Verwaltungsmodernisierung im Zeitalter der KI

Den Zielkonflikt zwischen nutzerfreundlicher Automatisierung und DSGVO/EU AI Act in der österreichischen Verwaltung auflösen

Forschungsfrage: Wie lässt sich der Zielkonflikt zwischen nutzerfreundlicher KI-Automatisierung und den Anforderungen von DSGVO und EU AI Act in der österreichischen Verwaltungspraxis auflösen?

Thomas Zojer
Politische Analyse
24. Juni 2026

Inhaltsverzeichnis

1 Einleitung

Die österreichische öffentliche Verwaltung gilt im europäischen Vergleich als digitaler Vorreiter. Der eGovernment MONITOR 2024 weist für Österreich eine Nutzungsquote digitaler Verwaltungsservices von 75 Prozent aus, und 94 Prozent der Nutzerinnen und Nutzer wollen diese Angebote weiterhin online in Anspruch nehmen (Initiative D21 & Kantar, 2024). Diese Spitzenposition ist jedoch kein Ruhekissen, sondern ein Sprungbrett: Mit dem Reifegrad künstlicher Intelligenz (KI) verschiebt sich der Anspruch von der bloßen Digitalisierung bestehender Abläufe hin zu einer qualitativen Neugestaltung von Services. Die OECD dokumentiert quer über Kerngovernment-Funktionen rund 200 Anwendungsfälle und sieht den größten Nutzen in der Gestaltung und Erbringung öffentlicher Leistungen (OECD, 2024). Konkret stehen proaktive bzw. antraglose Verwaltung, dialogfähige Chatbots und personalisierte Services im Zentrum der Erwartung an eine nutzerfreundliche Verwaltung von morgen.

Gleichzeitig agiert die Verwaltung nicht im rechtsfreien Raum, sondern in einem dichter werdenden Regulierungsgefüge. Zwei Regime prägen den Handlungsspielraum besonders: die Datenschutz-Grundverordnung (Verordnung [EU] 2016/679) mit ihren Prinzipien der Datenminimierung, der Zweckbindung und dem Schutz vor rein automatisierten Einzelentscheidungen, sowie die neue KI-Verordnung der Europäischen Union (Verordnung [EU] 2024/1689), die KI-Systeme risikobasiert reguliert und viele Verwaltungsanwendungen als hochriskant einstuft. Damit entsteht ein scheinbar paradoxes Spannungsfeld: Je nutzerfreundlicher, datengetriebener und automatisierter ein Service wird, desto stärker berührt er genau jene Schutzgüter, die DSGVO und AI Act absichern sollen.

Der vorliegende Essay verfolgt die These, dass dieser Zielkonflikt real, aber nicht binär ist. Er lässt sich nicht durch den Verzicht auf eine der beiden Seiten – Nutzerfreundlichkeit oder Rechtskonformität – auflösen, sondern durch eine substanzielle, in die Servicegestaltung eingebettete Governance teilweise versöhnen. *Untersucht werden drei Hypothesen: (H1) nutzerfreundliche KI-Automatisierung kollidiert strukturell mit Datenminimierung, Zweckbindung und Artikel 22 DSGVO; (H2) der EU AI Act stuft zentrale Verwaltungs-KI als Hochrisiko ein und erzeugt zusätzliche Compliance-Lasten; (H3) der Konflikt ist über Governance-Mechanismen – Transparenz, wirksame menschliche Aufsicht und Privacy-by-Design – teilweise auflösbar.*

Der Beitrag ist wie folgt aufgebaut: Kapitel 2 entwickelt den theoretischen Hintergrund zu Verwaltungsmodernisierung, KI im öffentlichen Sektor und dem regulatorischen Rahmen. Kapitel 3 prüft die drei Hypothesen entlang der Bereiche Nutzerfreundlichkeit, Recht und

Governance. Kapitel 4 diskutiert zwei konkrete Zielkonflikte, Limitationen und die Übertragbarkeit auf die österreichische Verwaltungspraxis. Kapitel 5 zieht ein Fazit und formuliert konkrete Handlungsempfehlungen.

Die Relevanz dieser Frage für Verwaltung und Politik ist unmittelbar praktischer Natur. Erstens entscheidet die Auflösung des Zielkonflikts darüber, ob die Effizienz- und Servicegewinne der KI überhaupt rechtssicher gehoben werden können. Zweitens bindet eine fehlgeleitete Umsetzung knappe Personal- und Budgetressourcen in Doppelprüfungen, Gutachten und Nachbesserungen. Drittens steht die Legitimität des Verwaltungshandelns auf dem Spiel, weil intransparente oder fehlerhafte Automatisierung verwaltungsgerichtlich angreifbar ist und das mühsam aufgebaute Vertrauen rasch zerstören kann. Für die politische Steuerungsebene ist der Konflikt damit kein technisches Detail, sondern eine Frage der Handlungsfähigkeit des Staates im digitalen Zeitalter.

Begrifflich versteht dieser Beitrag unter nutzerfreundlicher KI-Automatisierung den Einsatz datengetriebener, lernender oder regelbasierter Systeme, die den Aufwand der Bürgerinnen und Bürger im Kontakt mit der Verwaltung senken, indem sie Informationen bereitstellen, Anträge vereinfachen, Entscheidungen vorbereiten oder Leistungen proaktiv anstoßen. Der Begriff der Nutzerfreundlichkeit wird dabei nicht auf Bedienkomfort verengt, sondern umfasst Zugänglichkeit, Verständlichkeit, Verlässlichkeit und die Wahrung der Würde im Verfahren. Diese weite Fassung ist bewusst gewählt, weil sie verhindert, dass Datenschutz und Nutzerfreundlichkeit vorschnell als Gegensätze erscheinen.

Methodisch verfolgt der Essay einen analytisch-argumentativen Zugang ohne eigene empirische Erhebung. Er verknüpft die internationale, überwiegend peer-reviewte Forschung zu Akzeptanz, Governance und Recht mit dem österreichischen institutionellen Kontext und leitet daraus eine eigenständige Position ab. Die herangezogene Literatur stützt die Argumentation, ersetzt sie aber nicht; wo die Befundlage dünn ist, wird dies offengelegt. Ziel ist nicht eine erschöpfende juristische Kommentierung der beiden Regelwerke, sondern eine handlungsleitende Einordnung für Entscheidungsträgerinnen und Entscheidungsträger in Verwaltung und Politik.

2 Theoretischer Hintergrund

2.1 Verwaltungsmodernisierung und Nutzerorientierung

Verwaltungsmodernisierung hat sich von einer binnenorientierten Effizienzlogik zu einer ausdrücklich bürgerzentrierten Perspektive verschoben. Dechamps, Simonofski und Burnay (2025) zeigen in einer theoretisch wie empirisch fundierten Typologie, dass „Bürgerzentrierung" kein eindimensionaler Begriff ist, sondern unterschiedliche

Intensitätsstufen umfasst – von der reinen Information über Konsultation bis zur Ko-Produktion von Leistungen. Nutzerfreundlichkeit ist damit mehr als eine ansprechende Oberfläche; sie betrifft die Frage, wie weit der Staat den Aufwand auf Seiten der Bürgerinnen und Bürger reduziert. Die konsequente Weiterentwicklung dieses Gedankens führt zur proaktiven Verwaltung: Leistungen werden nicht mehr auf Antrag, sondern auf Basis vorhandener Daten automatisch angeboten oder gewährt. Genau hier wird KI zum entscheidenden Hebel, weil sie Anspruchsprüfungen, Mustererkennung und personalisierte Ansprache in einem Maßstab ermöglicht, der manuell nicht erreichbar wäre.

Konzeptionell knüpft diese Entwicklung an den Übergang vom New Public Management zu einem neo-weberianischen Staatsverständnis an, in dem Bürgerorientierung und rechtsstaatliche Verlässlichkeit zusammengedacht werden. Das Leitbild der proaktiven, im Idealfall unsichtbaren Verwaltung beschreibt einen Zustand, in dem Leistungen nach dem Once-Only-Prinzip ohne wiederholte Dateneingabe und ohne aktiven Antrag erbracht werden. Dechamps et al. (2025) machen jedoch deutlich, dass höhere Stufen der Bürgerzentrierung nicht automatisch wünschenswert sind, sondern an Bedingungen geknüpft bleiben: Wer Leistungen antizipiert, trifft Annahmen über Lebenslagen, und diese Annahmen können falsch, stigmatisierend oder bevormundend sein. Nutzerfreundlichkeit ist damit kein rein technisches, sondern ein normatives Gestaltungsziel, das ohne Datenschutz- und Grundrechtsbezug nicht zu haben ist (OECD, 2024).

2.2 Künstliche Intelligenz im öffentlichen Sektor

Wirtz, Weyerer und Geyer (2019) systematisieren zehn Anwendungsfelder von KI im öffentlichen Sektor – von der Bürgerkommunikation über Prozessautomatisierung bis zur prädiktiven Analytik – und benennen zugleich den Datenschutz als eine der zentralen Herausforderungen. Aus Akzeptanzsicht ergänzt Savveli, Rigou und Balaskas (2025) das Bild: Ihr systematisches Review von 30 empirischen Studien identifiziert wahrgenommenen Nutzen, einfache Bedienbarkeit, Vertrauen und – als kritischen Gegenpol – wahrgenommenes Risiko als wiederkehrende Determinanten positiver Einstellungen gegenüber KI-gestützten E-Government-Diensten. Damit ist bereits theoretisch angelegt, dass Datenschutzbedenken nicht außerhalb der Nutzerfreundlichkeit stehen, sondern in sie hineinwirken. Kuziemski und Misuraca (2020) warnen schließlich, dass der Einsatz automatisierter Entscheidungsfindung im öffentlichen Sektor bestehende Machtasymmetrien zwischen Staat und Individuum verstärken kann, wenn er nicht in einen geeigneten Bewertungsrahmen eingebettet wird.

Die Bandbreite der Anwendungsfelder reicht von dialogbasierten Bürgerassistenten über die automatisierte Vorprüfung von Anträgen bis zur prädiktiven Ressourcensteuerung (Wirtz et al., 2019). Gerade Chatbots sind ein doppelter Fall: Sie senken Zugangshürden und sind aus

Akzeptanzsicht attraktiv, verarbeiten aber freie Texteingaben, die unkontrolliert personenbezogene und besonders sensible Daten enthalten können. Savveli et al. (2025) ordnen die Akzeptanzfaktoren in mehrere Kategorien ein, darunter wahrgenommener Nutzen, wahrgenommene Bedenken, Vertrauen sowie individuelle und dienstbezogene Merkmale, und zeigen damit, dass Datenschutzbedenken keine Randnotiz, sondern eine eigene Akzeptanzdimension sind. Kuziemski und Misuraca (2020) illustrieren die Schattenseiten an realen Fällen, etwa der algorithmischen Profilierung Arbeitsloser in Polen und automatisierten Entscheidungen im kanadischen Migrationssystem; sie verdeutlichen, dass schlecht eingebettete Automatisierung gerade vulnerable Gruppen trifft und so die Legitimität des Verwaltungshandelns untergräbt.

Österreichs Ausgangslage begünstigt solche Anwendungen, weil eine registerbasierte Verwaltung und eine hohe digitale Durchdringung bereits bestehen (Initiative D21 & Kantar, 2024). Genau diese Datenverfügbarkeit ist aber zweischneidig: Sie macht proaktive, personalisierte Services technisch erst möglich und verschärft zugleich die datenschutzrechtliche Verantwortung, weil die Schwelle zur umfassenden Profilbildung sinkt. Die OECD (2024) hält fest, dass öffentliche Stellen gerade wegen ihrer besonderen Pflichten zu Datenschutz, Transparenz und Gleichbehandlung höhere Anforderungen erfüllen müssen als private Akteure. Die günstige technische Ausgangslage ist somit kein Freibrief, sondern erhöht die Sorgfaltsanforderung.

Begrifflich ist zwischen Entscheidungsunterstützung und Entscheidungsersetzung zu trennen. Solange ein System lediglich Vorschläge liefert, über die ein Mensch substanziell entscheidet, bleibt der Anwendungsbereich des Artikels 22 DSGVO unberührt; erst die faktische Ersetzung menschlicher Entscheidung löst dessen Schutzmechanismen aus (Verordnung [EU] 2016/679). Diese Grenze ist in der Praxis fließend, weil scheinbare Entscheidungsunterstützung bei hoher Befolgungsrate de facto zur Entscheidung wird. Für die Servicegestaltung ist die Einordnung zentral, da sie über die anwendbaren Pflichten und damit über Aufwand und Spielraum entscheidet.

2.3 Der regulatorische Rahmen: DSGVO und EU AI Act

Der rechtliche Rahmen besteht aus zwei sich überlagernden Schichten. Die Datenschutz-Grundverordnung verankert in Artikel 5 die Grundsätze der Datenminimierung und der Zweckbindung sowie in Artikel 22 das grundsätzliche Recht, nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung mit rechtlicher oder ähnlich erheblicher Wirkung unterworfen zu werden (Verordnung [EU] 2016/679). In Österreich konkretisieren die §§ 39 und 41 Datenschutzgesetz die automatisierte Einzelfallentscheidung (Datenschutzgesetz [DSG], BGBl. I Nr. 165/1999 i. d. g. F.). Die KI-Verordnung ergänzt diese

personenbezogene Logik um eine produkt- und risikobezogene: Sie reguliert KI-Systeme nach Risikoklassen und ordnet Anwendungen, die über den Zugang zu wesentlichen privaten und öffentlichen Diensten und Leistungen entscheiden, dem Hochrisiko-Bereich zu (Verordnung [EU] 2024/1689). Beide Regime verfolgen denselben Grundwert – den Schutz der Betroffenen –, setzen ihn aber mit unterschiedlicher Logik um. Die zentrale theoretische Spannung dieses Essays lässt sich so fassen: Die Akzeptanz- und Effizienzlogik der Nutzerorientierung drängt zu mehr Daten, mehr Automatisierung und mehr Antizipation, während die Schutzlogik des Rechts zu weniger Daten, mehr menschlicher Kontrolle und enger Zweckbindung drängt.

Die KI-Verordnung folgt einem abgestuften Risikoansatz: Sie verbietet bestimmte Praktiken, unterwirft Hochrisiko-Systeme strengen Pflichten und belässt es bei geringeren Risiken im Wesentlichen bei Transparenzauflagen (Verordnung [EU] 2024/1689). Ihre Anforderungen werden zeitlich gestaffelt wirksam, wobei für bereits eingesetzte Systeme öffentlicher Stellen verlängerte Übergangsfristen gelten. Entscheidend ist, dass die KI-Verordnung den datenschutzrechtlichen Rahmen nicht ersetzt, sondern ergänzt: Jede Verarbeitung personenbezogener Daten benötigt weiterhin eine Rechtsgrundlage nach Artikel 6 und gegebenenfalls eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO (Verordnung [EU] 2016/679). Daraus ergibt sich eine doppelte Pflichtenlage, deren Kohärenz nicht garantiert ist; Graux et al. (2025) sprechen von erheblicher regulatorischer Komplexität, weil identische Sachverhalte unter beiden Regimen unterschiedlich klassifiziert und beaufsichtigt werden können.

Hervorzuheben ist, dass beide Regelwerke denselben Grundwert verfolgen, den Schutz der von Verwaltungshandeln betroffenen Person, ihn aber aus unterschiedlichen Richtungen adressieren. Die DSGVO setzt am personenbezogenen Datum und an der einzelnen Verarbeitung an, der AI Act am System und seinem Risiko über den gesamten Lebenszyklus. Diese unterschiedliche Anknüpfung erklärt, warum dieselbe Anwendung zugleich als Datenverarbeitung und als Hochrisiko-System reguliert sein kann und warum Abstimmungsbedarf entsteht (Graux et al., 2025). Für die Verwaltungspraxis folgt daraus, dass eine isolierte Betrachtung nur eines Regimes regelmäßig zu kurz greift.

3 Hauptteil

3.1 H1 – Nutzerfreundlichkeit versus Datenschutzprinzipien

Die erste Hypothese behauptet einen strukturellen Konflikt zwischen nutzerfreundlicher KI-Automatisierung und den Kernprinzipien der DSGVO. Dieser Konflikt ist plausibel und lässt sich an der proaktiven Verwaltung exemplarisch zeigen. Proaktive Services beruhen darauf,

Ansprüche automatisch zu erkennen und Leistungen mit minimalem Zutun der Bürgerinnen und Bürger anzubieten. Das erfordert in der Regel die Verknüpfung von Datenbeständen über Verfahrens- und Behördengrenzen hinweg sowie eine fortlaufende Profilbildung, um Bedarfe zu antizipieren. Genau hier entsteht die Reibung mit Artikel 5 DSGVO: Datenminimierung verlangt, nur die für einen konkreten Zweck erforderlichen Daten zu verarbeiten, und Zweckbindung untersagt, einmal erhobene Daten beliebig für neue Zwecke weiterzuverwenden (Verordnung [EU] 2016/679). Die für Personalisierung attraktive Datenfülle steht damit in einem Grundsatzwiderspruch zum Sparsamkeitsgebot.

Hinzu tritt Artikel 22 DSGVO. Sobald eine nutzerfreundliche Automatisierung so weit reicht, dass über einen Leistungsanspruch faktisch ohne menschliches Zutun entschieden wird, gerät sie in den Anwendungsbereich des Verbots ausschließlich automatisierter Einzelentscheidungen mit erheblicher Wirkung. Die österreichischen §§ 39 und 41 DSG setzen diese Grenze im nationalen Recht um (Datenschutzgesetz [DSG], BGBl. I Nr. 165/1999 i. d. g. F.). Suksi (2021) verschärft die Diagnose über den Datenschutz hinaus: Viele klassische Verfahrensgarantien des Verwaltungsverfahrens – Begründungspflicht, Anhörung, Rechtsmittel – seien auf menschliche Sachbearbeitung zugeschnitten und drohten bei vollautomatisierter Bearbeitung leerzulaufen; der nationale Gesetzgeber müsse das Verfahrensrecht entsprechend anpassen. Damit ist der Konflikt nicht nur ein datenschutzrechtlicher, sondern ein rechtsstaatlicher.

Die eigene Bewertung relativiert H1 jedoch in einem entscheidenden Punkt: Datenschutz und Nutzerfreundlichkeit sind keine reinen Gegensätze. Das Akzeptanzmodell von Savveli et al. (2025) zeigt, dass wahrgenommenes Risiko ein zentraler Hemmschuh der Nutzung ist. Wer Datenschutz vernachlässigt, untergräbt damit genau jene Akzeptanz, die nutzerfreundliche Services erzeugen sollen. Auch Dechamps et al. (2025) und der hohe Vertrauensbezug im eGovernment MONITOR 2024 (Initiative D21 & Kantar, 2024) stützen diese Lesart: Vertrauen ist Voraussetzung, nicht bloß Nebenbedingung der Nutzung. H1 ist somit zu bestätigen, aber zu präzisieren – der Konflikt verläuft weniger zwischen „Service" und „Schutz" als zwischen kurzfristiger Datenmaximierung und langfristiger, vertrauensbasierter Nutzungsbereitschaft.

Die Reibung verschärft sich bei besonderen Datenkategorien. Personalisierte Services, die etwa Gesundheits-, Sozial- oder Herkunftsmerkmale berücksichtigen, berühren Artikel 9 DSGVO und damit ein grundsätzliches Verarbeitungsverbot mit engen Ausnahmen (Verordnung [EU] 2016/679). Je feiner ein KI-Service personalisiert, desto eher entsteht ein Profil im datenschutzrechtlichen Sinne und desto näher rückt die Anwendung an die Schwelle des Artikels 22. Suksi (2021) betont zudem, dass die Begründungs- und

Nachvollziehbarkeitspflichten des Verwaltungsverfahrens bei automatisierten Entscheidungen eigens abgesichert werden müssen, weil der klassische, an die handelnde Person gebundene Rechtsschutz andernfalls ins Leere läuft. In Österreich ist diese Absicherung über das Verwaltungsverfahrens- und Datenschutzrecht zu leisten, wobei die Paragrafen 39 und 41 DSG die datenschutzrechtliche Außengrenze markieren (Datenschutzgesetz [DSG], BGBl. I Nr. 165/1999 i. d. g. F.).

Ein praxisnahes Beispiel verdeutlicht die Spannung. Eine antraglose Gewährung familienbezogener Leistungen setzt voraus, dass Geburts-, Melde-, Einkommens- und Beschäftigungsdaten verknüpft und laufend abgeglichen werden. Aus Nutzersicht ist das der Idealfall, denn die Leistung kommt von selbst. Datenschutzrechtlich verlangt derselbe Vorgang jedoch eine klare Rechtsgrundlage, eine enge Zweckbindung und Vorkehrungen gegen eine schleichende Ausweitung der Datennutzung. Der Konflikt ist somit nicht akademisch, sondern entscheidet darüber, ob eine konkrete Serviceidee überhaupt realisierbar ist. H1 ist daher zu bestätigen, jedoch mit der Präzisierung, dass die Lösung in der Gestaltung der Datenflüsse liegt und nicht im Verzicht auf den Service.

Empirisch ist der Konflikt zudem rückgekoppelt: Wahrgenommene Datenschutzrisiken senken die Nutzungsbereitschaft, sodass eine datenschutzvergessene Automatisierung ihre eigenen Akzeptanzgrundlagen untergräbt (Savveli et al., 2025). Kleizen et al. (2023) zeigen ergänzend, dass sich dieses Vertrauen nicht durch bloße Beteuerungen herstellen lässt. Nutzerfreundlichkeit und Datenschutz sind damit weniger Gegenspieler als zwei Bedingungen desselben Ergebnisses, nämlich einer Verwaltung, die digitale Leistungen anbietet, die auch tatsächlich genutzt werden.

3.2 H2 – Der EU AI Act und die Compliance-Last für Verwaltungsservices

Die zweite Hypothese richtet den Blick auf die KI-Verordnung. Da viele Verwaltungsanwendungen über den Zugang zu wesentlichen Leistungen entscheiden, fallen sie in die Hochrisiko-Kategorie und unterliegen damit umfangreichen Pflichten: Risikomanagement, technische Dokumentation, Protokollierung, Transparenz gegenüber Betroffenen, menschliche Aufsicht und Qualitätsanforderungen an die Trainingsdaten (Verordnung [EU] 2024/1689). Diese Pflichten treffen nicht nur die Anbieter, sondern auch die einsetzenden Behörden. Für eine Verwaltung, die nutzerfreundliche Services in kurzen, iterativen Zyklen ausrollen möchte, bedeutet dies eine spürbare Verlangsamung und einen erheblichen Ressourcenaufwand.

Die Komplexität potenziert sich im Zusammenspiel der Regime. Die vom Europäischen Parlament beauftragte Studie von Graux, Garstka, Murali, Cave und Botterman (2025) kommt zu dem Befund, dass AI Act und DSGVO je für sich zielgenau sind, ihr Zusammenwirken aber erhebliche regulatorische Komplexität erzeugt. Ein praktisch besonders relevanter Reibungspunkt ist die Parallelität von Grundrechte-Folgenabschätzung (FRIA) nach dem AI Act und Datenschutz-Folgenabschätzung (DSFA) nach der DSGVO: Beide Instrumente überschneiden sich inhaltlich, unterscheiden sich aber in Umfang, Aufsicht und Verfahren, was zu Doppelarbeit und Rechtsunsicherheit führt (Graux et al., 2025). Wirtz, Weyerer und Sturm (2020) hatten bereits zuvor diagnostiziert, dass Governance-Kapazitäten der rasanten KI-Entwicklung strukturell hinterherhinken – die KI-Verordnung schließt diese Lücke normativ, verlagert die Last aber in die Verwaltungsorganisation.

Die eigene Bewertung bestätigt H2 nur teilweise. Die Compliance-Last ist real, doch sie ist nicht ausschließlich Bremse. Dieselben Pflichten – Dokumentation, Aufsicht, Risikomanagement – sind zugleich Qualitäts- und Vertrauenshebel und damit funktional eng mit Nutzerfreundlichkeit verknüpft. Österreich hat sich mit der Strategie AIM AT 2030 ausdrücklich zu einem grundrechts- und europarechtskonformen KI-Einsatz bekannt (Bundesregierung Österreich, 2021); die regulatorischen Anforderungen liegen damit auf der Linie der eigenen Strategie. Das eigentliche Risiko ist daher nicht die Regulierung als solche, sondern ein „Compliance-Theater", in dem Pflichten formal erfüllt, aber nicht in bessere Services übersetzt werden.

Die Hochrisiko-Pflichten sind in der Praxis voraussetzungsvoll. Behörden müssen ein Risikomanagement etablieren, die Datenqualität sichern, technische Dokumentation und Protokolle vorhalten, Transparenz gegenüber Betroffenen herstellen und eine wirksame menschliche Aufsicht organisieren (Verordnung [EU] 2024/1689). Da viele Systeme von kommerziellen Anbietern bezogen werden, entsteht eine Abhängigkeit in der Lieferkette: Die einsetzende Stelle haftet für die Einhaltung, kann die zugrunde liegende Technik aber häufig nicht vollständig durchdringen. Besonders kleinere Gemeinden und Bezirksbehörden stoßen hier an Kapazitätsgrenzen. Hinzu kommt ein paradoxer Effekt, den Graux et al. (2025) hervorheben: Die zur Nachvollziehbarkeit geforderte Protokollierung kann selbst umfangreiche personenbezogene Daten erzeugen und damit die Ausübung von Betroffenenrechten erschweren.

Zugleich ist die regulatorische Last in eine strategische Linie eingebettet, die Österreich bereits verfolgt. Mit AIM AT 2030 hat sich der Bund zu einem gemeinwohlorientierten, grundrechts- und europarechtskonformen KI-Einsatz bekannt und Governance-Strukturen samt ressortübergreifender Koordination geschaffen (Bundesregierung Österreich, 2021). Die

Anforderungen des AI Act laufen dieser Linie nicht zuwider, sondern operationalisieren sie. Wirtz et al. (2020) hatten allerdings gewarnt, dass Governance-Kapazitäten der technischen Entwicklung strukturell hinterherhinken; die eigentliche Aufgabe besteht deshalb darin, regulatorische Pflichten in Routinen, Werkzeuge und Kompetenzen zu übersetzen, statt sie als einmalige Formalprüfung abzuhaken. H2 ist somit teilweise zu bestätigen: Die Last ist real, aber gestaltbar und potenziell qualitätssteigernd.

3.3 H3 – Auflösung über Governance: Transparenz, Aufsicht und Privacy-by-Design

Die dritte Hypothese behauptet, dass der Konflikt durch Governance-Mechanismen teilweise auflösbar ist. Die empirische Evidenz stützt dies, mahnt aber zugleich zur Differenzierung. Grimmelikhuijsen (2023) zeigt experimentell, dass für das Vertrauen in automatisierte Entscheidungen die Erklärbarkeit deutlich wichtiger ist als die bloße Zugänglichkeit des Algorithmus; Transparenz im Sinne von Offenlegung allein genügt nicht. De Bruijn, Warnier und Janssen (2022) ergänzen, dass erklärbare KI (XAI) kein Allheilmittel ist, weil die komplexe, oft widersprüchliche Natur staatlicher Probleme einfache Erklärungen erschwert. Erklärbarkeit ist also notwendig, aber anspruchsvoll umzusetzen.

Auf der Seite der menschlichen Aufsicht liefert Hillo, Vento und Erkkilä (2025) belastbare Evidenz: In Survey-Experimenten mit finnischen Spitzenbeamten und einer Bevölkerungsstichprobe erhöhen sowohl Transparenz als auch menschliches Ermessen die wahrgenommene Legitimität automatisierter Entscheidungen. Menschliche Aufsicht ist damit nicht nur eine Rechtspflicht aus Artikel 22 DSGVO und dem AI Act, sondern auch ein Legitimations- und Akzeptanzfaktor. Allerdings setzt Kleizen, Van Dooren und Verhoest (2023) eine wichtige Grenze: Allgemeine Informationen über „ethische KI"-Maßnahmen haben kaum Effekt auf das Vertrauen der Bürgerinnen und Bürger. Symbolische Ethik-Label genügen nicht; Governance muss substanziell und erfahrbar sein, um zu wirken.

Daraus folgt die eigene zentrale These: Der Zielkonflikt ist als Gestaltungsproblem reformulierbar. Privacy-by-Design und eine integrierte Folgenabschätzung, die DSFA und FRIA zusammenführt (Graux et al., 2025), verlagern den Datenschutz aus der nachgelagerten Kontrolle in die Architektur des Service. Die OECD (2024) liefert hierfür einen Rahmen vertrauenswürdiger KI-Nutzung, der Transparenz, Rechenschaft und Kapazitätsaufbau verbindet, und Wirtz et al. (2020) bieten mit ihrem integrierten Governance-Modell eine organisatorische Klammer. H3 ist somit zu bestätigen – mit der Einschränkung, dass nur substanzielle, erfahrbare Governance den Konflikt entschärft, während rein kommunikative Maßnahmen wirkungslos bleiben.

Für die Auflösung des Konflikts ist die Unterscheidung zwischen Transparenz als bloßer Offenlegung und Transparenz als Erklärbarkeit zentral. Grimmelikhuijsen (2023) zeigt, dass erst eine verständliche Begründung und nicht der Zugang zum Quellcode das Vertrauen messbar erhöht, und dass sich dieser Effekt sogar auf das Vertrauen in die menschliche Entscheidungsinstanz überträgt. Erklärbarkeit muss daher adressatengerecht gestaltet sein, was bei komplexen Verfahren anspruchsvoll bleibt (de Bruijn et al., 2022). Bei der menschlichen Aufsicht ist ein Konstruktionsfehler zu vermeiden: Wo Beschäftigte algorithmische Vorschläge unter Zeitdruck nur bestätigen, droht eine Automatisierungsverzerrung statt echter Kontrolle. Wirksame Aufsicht verlangt deshalb Schulung, ausreichende Zeitbudgets und die reale Möglichkeit zur begründeten Abweichung.

Datenschutz wiederum lässt sich durch Privacy-by-Design früh verankern, etwa durch Datenminimierung auf Architekturebene, Pseudonymisierung und eine im System fest verdrahtete Zweckbindung, sodass nutzerfreundliche Funktionen und Schutzpflichten nicht nachträglich gegeneinander ausgespielt werden müssen (OECD, 2024). Eine integrierte Folgenabschätzung, die Datenschutz-Folgenabschätzung und Grundrechte-Folgenabschätzung zusammenführt, reduziert Doppelarbeit und stiftet Kohärenz zwischen den Regimen (Graux et al., 2025). Entscheidend bleibt die von Kleizen et al. (2023) belegte Einsicht, dass allgemeine Bekenntnisse zu ethischer KI das Vertrauen kaum bewegen. Governance wirkt nur, wenn sie substanziell, überprüfbar und im konkreten Service erfahrbar ist.

Aus diesen Bausteinen ergibt sich ein integriertes Lösungsmodell: Erklärbare Begründungen schaffen Vertrauen, wirksame menschliche Aufsicht sichert Legitimität und Rechtsschutz, Privacy-by-Design verankert Datenschutz in der Architektur, und eine gebündelte Folgenabschätzung hält den Aufwand beherrschbar. Keiner dieser Bausteine genügt für sich allein; erst ihr Zusammenspiel verschiebt das Verhältnis von Nutzerfreundlichkeit und Recht vom Gegensatz zur wechselseitigen Stützung. Damit ist der theoretische Kern der dritten Hypothese eingelöst: Der Zielkonflikt ist als Gestaltungsaufgabe lösbar, sofern Governance als Bestandteil des Service und nicht als nachgelagerte Kontrolle verstanden wird.

Bemerkenswert ist, dass dieselbe Maßnahme zwei Ziele zugleich bedient. Erklärbarkeit erfüllt eine rechtliche Pflicht und steigert zugleich die Akzeptanz (Grimmelikhuijsen, 2023; Savveli et al., 2025); menschliche Aufsicht genügt dem Recht und erhöht die wahrgenommene Legitimität (Hillo et al., 2025). Diese Doppelfunktion ist der Kern der Auflösungsthese: Governance ist nicht nur Kostenfaktor des Datenschutzes, sondern Produktionsfaktor der Nutzerfreundlichkeit. Damit verliert der vermeintliche Zielkonflikt an Schärfe, ohne vollständig zu verschwinden.

4 Diskussion

Die Befunde lassen sich an zwei konkreten Zielkonflikten zuspitzen. Der erste betrifft das Verhältnis von Personalisierung und Proaktivität einerseits und Datenminimierung und Zweckbindung andererseits. Eine antraglose Leistungsgewährung – etwa die automatische Auszahlung einer Beihilfe auf Basis bereits vorhandener Register- und Einkommensdaten – ist aus Nutzersicht der Idealfall einer „unsichtbaren" Verwaltung. Sie verlangt aber genau jene bereichsübergreifende Datenverknüpfung, die Artikel 5 DSGVO einhegen soll (Verordnung [EU] 2016/679). Der Konflikt ist nicht auflösbar, indem man eine Seite ignoriert; er verlangt eine bewusste Abwägung, klare Rechtsgrundlagen und technische Vorkehrungen wie Zweckbindung auf Architekturebene und Einwilligungs- bzw. Widerspruchsmechanismen.

Der zweite Zielkonflikt betrifft Effizienz und Automatisierungstempo gegenüber menschlicher Aufsicht und Verfahrensgarantien. Vollautomatisierung verspricht Geschwindigkeit und Konsistenz, kollidiert aber mit Artikel 22 DSGVO und den von Suksi (2021) betonten rechtsstaatlichen Verfahrensgarantien. Erschwerend kommt hinzu, dass „menschliche Aufsicht" teuer und in der Praxis nicht selten illusorisch ist: Wo Sachbearbeiterinnen und Sachbearbeiter algorithmische Vorschläge nur noch abnicken, entsteht eine Aufsicht dem Namen nach, nicht der Substanz nach – ein Risiko, das auch im Lichte der Erklärbarkeitsgrenzen von de Bruijn et al. (2022) ernst zu nehmen ist. Die Evidenz von Hillo et al. (2025) und Kleizen et al. (2023) zeigt zugleich, dass wirksame, nicht nur symbolische Aufsicht für Legitimität und Vertrauen unverzichtbar ist.

Diese Erkenntnisse unterliegen Limitationen. Die belastbare empirische Evidenz stammt überwiegend aus den Niederlanden, den nordischen Ländern und EU-weiten Analysen; spezifisch österreichische Studien zum konkreten Zielkonflikt zwischen KI-Nutzerfreundlichkeit und DSGVO/AI Act sind rar. Der eGovernment MONITOR 2024 liefert zwar aussagekräftige Nutzungs- und Vertrauensdaten für Österreich, ist aber nicht KI-spezifisch (Initiative D21 & Kantar, 2024). Die Übertragbarkeit der ausländischen Befunde ist gleichwohl plausibel, weil Österreich derselben kontinentaleuropäischen, rechtsstaatlich geprägten Verwaltungstradition angehört und demselben EU-Rechtsrahmen unterliegt – sie ist jedoch nicht mit Gewissheit gegeben und sollte durch nationale Forschung abgesichert werden.

Für die österreichische Verwaltungspraxis ist entscheidend, dass günstige institutionelle Voraussetzungen bereits bestehen. Mit Digital Austria, der ressortübergreifenden Koordination und der Strategie AIM AT 2030 verfügt der Bund über Strukturen, die eine eingebettete Governance tragen können (Bundesregierung Österreich, 2021). Kuziemski und

Misuraca (2020) erinnern jedoch daran, dass ohne gemeinsamen Bewertungsrahmen Machtasymmetrien wachsen; die organisatorische Klammer von Wirtz et al. (2020) und der OECD-Rahmen (2024) bieten hier anschlussfähige Modelle.

Über die beiden Zielkonflikte hinaus verbindet eine dritte Dimension die Befunde: Rechenschaft und Rechtsschutz. Automatisierte Entscheidungen müssen anfechtbar bleiben, und die dafür nötige Nachvollziehbarkeit steht in Spannung zum Wunsch nach schlanken, schnellen Prozessen. Die Evidenz weist hier einen Ausweg: Da wirksame Aufsicht und erfahrbare Transparenz die Legitimität erhöhen (Hillo et al., 2025), während symbolische Maßnahmen wirkungslos bleiben (Kleizen et al., 2023), lohnt sich die Investition in substanzielle Governance auch ökonomisch, weil sie Akzeptanz, Folgekosten und Anfechtungsrisiken zugleich adressiert. Vertrauen erweist sich als die verbindende Variable zwischen Nutzerfreundlichkeit und Rechtskonformität, weil beide Seiten auf dasselbe Konto einzahlen.

Die Übertragbarkeit der internationalen Befunde auf Österreich verdient eine differenzierte Betrachtung. Die zitierten Experimente stammen überwiegend aus den Niederlanden, Finnland und Belgien (Grimmelikhuijsen, 2023; Hillo et al., 2025; Kleizen et al., 2023), also aus Verwaltungssystemen mit vergleichbarer rechtsstaatlicher Prägung und demselben EU-Rechtsrahmen. Das stützt die Annahme, dass die Wirkungslogik von Transparenz, Erklärbarkeit und Aufsicht auch in Österreich greift. Dennoch unterscheiden sich Verwaltungskultur, Vertrauensniveau und institutionelle Pfade, sodass Effektstärken nicht unbesehen übernommen werden dürfen. Die belastbarste Schlussfolgerung lautet daher: Die Richtung der Zusammenhänge ist übertragbar, ihr genaues Ausmaß ist im österreichischen Kontext empirisch zu überprüfen.

Eine zweite konkrete Servicesituation unterstreicht die Tragweite: Bei KI-gestützten Chatbots, die rund um die Uhr Auskunft geben, entsteht Nutzen gerade durch niedrige Schwellen und freie Spracheingabe. Genau diese Offenheit führt jedoch dazu, dass Bürgerinnen und Bürger unaufgefordert sensible Informationen preisgeben, die das System protokolliert. Datenschutz durch Voreinstellung verlangt hier, Eingaben zu minimieren, sensible Inhalte herauszufiltern und Protokolle streng zweckgebunden vorzuhalten. Der Fall zeigt, dass die Lösung selten in einem Entweder-oder liegt, sondern in einer durchdachten Voreinstellung, die Nutzerfreundlichkeit ermöglicht und zugleich die Datenexposition begrenzt. Solche Voreinstellungen sind weniger spektakulär als die Debatte über Verbote, für die Verwaltungspraxis aber entscheidend.

Für die österreichische Praxis lassen sich daraus konkrete Hebel ableiten. Die bestehende Governance-Architektur rund um Digital Austria und die ressortübergreifende Koordination bietet einen institutionellen Rahmen, um einheitliche Standards für Erklärbarkeit, Aufsicht und Folgenabschätzung zu setzen (Bundesregierung Österreich, 2021). Die Datenschutzbehörde wiederum kann durch praxisnahe Leitlinien Rechtssicherheit schaffen, während die Fachressorts für die service- und domänenspezifische Umsetzung verantwortlich bleiben. Entscheidend ist die Verzahnung dieser Ebenen, denn isolierte Einzelmaßnahmen drohen, den von Kuziemski und Misuraca (2020) beschriebenen Machtasymmetrien nicht wirksam zu begegnen.

5 Fazit und Handlungsempfehlungen

Der Zielkonflikt zwischen nutzerfreundlicher KI-Automatisierung und den Anforderungen von DSGVO und EU AI Act ist real, aber nicht binär. Er lässt sich nicht durch den Verzicht auf eine der beiden Seiten auflösen, wohl aber durch eine substanzielle, in die Servicearchitektur eingebettete Governance teilweise versöhnen. Nutzerfreundlichkeit und Rechtskonformität teilen ein gemeinsames Fundament – das Vertrauen der Bürgerinnen und Bürger –, und genau dieses Vertrauen entsteht nur, wenn Transparenz erfahrbar, Aufsicht wirksam und Datenschutz in die Technik eingebaut ist. Österreich ist dafür institutionell gut aufgestellt, muss die regulatorischen Pflichten aber als Qualitätshebel statt als Bürde begreifen.

Damit die Empfehlungen nicht zum eingangs beschriebenen bloßen Formalismus verkommen, sind sie an messbare Wirkungen zu koppeln. Eine begleitende Evaluierung über Nutzungs-, Zufriedenheits- und Beschwerdedaten sowie über die Quote erfolgreicher Anfechtungen macht sichtbar, ob substanzielle Governance tatsächlich Vertrauen und Servicequalität steigert. Der eGovernment MONITOR liefert dafür eine etablierte, wenn auch nicht KI-spezifische Datenbasis (Initiative D21 & Kantar, 2024), die um KI-bezogene Indikatoren erweitert werden sollte.

Aus dieser Analyse leiten sich – als eigenständige Position, gestützt auf, aber nicht ersetzt durch die Literatur – folgende konkrete Handlungsempfehlungen ab:

Empfehlung 1 (Wer: Digital Austria / Bundeskanzleramt. Was: ein integriertes DSFA-FRIA-Template samt Prozessleitfaden, das Doppelarbeit beseitigt und Folgenabschätzungen bündelt. Bis wann: Q2 2027).

Empfehlung 2 (Wer: Behördenleitungen in Ressorts und Ländern. Was: ein verbindlicher Standard für „wirksame menschliche Aufsicht" inklusive Schulung gegen reines Abnicken algorithmischer Vorschläge. Bis wann: Ende 2026).

Empfehlung 3 (Wer: Datenschutzbehörde gemeinsam mit Digital Austria. Was: eine praxisnahe Leitlinie zu Datenminimierung und Zweckbindung für proaktive Services, inklusive Muster-Rechtsgrundlagen und Widerspruchsmechanismen. Bis wann: Q4 2026).

Empfehlung 4 (Wer: einsetzende Fachressorts. Was: standardmäßige, bürgerverständliche Erklärbarkeit jeder KI-gestützten Entscheidung statt bloßer Offenlegung von Quellcode. Bis wann: ab 2027 bei allen neuen KI-Services).

Empfehlung 5 (Wer: Bund / Digital Austria. Was: Aufbau von KI-Kompetenz und ein zentrales, öffentlich einsehbares Transparenz- und Use-Case-Register für Verwaltungs-KI. Bis wann: laufend, Vollausbau bis 2028).

In der Summe verschiebt dieser Ansatz die Debatte von einem vermeintlichen Entweder-oder hin zu einem Sowohl-als-auch: Eine Verwaltung, die Datenschutz und Grundrechte als Bestandteil guter Servicegestaltung versteht, kann nutzerfreundlicher und rechtskonformer zugleich werden – und sichert damit langfristig genau die Akzeptanz, die ihre digitale Vorreiterrolle trägt.

Literaturverzeichnis

Bundesregierung Österreich. (2021). Strategie der Bundesregierung für Künstliche Intelligenz – Artificial Intelligence Mission Austria 2030 (AIM AT 2030). Digital Austria. https://www.digitalaustria.gv.at/dam/jcr:44ad1b93-6358-42b8-9f65-1e74c9a39e7f/KI%20Strategie_AIM_AT_2030_UAbf.pdf

Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999 in der geltenden Fassung. Republik Österreich. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

de Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. Government Information Quarterly, 39(2), 101666. https://doi.org/10.1016/j.giq.2021.101666

Dechamps, S., Simonofski, A., & Burnay, C. (2025). Citizen-centricity in digital government: A theoretical and empirical typology. Government Information Quarterly, 42(1), 102005. https://doi.org/10.1016/j.giq.2024.102005

Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). Interplay between the AI Act and the EU digital legislative framework (PE 778.575). European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf

Grimmelikhuijsen, S. (2023). Explaining why the computer says no: Algorithmic transparency affects the perceived trustworthiness of automated decision-making. Public Administration Review, 83(2), 241–262. https://doi.org/10.1111/puar.13483

Hillo, J., Vento, I., & Erkkilä, T. (2025). Algorithmic governance: Experimental evidence on citizens' and public administrators' legitimacy perceptions of automated decision-making. Public Administration. Vorab-Onlineveröffentlichung. https://doi.org/10.1111/padm.70028

Initiative D21 & Kantar. (2024). eGovernment MONITOR 2024: Nutzung und Akzeptanz digitaler Verwaltungsangebote in Deutschland, Österreich und der Schweiz. https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2024/egovernment_monitor_24.pdf

Kleizen, B., Van Dooren, W., & Verhoest, K. (2023). Do citizens trust trustworthy artificial intelligence? Experimental evidence on the limits of ethical AI measures in government. Government Information Quarterly, 40(4), 101834. https://doi.org/10.1016/j.giq.2023.101834

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. Telecommunications Policy, 44(6), 101976. https://doi.org/10.1016/j.telpol.2020.101976

OECD. (2024). Governing with artificial intelligence: The state of play and way forward in core government functions. OECD Publishing. https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html

Savveli, I., Rigou, M., & Balaskas, S. (2025). From e-government to AI e-government: A systematic review of citizen attitudes. Informatics, 12(3), 98. https://doi.org/10.3390/informatics12030098

Suksi, M. (2021). Administrative due process when using automated decision-making in public administration: Some notes from a Finnish perspective. Artificial Intelligence and Law, 29(1), 87–110. https://doi.org/10.1007/s10506-020-09269-x

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (Datenschutz-Grundverordnung). ABl. L 119, 4.5.2016, S. 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (Verordnung über künstliche Intelligenz). ABl. L, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. International Journal of Public Administration, 42(7), 596–615. https://doi.org/10.1080/01900692.2018.1498103

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. International Journal of Public Administration, 43(9), 818–829. https://doi.org/10.1080/01900692.2020.1749851