der Nachweisdaten notwendig, um den Vertrag zu erfüllen.

  Zudem kann auch das berechtigte Interesse des Veranstalters gelten: Es soll sichergestellt sein, dass nur passende Personen erscheinen. Dies ist schließlich auch für das Fachpublikum selbst ein relevantes Kriterium.

- **Automatisierte Entscheidung mit erheblicher Auswirkung:** Ob jemand aufgrund seiner Qualifikation zum Event zugelassen wird oder nicht, hat für den Betroffenen erhebliche Auswirkungen. Auch wenn diese Entscheidung nicht existenziell sein wird, können dadurch berufliche Nachteile entstehen und daher darf eine solche nicht leichtfertig einer KI überlassen werden.

  Zudem sind nach Art. 22 DSGVO Entscheidungen allein durch eine Maschine unzulässig – es sei denn, dass es für den Vertrag erforderlich ist, es eine gesetzliche Erlaubnis gibt oder die Person ausdrücklich eingewilligt hat.

  Die Erforderlichkeit könnte dadurch begründet werden, dass es sich um ein Fachbesucher-Event handelt und ein

Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

gewisser Standard von den Teilnehmenden erwartet wird.

Allerdings muss diese Aufgabe nicht zwangsläufig eine KI übernehmen. Der Einsatz einer KI ist also nicht unbedingt erforderlich, sondern vielmehr komfortabler und effizienter.

Eine gesetzliche Erlaubnis ist in diesem Fall ebenfalls nicht ersichtlich. Eine Einwilligung bei Upload ist kritisch zu betrachten. Auch wenn diese freiwillig ist, kann der Eindruck erweckt werden, dass ohne KI kein Zugang gewährt wird, dass die menschliche Überprüfung länger dauern könnte und so mit Nachteilen verbunden sein könnte.

Um datenschutzrechtlich abgesichert zu sein, ist zu empfehlen, die KI eine Vorprüfung machen zu lassen. Auf Basis dieser Vorauswahl kann dann ein Mitarbeitender die Auswahl zumindest stichprobenartig überprüfen und ggf. korrigieren. Zudem sollte die KI im Zweifelsfall immer den Mitarbeitenden benachrichtigen. So wird ein rein automatisiertes Endurteil vermieden und offensichtliche Fehler lassen sich unverzüglich korrigieren.

- **Transparenz und Datensparsamkeit:** Die Teilnehmenden müssen wissen, dass ihr Dokument von einer KI analysiert wird. Das Upload-Formular sollte dazu einen Hinweis enthalten, wie z. B. : “Die Prüfung Ihres Nachweises erfolgt automatisiert durch ein KI-System.” Auch die Datenschutzerklärung ist entsprechend anzupassen.

  Für den Fall einer Ablehnung sollte es eine Kontaktmöglichkeit geben, um das Ergebnis von einem Menschen überprüfen zu lassen (Review-Prozess). Die DSGVO verlangt bei zulässigen automatisieren Entscheidungen zudem, dass auf Verlangen menschliches Eingreifen möglich sein muss.

  Zu berücksichtigen ist auch, dass der KI-Algorithmus evtl. Dokumente sieht, die mehr Daten enthalten als nötig, wie z.B. das Geburtsdatum auf einem Ausweis. Die KI ist so zu programmieren, dass irrelevante Felder ignoriert und diese Informationen auch nicht gespeichert werden.

  Hier sind schon beim Upload der Dokumente klare Präferenzen zu setzen. So wäre z. B. ein Bestätigungsschreiben vom Arbeitgeber dem Personalausweis vorzuziehen.

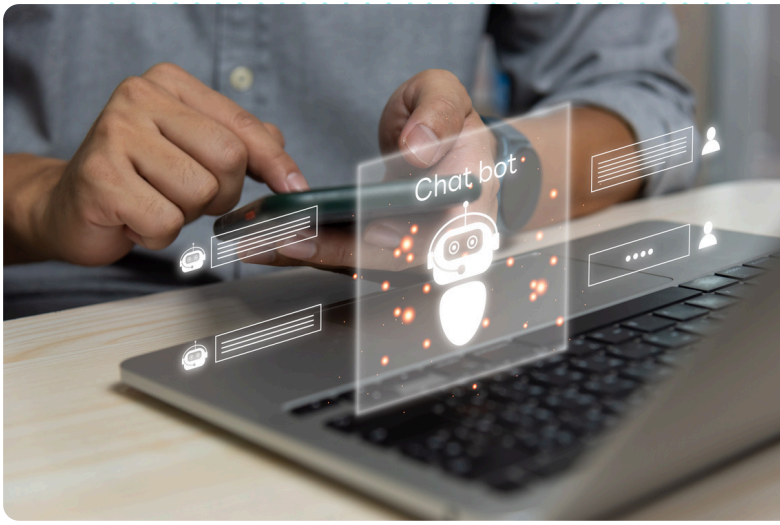
Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

Darüber hinaus sollten die Daten nach der Verifizierung umgehend gelöscht werden. Es handelt sich oft um besonders schützenswerte Daten und deren Speicherung ist nach Verifizierung nicht mehr notwendig.

Fazit & Empfehlung

Ja, eine automatisierte Fachbesucher-Prüfung ist mit Vorsicht machbar.
Datenschutzrechtlich ist dies zulässig, wenn die menschliche Komponente nicht völlig eliminiert wurde und die Transparenzpflichten eingehalten werden.

- **Wenn möglich, halbautomatisch gestalten:** Die KI sortiert vor, ein Mitarbeitender bestätigt im Zweifel oder korrigiert die Entscheidung (Vermeidung einer rein automatisierten Ablehnung).
- **Transparenz:** Klar kommunizieren, dass eine KI die Prüfung vornimmt. Im Ablehnungsfall Möglichkeit zum Widerspruch durch menschlichen Prüfer anbieten.
- **Rechtsgrundlage:** Vertrag/AGB so gestalten, dass Prüfung zulässig ist.
- **Datensparsamkeit:** Nur notwendige Infos prüfen. Teilnehmer auffordern, unnötige Daten ggf. zu schwärzen
- **Speicherbegrenzung:** Nachweisdokumente löschen, sobald Entscheidung erfolgt ist. Nur das Ergebnis der Prüfung vermerken.
- **Genauigkeit & Bias:** Testen und sicherstellen, dass keine Personengruppe benachteiligt wird, z.B. müssen auch ausländische Zertifikate berücksichtigt und nicht pauschal schlechter bewertet werden. Backup-Plan: Falls das KI-System ausfällt oder unsicher ist, muss ein menschlicher Mitarbeitender übernehmen können – auch hierfür braucht es Kapazitäten und Prozesse.



Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

Use Case 5: KI-gestützter Check-in per Gesichtserkennung

Szenario

Der Einlass zu einem Event soll durch Gesichtserkennungs-Technologie automatisiert werden. Teilnehmende laden im Voraus ein Foto von sich hoch, das für die Identifikation am Eingang verwendet wird. Ziel ist es, Warteschlagen zu vermeiden und den Zutritt zu beschleunigen.

Relevante Fragenstellung

Darf für die automatisierte Ticketkontrolle per KI Gesichtserkennung verwendet werden?

Datenschutz & KI Check

Gesichtsbilder sind biometrische Daten und fallen somit unter die besonderen Kategorien personenbezogener Daten.

- **Rechtsgrundlage:** Für eine datenschutzkonforme Nutzung von biometrischen Daten ist eine ausdrückliche Einwilligung der Betroffenen erforderlich.

Aufgrund der Gefahr von Massenüberwachung, durch eine permanente Videoaufzeichnung und dem Erstellen von Bewegungsprofilen ist die Privatsphäre der Teilnehmenden massiv beeinträchtigt.

Eventbetreiber müssen daher genau nachweisen können, wann und wie diese Einwilligung erteilt wurde. Zudem ist vor Einsatz einer solchen Technologie eine sorgfältige Datenschutz-Folgenabschätzung (eine Art Risikobewertung) durchzuführen.

- **KI-Verordnung:** Der Einsatz von Echtzeit-Gesichtserkennung in öffentlich zugänglichen Räumen ist nach der KI-Verordnung grundsätzlich untersagt. Allerdings richtet sich dieses Verbot primär an die zuständigen Strafverfolgungsbehörden.

Für privatwirtschaftliche Eventbetreiber gilt kein generelles Verbot. Die biometrische Echtzeit-Identifizierung fällt regelmäßig in den Hochrisikobereich der KI-Verordnung und unterliegt damit strengen Anforderungen.

Aufgrund der hohen Sensibilität und des erheblichen Missbrauchsrisikos sind besonders strenge technische und organisatorische Maßnahmen erforderlich. Dazu gehören u.a. Verschlüsselung, restriktive Zugriffskonzepte und kurze Speicherfristen.

Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

Darüber hinaus ist eine datenschutzfreundliche Systemarchitektur („Privacy by Design“) eine zwingende Anforderung. Um die Datenhoheit zu bewahren, sollten möglichst lokal betriebene Systeme oder strikt kontrollierte Datenumgebungen eingesetzt werden.

Biometrische Daten sollten zudem zweckgebunden verarbeitet und nach Wegfall des Zwecks – in der Regel unmittelbar nach dem Event – gelöscht werden.

Fazit & Empfehlung

Echtzeit-Gesichtserkennung bei Veranstaltungen ist **unter sehr strengen Voraussetzungen möglich.**

- **Gesichtserkennung nur optional** anbieten und nur mit Einwilligung
- **Löschung** der biometrischen Daten unmittelbar nach dem Einsatzzweck
- **Speicherung von Gesichtsvektoren** anstelle von Rohbildern
- **Sorgfältige Interessensabwägung**, Dokumentation und Datenschutzfolgenabschätzung im Vorfeld durchführen

Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

Use Case 6: Emotionserkennung/Mimik-Tracking

Szenario

Der Veranstalter möchte KI einsetzen, um die Stimmung der Teilnehmer per Mimik-Analyse vor Ort live zu analysieren und damit die Event-Steuerung zu optimieren. So lassen sich z. B. die Reaktionen auf einzelne Veranstaltungen gezielt erfassen oder der richtige Zeitpunkt für eine Pause genauer bestimmen.

Relevante Fragenstellung

Dürfen mithilfe von KI Emotionen von Teilnehmenden analysiert werden?

Datenschutz & KI Check

Datenschutzrechtlich ist die Emotionserkennung per Gesichtsmuster als Verarbeitung von biometrischem Daten und auch gesundheitsbezogener Daten einzustufen. Der DSGVO Anwendungsbereich ist somit eröffnet.

- **Rechtsgrundlage:** Biometrische Daten sind der besonderen Kategorie personenbezogener Daten zuzuordnen. Diese dürfen nur mit ausdrücklicher Einwilligung oder aus speziellen Gründen verarbeitet werden.

  Marktforschung wird nicht als ein solcher spezieller Grund greifen, das wäre unverhältnismäßig. Die Interessen zur Wahrung sensibler Daten übersteigen den Verwertungszweck.

  Eine Verarbeitung mittels Einwilligung wäre in der Theorie datenschutzkonform – unter der Voraussetzung, dass der Veranstaltungsteilnehmer diese auch erteilt.

- **Emotionserkennung mittels KI:** In der Arbeitswelt und im Rahmen der Tätigkeit von Bildungseinrichtungen verbietet die KI-Verordnung Emotionserkennung und stuft diese als verbotenen Praxis ein.

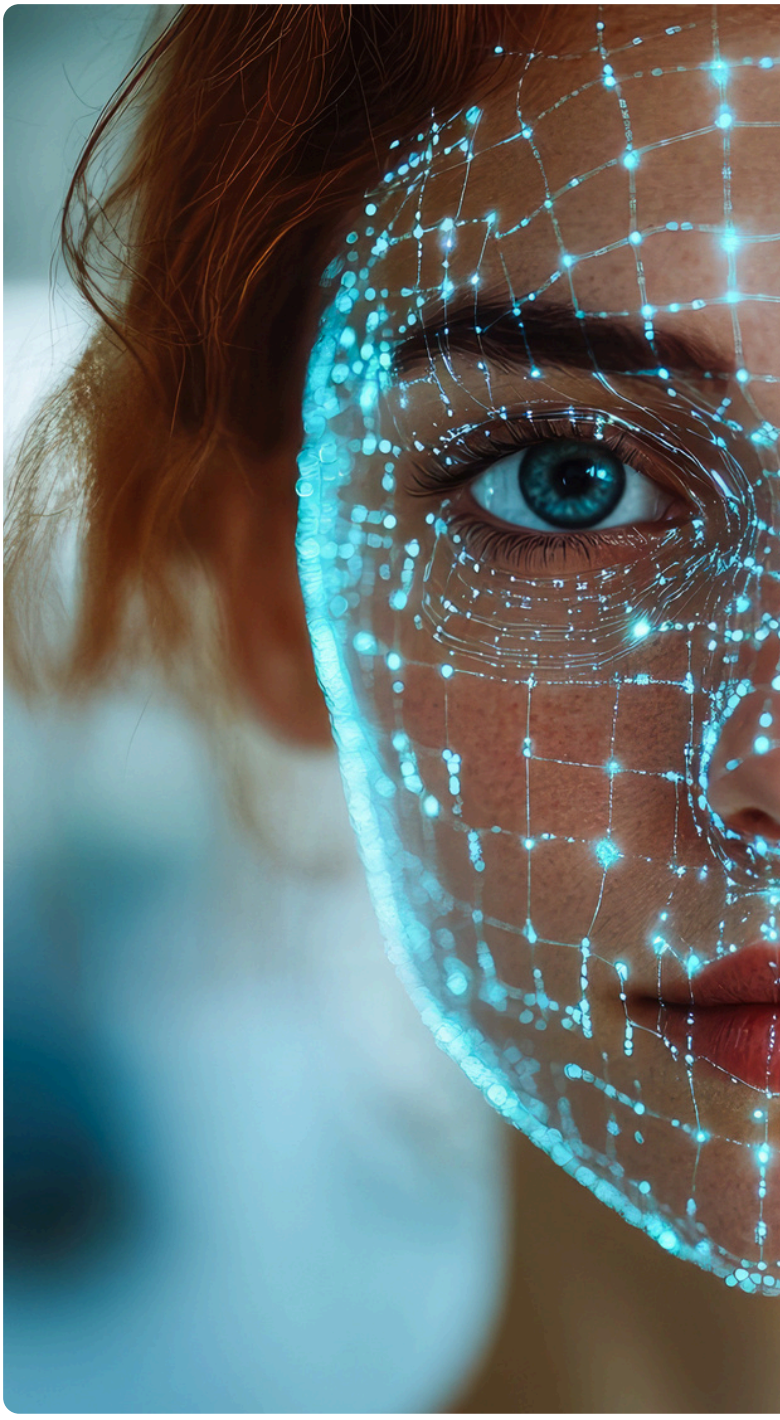
  Öffentliche Veranstaltungen sind in der KI-Verordnung dagegen nicht explizit verboten. Mit Blick auf den Schutzzweck der KI-Verordnung, den Menschen in seinen Rechten zu schützen, ist der Einsatz einer solchen Methodik aber kritisch zu hinterfragen und in der Regel abzulehnen.

Use Cases Automatisierung von Prüf- und Entscheidungsprozessen

Fazit & Empfehlung

Emotionserkennung bei öffentlichen Veranstaltungen ist **per se nicht verboten.** Die Erfassung von Emotionen und / oder von Mimik ist aber äußerst **kritisch zu betrachten** und nur mit ausdrücklicher Einwilligung der Betroffenen durchzuführen.

- **Wenn überhaupt, dann freiwillig und transparent:** Ein möglicher Anwendungsfall wäre die Durchfüh-rung eines Experiments, z. B. um das Potenzial der eingesetzten KI aufzuzeigen. Die Teilnahme darf aus-schließlich auf freiwilliger Basis erfolgen und der Use Case muss ausdrücklich und transparent erläutert werden.



Use Cases rund um Personalisierung & Profiling

Use Case 7: Churn Prediction/No-Show-Prognosen

Szenario

Das Event ist ausgebucht, aber erfahrungsgemäß tauchen 10 - 15 % der angemeldeten Personen am Eventtag nicht auf (No-Shows). Die KI soll nun vorhersagen, welche der angemeldeten Teilnehmenden wahrscheinlich fern-bleiben.

Relevante Fragenstellung

Dürfen Daten von Teilnehmenden für ein Prognosemodell verwendet werden, um mit Hilfe von KI Aussagen zu treffen und zum Beispiel „unsichere“ Kandidaten persönlich an die Teilnahme zu erinnern?

Datenschutz & KI Check

Auf Basis von Daten früherer Events wie z. B. An- und Abmeldung, Ticketart (kostenlos oder -pflichtig) oder No-Shows soll die KI eine “No-Show-Wahrschein-lichkeit" ausrechnen. Hierbei handelt es sich um ein Profiling, also um die automatisierte Auswertung personen-bezogener Daten.

- **Rechtsgrundlage:** Hier besteht ein berechtigtes Interesse, schließlich soll mit dem Profiling die Eventplanung und das Teilnehmendenerlebnis optimiert werden. Dazu gehört z. B. die Anpassung des Catering oder die rechtzeitige Einladung von Nachrückern.

  Dieses Interesse ist gegen das Interesse der Teilnehmenden abzuwägen, durch diese Vorhersagen keine Nachteile zu erhalten, wie z.B. nicht von der Gästeliste gestrichen zu werden.

  Solange also die KI oder ein KI-Agent für Erinnerungs-E-Mails verwendet wird, greift die Rechtsgrundlage des berech-tigten Interesse. Ist es dagegen das Ziel, unliebsame Teilnehmer auszuladen, um Platz zu schaffen, fehlt es an einer rechtlichen Grundlage.

  Profiling verlangt zudem ein hohes Maß an Transparenz und darf nicht heimlich stattfinden. Daher ist in der Datenschutz-erklärung explizit zu erwähnen, dass Profiling zu Vorhersagen von Teilnahme-Wahrscheinlichkeiten genutzt wird.

- **Automatisierte Entscheidung:** Die Vor-hersage selbst ist noch keine Entscheidung per se. Wenn allerdings in einem weiteren Schritt anhand von Wahrscheinlichkeiten jemand von der Gästeliste gestrichen wird, handelt es sich hierbei um eine

Use Cases rund um Personalisierung & Profiling

automatische Entscheidung mit erheblicher Auswirkung. Und diese ist ohne Einwilligung oder menschliche Prüfung unwirksam. Oder anders gesagt: Eine KI alleine kann kein rechtskonformes Profiling durchführen. Es muss immer letztendlich ein Mensch entscheiden, wie mit den Informationen umzugehen ist.

- **Datenminimierung & Bias:** Beim Profiling mittels KI ist es zudem entscheidend, welche Daten verwendet werden. Mithilfe eine Datenstrategie ist im Vorfeld festzulegen, welche Faktoren relevant sind. Im weiteren Prozess ist darauf zu achten, auch wirklich nur diese einzusetzen.

  Irrelevante persönliche Daten für ein No-Show, wie z. B. Geschlecht oder Alter, sollten nicht herangezogen werden, um unerwünschte Verzerrungen zu vermeiden. So können Scheinkorrelationen, wie z. B. “Personen unter 25 Jahre sagen öfters ab” entstehen und bestimmte Gruppen würden diskriminiert. Es gilt, nur so viele Daten wie nötig und so wenig wie möglich sowie gar keine sensiblen Daten einfließen zu lassen.

  Zudem sollten die Vorhersagen möglichst anonym gestaltet sein oder zumindest der Trainingsprozess mit pseudonymisierten Daten erfolgen.

Fazit & Empfehlung

Ja, ein KI-gestützter No-Show-Prophet ist datenschutzrechtlich machbar, sofern er verantwortungsvoll eingesetzt wird. Er steigert Effizienz und Betreuung, darf aber weder diskriminieren noch stigmatisieren. Rückfragen sind zulässig, der Entzug von Zugangsrechten nicht.

- **Nur relevante Daten** wie z. B. Anmeldezeitpunkt oder frühere Event-Historie nutzen. Keine potenziell diskriminierenden oder irrelevanten Merkmale einfließen lassen.
- **Interne Dokumentation,** warum dieses Profiling von berechtigtem Interesse gedeckt ist (Optimierung, Planung) und Darlegung, dass die Betroffenenrechte gewahrt bleiben.
- **In der Datenschutzerklärung ergänzen,** dass Profiling zu Vorhersagen von Teilnahme-Wahrscheinlichkeiten genutzt wird.
- **Kein vollautomatisches Aussortieren.** KI-Vorhersagen nur als Entscheidungshilfe für Mitarbeitende, nicht als endgültiges Urteil pro/contra Teilnehmenden.
- **Auf Datenqualität achten:** Nur verlässliche Daten nutzen.
- **Pseudonymisierte Daten** für die Modellierung, z.B.Teilnehmer-ID statt Namen nutzen.

Use Cases rund um Personalisierung & Profiling

Use Case 8: Zusammenfassung von Teilnehmendenprofilen & KI-generiertem Markentingtext

Szenario

Es wurden im Rahmen einer Veranstaltung diverse Daten gesammelt, um von jedem Teilnehmenden eine kurze Profil-Zusammenfassung zu erstellen. So sollen z. B. Ausstellende oder Sponsoren einen Überblick erhalten, wer kommt. Oder den Teilnehmenden selbst sollen personalisierte Networking Vorschläge unterbreitet werden.

Relevante Fragenstellung

Darf eine KI aus Teilnehmerprofilen kleine Texte generieren, die dann etwa im Networking-Portal oder in Ausstellerunterlagen auftauchen?

Datenschutz & KI Check

Eine Profil-Zusammenfassung ist immer personenbezogen und enthält Daten, um eine Person zu identifizieren oder zu beschreiben. Neben der personenbezogenen Datenverarbeitung ist in diesem Szenario die Veröffentlichung der Daten auch rechtlich zu bewerten.

- **Rechtsgrundlage:** Hat der Teilnehmer seine Daten im Rahmen der Registrierung selbst angegeben und dient deren Verarbeitung dem Zweck, Networking zu ermöglichen, erfolgt die Nutzung grundsätzlich im Einklang mit dem zugrunde liegenden Vertragszweck. Das Networking ist Teil der gebuchten Eventleistung. Idealerweise stimmen die Teilnehmer dem Nutzungszweck in den Teilnehmendenbedingungen zu, wie z. B. „ihr Profil ist für andere Teilnehmenden/Ausstellenden sichtbar“.

  Die Profile können auch von einer KI generiert werden, solange die KI nur diese Datensätze benutzt. Besonders kritisch ist hier die Anreicherung von Profilen mit externen Daten, wie z. B. aus einem LinkedIn-Profil, zu bewerten. Nur bei einer ausdrücklichen und transparenten Einwilligung, zum Beispiel via Optin-Checkbox (“Ich bin damit einverstanden, dass mein Profil für das Networking automatisiert um öffentlich zugängliche Informationen aus meinen LinkedIn-Profil ergänzt wird.”) liegt eine Rechtsgrundlage vor. Diese Konstellation kann aber auch über die Rechtsgrundlage des berechtigten Interesse gelöst werden. So kann argumentiert werden, dass Teilnehmende ein berechtigtes Interesse an einem möglichst vollständigen Networking-Profil haben. Dazu dürfen nur Daten aus öffentlich zugänglichen Profilen sowie aus rein beruflichem Kontext herangezogen werden.

Use Cases rund um Personalisierung & Profiling

Zudem müssen die Teilnehmer zwingend in der Datenschutzerklärung oder durch eine gesonderte E-Mail darüber informiert werden, aus welchen konkreten Quellen die KI zieht und welche Datenkategorien betroffen sind. Ebenso kritisch zu betrachten ist in diesem Szenario die Weitergabe der Profile an Dritte, wie den Ausstellenden oder Sponsoren. Die DSVGO verlangt auch hier eine Rechtsgrundlage. Eine Einwilligung kann im Registrierungsprozess eingeholt werden. Ohne eine solche Einwilligung fehlt es an einer Rechtsgrundlage. Diese lässt sich nicht aus dem Vertrag oder aus dem berechtigten Interesse ableiten.

- **Automatisierte Entscheidungen:** Der Einsatz von KI ist grundsätzlich möglich, insbesondere dann, wenn die KI nur sprachlich einen Text generiert und nicht über die Person entscheidet. Somit hat dies keine erheblichen Auswirkungen auf die Daten. Hinter dem Networking steht der gewollte Zweck des Verbindens.

- **Transparenz und Inhaltliche Richtigkeit:** Solange die KI im Hintergrund arbeitet, ist hier auch keine Kommunikation über die Verwendung verpflichtend. Beim Einsatz von KI sind die generierten Profiltexte zumindest stichprobenartig zu kontrollieren, um zu vermeiden, dass die KI falsche oder auch unangemessen Sachen formuliert.

Fazit & Empfehlung

Liegt eine Einwilligung vor oder ist die **Profil-Zusammenfassung Teil des Event-Services,** ist dies **rechtlich unproblematisch.** Erfolgt die Verarbeitung im Hintergrund und auf Basis freigegebener Daten, ist sie datenschutzkonform.

- **Rechtsgrundlage:** Sicherstellen, dass Teilnehmende wissen, welche Profildaten sichtbar sind. Einwilligungen einholen, insbesondere für die Weitergabe an Sponsoren.

- **Datengrundlage begrenzen:** Nur vom Teilnehmenden angegebene Daten nutzen. Externe Informationen ohne Rechtsgrundlage nicht verwenden.

- **Keine freien KI-Recherchen:** Keine zusätzlichen Internetdaten nutzen. KI nur zur Formulierung, nicht zur Recherche einsetzen.

- **Review-Prozess:** KI-generierte Profile durch Menschen prüfen oder stichprobenartig freigeben.

- **Zweckbindung beachten:** Profile nur für Networking/Marketing im Event-Kontext oder für vereinbarte Zwecke nutzen.

- **Löschung nach Zweck:** Profile nach dem Event löschen oder transparent über Speicherfristen informieren.

Use Cases rund um Marketing & Content Creation

Use Case 9: KI-generierte Texte und Bilder für Event-Marketing

Szenario

Jedes Event braucht Werbung und Promotion. Die KI soll dabei unterstützen, Texte und Bilder für Flyer und Social-Media zu erstellen. Auch der CEO soll als Avatar Werbung machen.

Relevante Fragenstellung

Darf das Marketing-Material mit KI generiert und veröffentlicht werden?

Datenschutz & KI Check

Bei der Einordnung, ob der Anwendungsbereich der DSGVO eröffnet ist, ist zu differenzieren: Bei rein fiktiven Inhalten, Texten und Grafiken ohne Personenbezug, werden keine personenbezogenen Daten verarbeitet und der Anwendungsbereich ist nicht eröffnet.

- **Rechtsgrundlage:** Basiert der KI-generierte Inhalt auf einer Vorlage mit personenbezogenen Daten, wie zum Beispiel Fotos von einem vorausgegangenen Event, kann eine Person identifiziert werden. Die Person muss also der Veröffentlichung zustimmen und einwilligen. Ohne eine solche Einwilligung handelt es sich um einen Datenschutzverstoß.

  Ein Avatar mit generischer KI-Stimme und Gesicht ist dagegen datenschutzrechtlich unbedenklich.

- **KI und Urheberrecht:** Rein KI-generierte Inhalte unterfallen zumindest in Deutschland, nicht dem klassischen Urheberschutz. Er greift erst dann, wenn der generierte Inhalt durch einen Menschen nachbearbeitet wird.

  Bei der Veröffentlichung von rein KI-generierten Inhalten sollte daher das Bewusstsein vorhanden sein, dass diese rechtlich nicht geschützt sind und von Dritten beliebig anderweitig verwendet werden können. Beinhalten KI-generierte Inhalte dagegen urheberrechtlich oder auch markenrechtliche geschützte Inhalte, wie zum Beispiel das firmeneigene Logo oder das Logo eines Kooperationspartners, ist die Verwendung der Daten zu prüfen und vertraglich abzusichern.

  Zudem ist zu prüfen, ob die KI das richtige Logo verwendet – und ob sie das Logo auch richtig und nicht verzerrt oder abgewandelt darstellt.

- **Transparenz:** Die KI-Verordnung sieht keine pauschale Kennzeichnungspflicht für KI-generierte Inhalte vor.

Eine Transparenzpflicht besteht nur dann, wenn Inhalte künstlich erzeugt oder manipuliert wurden und für Dritte nicht erkennbar ist, dass es sich um KI-generiertes Material handelt.

Ist für den durchschnittlichen Betrachter offensichtlich, dass der Inhalt künstlich erstellt wurde, kann eine gesonderte Kennzeichnung entbehrlich sein. Entscheidend ist somit nicht allein die Veröffentlichung, sondern ob ohne Hinweis eine Irreführungs- oder Täuschungsgefahr besteht.

- **Deepfakes:** Bei Deepfakes handelt es sich um KI-generierte oder manipulierte Videoinhalte, die reale Personen täuschend echt darstellen oder imitieren. Gerade wegen ihres hohen Missbrauchs- und Manipulationspotenzials bergen sie erhebliche Risiken: Sie können zur Desinformation, Rufschädigung oder gezielten Täuschung eingesetzt werden.

  Deepfakes sind daher nicht grundsätzlich verboten, unterliegen jedoch strengen Anforderungen und Transparenzpflichten: Solche Inhalte müssen laut KI-Verordnung bei Veröffentlichung grundsätzlich **klar als künstlich erzeugt oder manipuliert** gekennzeichnet werden. So kann natürlich auf Basis eines Fotos eines CEO oder eines Prominenten ein Avatar zu Marketingzwecken erstellt werden – allerdings nur mit dessen Kenntnis und Zustimmung.

Fehlen Einwilligung und Kennzeichnung, drohen erhebliche rechtliche Konsequenzen. Deepfakes können zudem Persönlichkeitsrechte (insbesondere dem Recht am eigenen Bild) und gegebenenfalls Urheberrechte verletzen.

Zudem ist selbst der legale Einsatz von Deepfakes möglicherweise imageschädigend und nicht für das Unternehmen bzw. deren Marke förderlich.

Fazit & Empfehlung

KI-generierte Texte und Grafiken sind in der Eventbewerbung erlaubt, solange keine personenbezogenen Daten verwendet werden. Andernfalls ist eine ausdrückliche Einwilligung erforderlich.

- **Kennzeichnung von KI-Inhalten:** KI-generierte Inhalte als solche kennzeichnen.
- **Urheberrecht:** KI-Bilder haben keinen klassischen Urheberschutz in Deutschland.
- **Deepfake-Verbot beachten:** Keine Imitation realer Personen ohne Erlaubnis.
- **Fact-Checking bei KI-Texten:** Fakten und Zahlen vor Veröffentlichung prüfen.

Use Cases rund um Marketing & Content Creation

Use Case 10: Vorträge aufzeichnen, transkribieren und zusammenfassen

Szenario

Die Sessions einer Konferenz sollen aufgezeichnet und on-demand bereitgestellt werden. Zusätzlich soll der Vortrag durch ein KI-Tool transkribiert und als Zusammenfassung allen Teilnehmenden im Anschluss zugeschickt werden.

Relevante Fragenstellung

Dürfen Aufzeichnungen von Konferenzen und Personen sowie Zusammenfassungen durch KI bearbeitet werden?

Datenschutz & KI Check

Ein Vortrag beinhaltet zumindest die Stimme des Sprechers und bei einem Video auch ein Bild. Stimme und Bild sind personenbezogene Daten. Bei Fragen aus dem Publikum werden auch deren personenbezogene Daten erfasst, in jedem Fall die Stimme und möglicherweise auch Name und Bild.

- **Rechtsgrundlage:** Bei Referenten und Speakern wird in der Regel die Aufzeichnung und Verarbeitung vertraglich festgelegt und somit ist eine vertragliche Rechtsgrundlage gegeben.

  Bei der Aufzeichnung und Nachbereitung eines Events ist mit Blick auf die Teilnehmenden dagegen mit dem berechtigten Interesse des Veranstalters zu argumentieren. Das berechtige Interesse besteht in der Dokumentation der Veranstaltung, der Bereit-stellung von Inhalten für Teilnehmende sowie der Qualitätssicherung und wirtschaftlichen Verwertung der Inhalte.

  Die Verarbeitung ist zulässig, sofern sie zur Wahrung dieser Interessen erforderlich ist und keine überwiegenden Interessen oder Grundrechte der Betroffenen entgegenstehen. Im Rahmen der Interessenabwägung sprechen insbesondere folgende Faktoren für die Zulässigkeit:

  - Transparente Information bereits bei Registrierung und vor Ort
  - Erwartbarkeit von Aufzeichnungen
  - Fokus der Kameras auf Bühne und Referenten
  - Möglichkeit für Teilnehmende, sich nicht aktiv zu beteiligen (z.B. keine Wortmeldungen)
  - Datensparsame Ausgestaltung

- **Strafrechtlicher Rahmen:** Neben datenschutzrechtlichen Vorgaben sind bei der Aufnahme von Teilnehmenden auch strafrechtliche Aspekte zu beachten, konkret die Verletzung der Vertraulichkeit des Wortes.

  Demnach ist die Aufnahme des nicht öffentlich gesprochenen Wortes ohne Einwilligung strafbar. Bei geschlossenen Veranstaltungen mit einem registrierten Teilnehmerkreis kann nicht ohne Weiteres von "Öffentlichkeit" ausgegangen werden.

  Der Straftatbestand entfällt jedoch, wenn die Aufzeichnung erkennbar erfolgt und sich die Beteiligten bewusst äußern. Entscheidend ist, dass keine heimlichen Aufnahmen stattfinden und die Betroffenen vorab transparent informiert werden.

- **Transkription und Zusammenfassung durch KI:** Mit rechtmäßiger Aufzeichnung ist in der Regel auch die Transkription datenschutzrechtlich abgedeckt. Beim Transkript handelt es sich um eine andere Datenform mit gleichem Inhalt. Als Rechtsgrundlage gilt also das berechtigte Interesse in Form einer effizienten und sauberen Dokumentation im Arbeits- bzw. Eventalltag.

Bei Einsatz von KI kann das berechtige Interesse nur dann als Rechtsgrundlage herangezogen werden, wenn **technisch sichergestellt ist, dass die Daten nicht zweckentfremdet werden.**

Es ist zum einen darauf zu achten, dass bei der Zusammenfassung **keine neuen personenbezogene Schlüsse** gezogen werden. Zum anderen sind **Inhalte zu anonymisieren.** Um den Grundsatz der Datenminimierung zu beachten und das Risiko von Datenmissbrauch zu verringern, bietet es sich an, aus dem Transkript vorab eindeutig personenbezogene Stellen zu streichen.

Bei Nutzung eines KI-Tools, das über externe Plattform betrieben wird, ist sicherzustellen, dass die datenschutzrechtlichen Anforderungen eingehalten werden. Insbesondere ist – sofern der Anbieter als Auftragsverarbeiter tätig wird – ein entsprechender Auftragsverarbeitungsvertrag (AVV) abzuschließen.

Bei internationalen Datentransfers muss zudem exakt geprüft sein, ob der Anbieter tatsächlich unter dem EU-U.S. Data Privacy Framework zertifiziert ist oder ob auf Standard Contractual Clauses (SCCs) zurückgegriffen werden muss.

- **Veröffentlichung:** Bei der Veröffentlichung von Aufzeichnungen ist neben dem Datenschutz auch das Persönlichkeitsrecht (Recht am eigenen Bild) zu beachten. Die Veröffentlichung stellt datenschutzrechtlich eine weitere Verarbeitung dar.

- Als Rechtsgrundlage gilt auch hier das berechtige Interesse des Veranstaltenden, beispielsweise zur Öffentlichkeitsarbeit oder zur wirtschaftlichen Verwertung der Inhalte. Maßgeblich ist dabei insbesondere die Erwartbarkeit der Veröffentlichung, transparente Informationen und eine datensparsame Ausgestaltung der Aufnahmen.

  Zu beachten ist daneben noch das Recht am eigenen Bild. Grundsätzlich dürfen Bildnisse nur mit Einwilligung der abgebildeten Personen veröffentlicht werden. Eine Einwilligung kann jedoch entbehrlich sein, wenn es sich beispielsweise um öffentliche Versammlungen handelt und keine einzelne Person hervorgehoben wird. Wird nur eine inhaltliche Zusammenfassung veröffentlicht, die keine personenbezogenen Daten enthält oder die Daten anonymisiert wurden, liegt keine Verarbeitung personenbezogener Daten vor. In diesem Fall bestehen weder datenschutzrechtliche noch persönlichkeitsrechtliche Beschränkungen hinsichtlich der Veröffentlichung.

Fazit & Empfehlung

Die Aufzeichnung, Transkription und KI-gestützte Zusammenfassung von Konferenzinhalten sind **bei transparenter Gestaltung** und sorgfältiger Interessenabwägung vom berechtigten Interesse des Veranstalters **gedeckt.** Entscheidend sind die Vermeidung heimlicher Aufnahmen, eine datensparsame Umsetzung, eine klare Information der Betroffenen sowie eine rechtssichere Einbindung etwaiger KI-Dienstleister.

- **Vertragliche Regelung:** Mit Referenten/Speakern Vereinbarungen zu Aufzeichnung und Verarbeitung treffen.

- **Datenschutzfreundliche Umsetzung:** Kameras auf die Bühne richten, Publikumsfragen nur per Audio; Teilnehmende in Transkripten anonymisieren („Frage aus dem Publikum“).

- **KI-Tools unter Kontrolle:** Transkription/Zusammenfassung möglichst intern oder in der EU-Cloud; externe Dienste nur mit AVV.

- **Löschung:** Rohaufnahmen zeitnah löschen oder geschützt archivieren; Transkripte nach Erstellung der Zusammenfassung löschen.

- **Betroffenenrechte:** Löschungswünsche ernst nehmen und zeitnah umsetzen.

Management Summary

Die rechtliche Analyse der untersuchten Use Cases zeigt: **Die meisten KI-Anwendungen sind zulässig, erfordern jedoch sorgfältige Compliance-Maßnahmen.**

Die meisten Event-KI-Systeme fallen in die Kategorie "minimales Risiko" und sind ohne aufwändige Zulassungsverfahren nutzbar.

Biometrie bleibt heikel: Gesichtserkennung und biometrische Kategorisierung sind entweder verboten oder mit höchsten Compliance-Anforderungen verbunden – QR-Code und RFID sind die praktikableren Alternativen.

Transparenz ist zentral: Kennzeichnungspflichten für KI-Interaktionen und umfassende Datenschutzinformationen sind durchgängige Anforderungen.

DSGVO und KI-Verordnung ergänzen sich: Beide Regelwerke müssen parallel beachtet werden. Die KI-Verordnung ergänzt den Datenschutz um spezifische, technische Anforderungen.

Compliance ist Wettbewerbsvorteil: Rechtskonforme KI-Implementierung schafft Vertrauen bei Teilnehmenden und vermeidet Sanktionen.

Künstliche Intelligenz bietet der Veranstaltungsbranche **erhebliche Potenziale zur Effizienzsteigerung, Personalisierung und Verbesserung des Teilnehmererlebnisses**. Veranstalter im Eventbereich sollten die Chance nutzen, mit KI zu arbeiten und gleichzeitig in eine robuste Compliance-Struktur investieren.

Die frühzeitige **Einbindung von Datenschutzbeauftragten und Rechtsberatung, die Dokumentation aller KI-Systeme und die transparente Kommunikation mit den Teilnehmenden sind essenziell** für den erfolgreichen und rechts-sicheren Einsatz von künstlicher Intelligenz im Veranstaltungsbereich.

Die regulatorische Landschaft wird sich weiter entwickeln. Veranstalter, die heute die Grundlagen für rechtskonforme KI-Nutzung legen, sind optimal für die Zukunft des digitalen Event-Managements positioniert.

Weitere Informationen rund um den Einsatz von KI in der Eventbranche finden Sie **in diesem Whitepaper.**

Über die Autoren

Christian Schmoll
Fachanwalt für IT-Recht

Christian Schmoll ist der Datenschutz-beauftrage von doo. Er ist Rechtsanwalt und Fachanwalt IT-Recht und berät seit 2005 in den Bereichen IT-Recht, Datenschutz und Compliance. Er ist Certified Information Privacy Professional/Europe (CIPP/E), Certified Information Privacy Manager (CIPM), zertifizierter Datenschutz-beauftragter (TÜV) und ISO 27001 Lead Auditor.

Julia Zeller
Anwältin

Julia Zeller berät als Volljuristin bei Compliance.One zu den rechtlichen Leitplan-ken der Digitalisierung. Ihre Schwerpunkte bilden das IT-Recht, der Datenschutz sowie das Recht der Künstlichen Intelligenz. Neben der strategischen Compliance-Beratung gibt sie ihr Fachwissen als Referentin in Schulungen und Webinaren weiter. Zudem ist sie als Rechts-expertin im Radio tätig, wo sie aktuelle juristische Entwicklungen anschaulich und praxisnah für ein breites Publikum einordnet.

doo SMART EVENT AUTOMATION

LASSEN SIE SICH BERATEN UND
SPRECHEN SIE MIT UNSEREN
EXPERT*INNEN!

doo GmbH
Hultschiner Straße 8, 81677 München
+49 89 24 88 15 35 5
business@doo.net
doo.net