Schieb Report

Ausgabe 2024.25

Eure Daten für die KI? Widerspruch möglich!

Kaum ein Thema ist so heiß diskutiert wie Künstliche Intelligenz (KI). Die funktioniert um so besser, je mehr Informationen sie gefüttert bekommt. Facebook nutzt hier beispielsweise eure Daten. Wenn ihr das nicht wollt: widersprecht!

Widerspruch statt Einwilligung

Anbieter wie Facebook haben eine riesige Menge an Informationen über euch gespeichert. Weil ihr sie ihnen freiwillig gebt. Um anderen Benutzern mitzuteilen, was ihr gerade macht, was euch beschäftigt, wie eure Meinung zu Themen ist. An das Training einer KI habt ihr sicherlich dabei weniger gedacht und diesem Verarbeitungszweck auch nicht zugestimmt. Trotzdem: Facebook will eure Daten dafür nutzen.

Wenn ihr das nicht wollt - und das ist jedem Benutzer frei überlassen - dann nutzt diesen Link, um einen Antrag auf den Ausschluss der Verwendung eurer Informationen für das Training von KI zu stellen.

Einspruch gegen die Verwendung deiner Informationen für KI bei Meta

Du kannst bei Meta gegen die Verwendung deiner in unseren Produkten und Diensten geteilten Informationen für das Trainieren der KI bei Meta Einspruch einlegen. Sende dieses Formular ein, um deine Rechte diesbezüglich auszuüben.

KI bei Meta umfasst die Gesamtheit unserer generativen KI-Features und -Erlebnisse, u. a. Meta AI und die KI-gestützten Creative Tools sowie die Modelle, auf denen diese Funktionen basieren.

Zu den Informationen, die du über die Produkte und Services von Meta geteilt hast, zählt unter anderem Folgendes:
– Beiträge
– Fotos und deren Bildunterschriften
– Nachrichten, die du an eine KI sendest

Wir trainieren unsere KIs nicht mit den Inhalten von Privatnachrichten, die du mit Familienmitgliedern oder Freund*innen austauschst.

Wir prüfen deinen Einspruch gemäß den geltenden Datenschutzgesetzen. Wenn deinem Antrag stattgegeben wird, wird er künftig berücksichtigt.

Möglicherweise verarbeiten wir zur Entwicklung und Verbesserung der KI bei Meta Informationen über dich, selbst wenn du dagegen Einspruch erhebst oder unsere Produkte und Dienste nicht nutzt. Das ist unter

- Damit dieser Link funktioniert, müsst ihr über euer Facebook-Konto angemeldet sein. Nur so funktioniert die Zuordnung zu euren Daten.

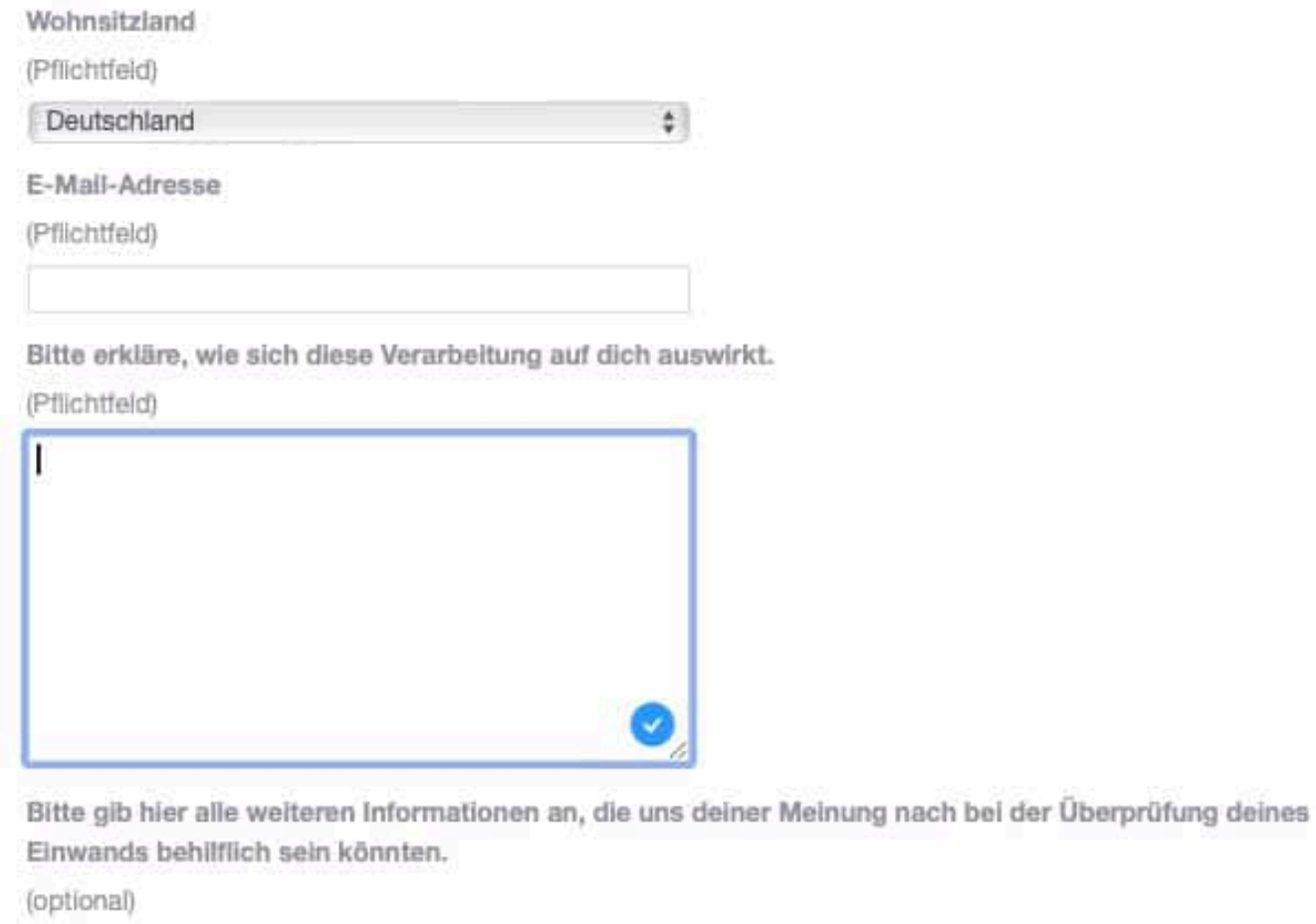
- Wählt das Land aus, in dem ihr euren Wohnsitz habt.

- Gebt eure E-Mail-Adresse an.

- Erklärt, warum ihr der Meinung seid, dass die Verarbeitung eurer Daten Auswirkungen auf euch habt.

- Schickt die Daten durch einen Klick auf **Senden** ab.

- Facebook/Meta prüft die Anfrage und teilt euch die Entscheidung mit.



OptOut? Datensammlung?

Keine Frage, wenn ihr die Verarbeitung eurer Daten nicht möchtet, dann ist dieser Widerspruch ein gangbarer Weg. "Besser als nichts" wird der Eine oder Andere sagen. Das kann aber nicht darüber hinwegtäuschen, dass das Vorgehen Fragen aufwirft:

- Warum müsst ihr Namen und E-Mail-Adresse eingeben, wenn diese doch in eurem Konto (mit dem ihr angemeldet sein müsst) schon vorhanden sind?

- Ihr müsst der Nutzung eurer Daten für eine quasi neue Leistung widersprechen, statt ihr zuzustimmen. OptIn, also die aktive Zustimmung, ist eigentlich Stand der Dinge, nicht OptOut (die Verarbeitung wird durchgeführt, es sei denn, ihr widersprecht).

Die ersten Beschwerden sind bereits unterwegs, dieses Thema bleibt also spannend.

macOS: Software von kleinen Entwicklern installieren

Software ist eines der größeren Einfallstore für Schadsoftware auf einem Mac. Grund genug für Apple, nur die Installation geprüfter Software zuzulassen. Was aber, wenn ihr eine ganz spezifische Anforderung habt von einem kleinen Entwickler und macOS diese verweigert? Es gibt eine Lösung!

Kann eine Prüfung schützen?

Auf den ersten Blick verlassen sich viele Anwender darauf, dass der Virenschutz, der auf nahezu jedem Rechner installiert ist, schon vor allen Gefahren durch Schadsoftware schützt. Das ist aber leider nur die halbe Wahrheit.

Viele Angriffe mit Malware sind heute nicht mehr auf die Masse angelegt, sondern finden gezielt statt. Diese Massenwirkung aber ist es, die die Erkennung durch die meisten Antivirenprogramme erst ermöglicht: Viele Geräte mit ähnlichem, Fehlverhalten und Muster, die vermehrt erkannt werden, begünstigen die Erkennung.

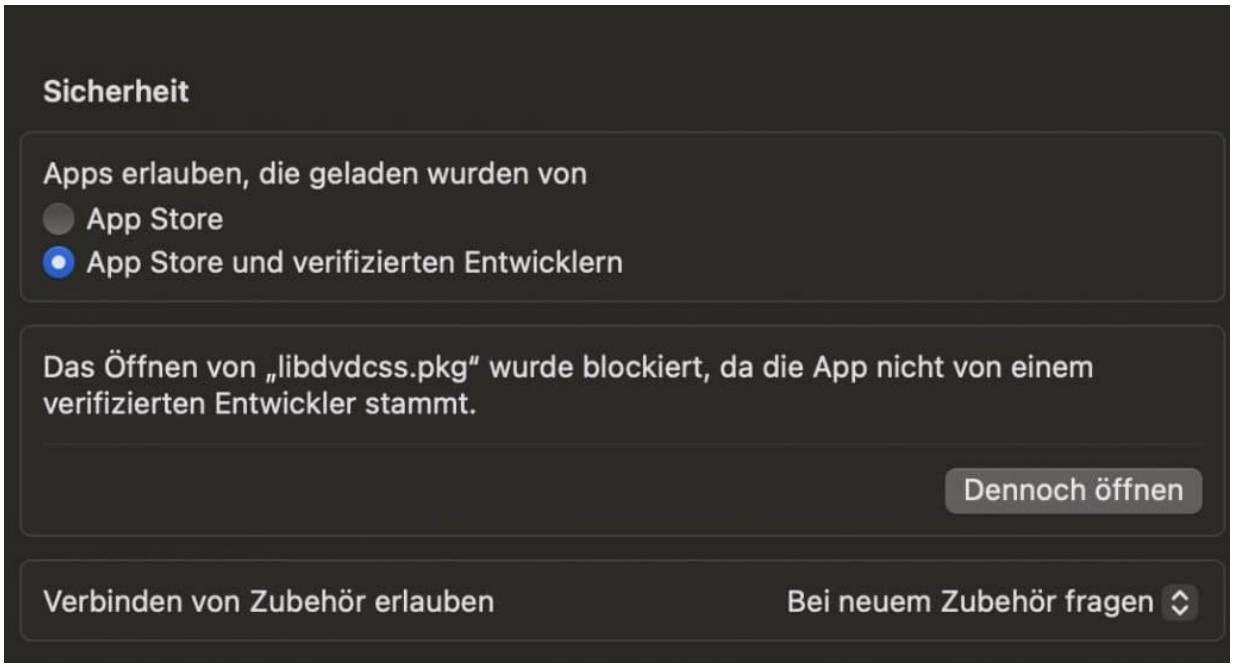
- Das führt dazu, dass viele Hersteller Software bereits vor der Veröffentlichung unter die Lupe nehmen und auf absichtliches oder versehentliches Fehlverhalten untersuchen.

- Nach erfolgreicher Prüfung erhalten diese Programme ein Softwarezertifikat, anhand dessen das Betriebssystem erkennen kann, dass sie geprüft sind.

- Diese Prüfung ist in den meisten Fällen kostenpflichtig. Wer Tausende von Lizenzen verkauft, wird diese Gebühren vielleicht auf sich nehmen. Die kleinen Entwickler aber scheuen diesen Schritt oft.

Installation von Programmen ohne Zertifikat

MacOS lässt in der Standardeinstellung nur die Installation von Programmen zu, die entweder aus dem AppStore kommen.

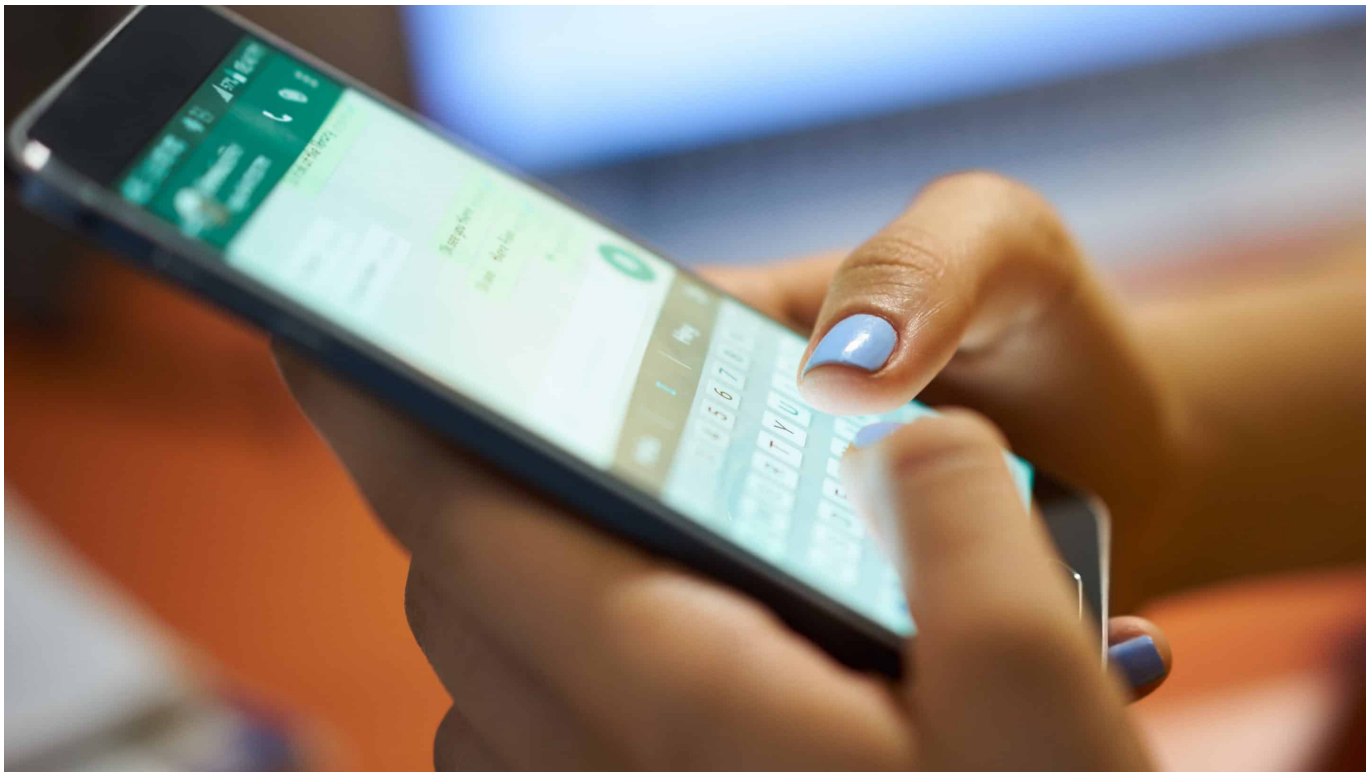


- Ihr könnt dies ein wenig aufweichen, wenn ihr unter **Einstellungen** > **Datenschutz & Sicherheit** > **Sicherheit** "oder von verifizierten Entwicklern" aktiviert.

- Wenn der Entwickler der Software nicht verifiziert ist, dann verweigert macOS die Installation, ohne, dass ihr sie im ersten Schritt freigeben könnt.

- Die Lösung: Ruft den Sicherheits-Dialog wie gerade beschrieben auf. Die gerade gestartete Software erscheint unter den Optionen für **Sicherheit**. Wenn ihr vollkommen sicher seid, dass es sich hier um eine unkritische Software handelt, die keine Schadfunktionen hat, dann klickt auf **Dennoch öffnen**.

EU plant Chatkontrolle für Messenger: Das steckt dahinter



Die EU plant eine sogenannte Chatkontrolle: Bestimmte Inhalte sollen vor dem Versenden mit dem Messenger gecheckt werden. Ein äußerst umstrittenes Vorhaben.

Die Pläne der sogenannten Chatkontrolle sind äußerst umstritten. Viele Politiker in der EU und in den EU-Staaten, aber auch zahlreiche Experten und Bürgerrechtler warnen davor, die Pläne der EU-Kommission umzusetzen, da die Privatsphäre der Menschen bedroht sei. Die geplante Chatkontrolle würde praktisch alle Smartphone-Nutzer in der EU betreffen.

Nach monatelangem Streit in der EU liegt nun ein korrigierter Vorschlag aus Belgien vor, wie eine Chatkontrolle aussehen könnte, um zum einen die gewünschten Ziele zu erreichen und andererseits berechtigte Kritik zu berücksichtigen.

Worum geht es bei der geplanten Chatkontrolle?

Der Hauptgrund für die Einführung der geplanten Maßnahmen ist der Schutz von Kindern vor sexuellem Missbrauch und die Bekämpfung der Verbreitung von Kinderpornografie.

Der Ursprung für die Idee der geplanten Chatkontrolle in der EU lässt sich auf die wachsende Besorgnis über den Missbrauch verschlüsselter Kommunikationsdienste für kriminelle Aktivitäten zurückführen, insbesondere im Zusammenhang mit Kinderpornografie und sexuellem Missbrauch von Kindern.

In den letzten Jahren spielen Instant-Messaging-Dienste wie WhatsApp, Signal und Telegram eine immer größere Rolle in der Online-Kommunikation. Diese Dienste verwenden eine sehr zuverlässige und effektive Ende-zu-Ende-Verschlüsselung, um die Privatsphäre und Sicherheit ihrer Nutzer zu gewährleisten.

Dies bedeutet jedoch auch, dass Strafverfolgungsbehörden nicht auf die Inhalte der Nachrichten zugreifen können, selbst wenn sie einen rechtmäßigen Grund dafür haben.

Das steckt hinter dem Begriff "Going dark"

Dieses Problem wurde von der Europäischen Kommission (EU) als "**going dark**"

bezeichnet, d.h. dass die Strafverfolgungsbehörden zunehmend Schwierigkeiten haben, die Online-Aktivitäten von Kriminellen zu überwachen und zu verfolgen.

Insbesondere im Zusammenhang mit Kinderpornografie und sexuellem Missbrauch von Kindern hat die EU-Kommission festgestellt, dass die derzeitigen Maßnahmen nicht ausreichend sind, um das Problem in den Griff zu bekommen.

Im Juli 2020 veröffentlichte die EU-Kommission eine Strategie zur Bekämpfung sexuellen Missbrauchs von Kindern, in der sie vorschlug, dass Anbieter von Kommunikationsdiensten verpflichtet werden sollten, Maßnahmen zur Erkennung und Meldung von Kinderpornografie und anderen Formen des Missbrauchs zu ergreifen. Dieser Vorschlag schloss auch die Möglichkeit ein, dass die Anbieter verpflichtet werden könnten, ihre verschlüsselten Kommunikationskanäle nach verdächtigen Inhalten zu durchsuchen.

Im Mai 2021 legte die EU-Kommission einen Gesetzesvorschlag vor, der vorsieht, dass Anbieter von Kommunikationsdiensten verpflichtet werden, Technologien zur Erkennung von Kinderpornografie und anderen Formen des Missbrauchs einzusetzen. Dieser Vorschlag sieht auch vor, dass die Anbieter verpflichtet werden können, verdächtige Inhalte zu melden und gegebenenfalls den Zugang zu diesen Inhalten zu sperren.

Der Vorschlag der EU-Kommission hat jedoch auch Bedenken hinsichtlich des Datenschutzes und der Privatsphäre aufgeworfen. Kritiker argumentieren, dass die geplanten Chatkontrollen das Recht auf Privatsphäre und Datenschutz verletzen und potenziell missbraucht werden könnten.

Es gibt aber auch Bedenken hinsichtlich der Wirksamkeit der vorgeschlagenen Technologien zur Erkennung von verdächtigen Inhalten, da diese möglicherweise

nicht in der Lage sind, zwischen legalen und illegalen Inhalten zu unterscheiden, was zu falsch positiven Ergebnissen führen könnte.

Was sind die technischen Aspekte?

Wer mit Chat-Anwendungen wie Whatsapp, Signal, Threema oder Telegram kommuniziert, kann sich bislang darauf verlassen: Niemand kann mitlesen. Die in modernen Chat-Apps verwendete Ende-zu-Ende-Verschlüsselung verhindert das zuverlässig. Selbst Betreiber der Apps wissen nicht, was geschrieben und ausgetauscht wird.

Doch diesen Schutz nutzen auch Kriminelle aus.

Deswegen sollen alle Messenger-Anbieter künftig eine Risikobewertung ihrer Dienste durchführen und in Kategorien wie "hoch", "mittel" und "niedrig" einteilen.

Es gilt als gesichert, dass Dienste, die eine anonyme und verschlüsselte Kommunikation erlauben, nach den Plänen als „hoch“ riskant eingestuft werden. Dazu gehören alle gängigen Messenger wie Whatsapp, Signal, Threema oder Telegram.

Messenger-Dienste mit hohem Risiko sollen dann verpflichtet sein, die zu versendenden Inhalte der Nutzer – noch vor der Verschlüsselung – direkt auf den Geräten der Nutzer zu scannen und illegale Inhalte proaktiv an Behörden zu melden.

Vorteil dieses Verfahrens: Die Verschlüsselung selbst wird nicht direkt geschwächt. In früheren Versionen der angestrebten Regelung wurden Mechanismen vorgesehen, die Verschlüsselung auszuhebeln oder dass Messenger-Betreiber mit Strafverfolgungsbehörden kooperieren müssen. Diese Pläne wurden aber verworfen.

Auch WhatsApp wäre betroffen

Wie soll die Chatkontrolle erfolgen?

Wenn die Pläne der Chatkontrolle umgesetzt werden, würde sich für Nutzer von Messenger-Apps einiges ändern. Die Apps müssten die Inhalte vor der Verschlüsselung und vor dem Absenden auf möglicherweise illegale Inhalte überprüfen. Und das auf den Geräten selbst, also auf den Smartphones der Nutzer. Ein Verfahren, das sich **Client-Side-Scanning** nennt.

Überprüft werden sollen ausschließlich Fotos und Videos. Texte und Audios wären von der geplanten Chatkontrolle nicht betroffen.

Der Vorgang ist allerdings aufwändig. Dazu müssten entweder digitale

Fingerabdrücke, sogenannte Hashcodes (eine Art mathematische Quersumme aus den Pixeln eines Bildes) bereits bekannter pornografischer Inhalte auf allen Geräten der Nutzer gespeichert sein; oder es müsste vor jedem Sendevorgang in einem Messenger ein Abgleich mit Servern erfolgen, die den im Gerät erzeugten Hashcode (Fingerabdruck) überprüfen.

Bei diesem Verfahren würden nicht kriminelle Fotos selbst auf den Geräten der Nutzer landen und es würden auch nicht die Fotos zur Überprüfung an die Server der Messenger-Betreiber geschickt, sondern lediglich ein Hashcode. Eine Art digitaler Fingerabdruck. Anhand des Hashcodes lässt sich kein Foto rekonstruieren, es lässt sich lediglich feststellen, ob zwei Fotos identisch sind.

Allerdings sind auch „false positive“-Fälle möglich: In solchen Fällen kämen Menschen unter Verdacht, weil ihre Fotos möglicherweise nur aus mathematischer Sicht eine gewisse Ähnlichkeit zu bekannten kriminellen Fotos aufweisen. Sie würden dann den Behörden gemeldet und müssten sich erklären.

Was Kritiker befürchten

Kritiker argumentieren, das würde nicht nur die Privatsphäre schwächen, sondern stelle auch ein Sicherheitsrisiko dar. Denn es ist denkbar, dass Cyberbetrüger genau diesen Mechanismus ausnutzen, um Daten abzugreifen oder Smartphones zu Spionen umfunktionieren.

Außerdem drohe eine anlasslose Massenüberwachung, sagen Kritiker. Denn jeder stehe jederzeit unter dem potenziellen Verdacht – und zwar beim Absenden jeder einzelnen Nachricht, die Fotos oder Videos enthält – kriminelle Inhalte zu verteilen. Außerdem würde die Ende-zu-Ende-Verschlüsselung geschwächt oder sogar aufgehoben, da die Inhalte vor der Verschlüsselung gescannt werden

müssen

Das Online-Zugangsgesetz 2.0 ist da: Die digitale Verwaltung lässt weiter auf sich warten

Bund und Länder haben sich beim wichtigen Online-Zugangsgesetz 2.0 auf Kompromisse verständigt – zum Schaden aller Bürger. Auch in den nächsten Jahren bekommen wird keine komplett digitale Verwaltung.

Beamte lassen sich gerne sperrige Begriffe einfallen. Und weil so viele Beamte im Bundestag sitzen, haben auch viele Vorschriften und Gesetze merkwürdige Namen.

Rentenversicherungsbeitragsüberleitungsverordnung zum Beispiel.

Oder, noch trauriger: **Online-Zugangsgesetz**.

Als Bürger kann man damit nichts anfangen. Doch dieses Gesetz ist wichtig, es soll uns nämliche digitale Behörden bringen – und lästige Behördengänge ersparen.

Immer noch gibt es viel zu viele Faxgeräte in Behörden

Onlinezugangsgesetz 2.0

Das neue Onlinezugangsgesetz 2.0 sollte eigentlich strukturelle Hindernisse der Verwaltungsdigitalisierung abbauen.

Allerdings haben sich die Länder durchgesetzt, sodass einheitliche Standards und

eine Ende-zu-Ende-Digitalisierung nach wie vor in weiter Ferne liegen. Beides wären für eine vertrauensvolle und zeitgemäße Digitalisierung der Verwaltung allerdings erforderlich.

Zwar sieht das Gesetz vor, dass der Bund die Standards für Dienstleistungen des Bundes festlegt, doch der Bundesrat hat die Regelung ausgehebelt – und damit das Gesetz geschwächt.

Nun hat der IT-Planungsrat, ein Gremium der Länder, aktives Mitspracherecht und muss den Standards "de facto einstimmig" zustimmen. Außerdem können die Länder von den Vorgaben des Bundes zur Ende-zu-Ende-Digitalisierung abweichen, da eine sogenannte "Ausstiegsklausel" eingefügt wurde.

Experten befürchten, dass dies den Fortschritt der Verwaltungsdigitalisierung weiter verzögern könnte.

Symbolbild für das Tempo bei der Digitalisierung der deutschen Verwaltung

Bislang Komplettversagung bei Bund und Ländern

Doch schauen wir genauer drauf: Jetzt kommt also – nach langem Streit – doch nochmal das sogenannte Online-Zugangsgesetz in den Bundesrat. Wir wissen: es soll die digitale Verwaltung bei uns in Deutschland voranbringen. Wie genau?

Bislang muss man leider von einem Komplettversagen sprechen. Eigentlich sollten bis Ende 2022 bereits 575 Verwaltungsleistungen von Bund, Ländern und Kommunen digitalisiert worden sein. Doch die Verwaltung hat gerade mal 25% geschafft.

Deshalb ist das OZG 2.0 so wichtig, damit das längst überfällige Versprechen,

dass wir uns viele Behördengänge sparen können, endlich eingelöst wird.

Kern des OZG 2.0, das ein Prestigeobjekt der Ampel ist, ist ein einklagbarer Rechtsanspruch auf digitale Leistungen des Bundes, der von 2029 an auf die Mehrzahl der Verwaltungsakte greifen soll.

Das vielleicht Wichtigste ist ein einheitliches digitales Bürgerkonto, das überall gelten soll. Eine Art Online-Ausweis für alle digitalen Behördengänge.

Damit soll man Anträge stellen können, aber auch den Personalausweis komplett digital beantragen oder Widersprüche einreichen. Dazu verwendet man dann den Personalausweis. Moderne Personalausweise haben eine Online-Ausweisfunktion (eID). Damit soll man sich künftig bei der BundID anmelden können.

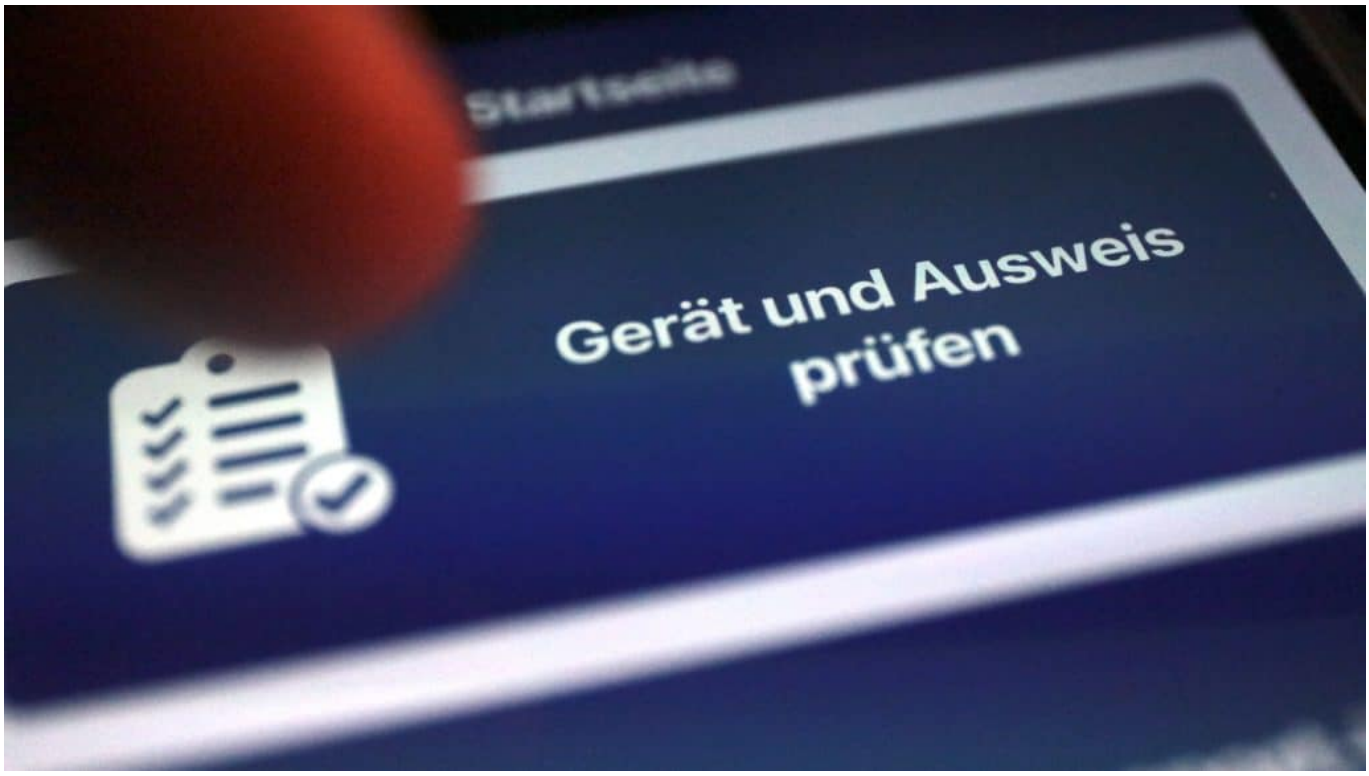
Streit zwischen Bund und Ländern hat geschadet

Das Thema hat ja lange schon für Streit gesorgt zwischen Bund und Ländern.

Einige Bundesländer, darunter NRW, haben eine eigene, landesweite ID-Lösung. NRW hat schon früh zugestimmt, diese zugunsten einer einheitlichen bundesweiten Lösung aufzugeben.

Andere Bundesländer wie Bayern oder Baden-Württemberg haben sich anfangs gesträubt; müssen aber jetzt in den nächsten Jahren auf die BundesID umstellen.

Ein weiterer Konflikt lag bei den Kompetenzen: Der Bund wollte verstärkt eine Führungsrolle übernehmen, er will Standards vorschreiben können. Das ist auch absolut sinnvoll, denn es braucht dringend eine Vereinheitlichung bei Datenformaten und Datenaustausch; es gibt ein viel zu großes Durcheinander.



In NRW soll die Verwaltung komplett auf die BundID umstellen

Viele Amtsgänge lassen sich künftig digital erledigen

Aber was ändert sich für Bürger noch konkret, wenn die digitale Verwaltung möglicherweise mal Tempo aufnimmt (langsamer geht ja kaum)? Wie sehen "Amtsgänge" dann aus, was dürfte für mich deutlich bequemer werden? Was könnte da alles noch gehen?

Das wichtigste ist: Einheitle BundID, egal ob ich es mit einer Kommune, dem Land (etwas bei Steuerfragen) oder dem Bund zu tun habe. Künftig haben wir Bürger auf alles mit dem Personalausweis Zugriff.

Da alle relevanten Daten in der BundID gespeichert sind, müssen sie nicht x-mal eingegeben werden. Die Daten müssten nur noch freigegeben werden.

Mögliche Anwendungsfälle sind die Beantragung von Personalausweis, Reisepass, Führerschein, Geburtsurkunden, Eheschließungen, Wohngeld, BAföG, Elterngeld, KFZ-Zulassung und -Ummeldung, Ummeldung des Wohnsitzes, Gewerbeanmeldung und vieles mehr.

Alles bequem online machbar. In anderen Ländern längst Wirklichkeit. Hier in Deutschland klingt es wie Science-fiction.

Digitale Verwaltung und Datenschutz

Nicht alle Menschen finden diesen Gedanken so toll, so etwas digital zu erledigen. Sorgen drehen sich oft um Datenschutz - gerade, wenn es um sensible Sachen auf dem Amt geht. Wie wird dem bislang Rechnung getragen?

Die Sorgen sind berechtigt, denn Behörden verarbeiten sensible persönliche Daten. Deshalb hängt die Latte hoch: Die Verantwortlichen müssen hohen Aufwand betreiben, damit die Datensicherheit auch wirklich gewährt wird.

Die gute Nachricht: Behörden sind verpflichtet, transparent zu machen, welche Daten zu welchem Zweck verarbeitet werden. Die Behörden sind außerdem angehalten, nur wirklich notwendige Daten zu erheben, zu erfassen und speichern.

Bürger haben das Recht, Auskunft über ihre gespeicherten Daten zu erhalten und können die Berichtigung oder Löschung ihrer Daten verlangen. Für den Zugang zu digitalen Verwaltungsdiensten werden sichere Identifikations- und Authentifizierungsmethoden verwendet, wie der elektronische Personalausweis (eID) oder spezielle Authentifizierungs-Apps. Diese Methoden stellen sicher, dass nur berechtigte Personen auf die Daten zugreifen können.

Sensible Daten werden – so sieht es das OZG 2.0 vor – durch moderne Verschlüsselungstechniken geschützt, sowohl während der Übertragung als auch bei der Speicherung. Behörden müssen in robuste IT-Sicherheitsinfrastrukturen investieren, um Daten vor unbefugtem Zugriff und Cyberangriffen zu schützen.

Rathäuser bislang nicht so gut aufgestellt

Das Land NRW hat ein „Serviceportal.NRW“ eingeführt. Hier wurde bereits zum 31.05.2024 das „Servicekonto NRW“ durch die BundID ersetzt. Löblich.

Auf kommunaler Ebene sieht es sehr unterschiedlich aus. Einige Kommunen bieten bereits zahlreiche Behördengänge online an, beispielsweise die Beantragung von Meldebescheinigungen, die Anmeldung von Wohnsitzen, die Beantragung von Führungszeugnissen und die Terminvereinbarung für persönliche Besuche im Rathaus. Als besonders fortschrittlich gelten Dortmund, Düsseldorf und Köln.

Das ist aber genau das Problem: Einige Städte schreiten voran, andere sind digital technisch noch in der Steinzeit. Das soll das OZG 2.0 ändern. Die Bürger können bis Ende 2024 große Fortschritte erwarten, bis Ende 2025 sollten alle Verwaltungsleistungen digital sein.

Ein ähnliches Versprechen gab es schon einmal. Jetzt haben die Bürger aber sogar Anspruch darauf.