© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

DIGITALISIERUNG DER ÖFFENTLICHEN VERWALTUNG UND DER SCHUTZ PERSONENBEZOGENER DATEN: RECHTLICHE HERAUSFORDERUNGEN UND PERSPEKTIVEN FÜR USBEKISTAN

MELIBAYEV TEMUR NIKOLAY O'G'LI
TDYU huzuridagi M.S.Vosiqova nomidagi akademik litsey 2-kurs o'quvchisi
DOI:https://doi.org/10.5281/zenodo.24121208

Zusammenfassung

Die Digitalisierung der öffentlichen Verwaltung verändert die Beziehungen zwischen Staat, Bürgerinnen und Bürgern sowie Unternehmen. Elektronische Dienstleistungen, digitale Register, automatisierte Verwaltungsverfahren und datenbasierte Entscheidungsprozesse können die Effizienz, Transparenz und Zugänglichkeit staatlicher Leistungen verbessern. Gleichzeitig entstehen neue rechtliche Risiken: Eine übermäßige Erhebung personenbezogener Daten, unzureichende Informationssicherheit, intransparente algorithmische Entscheidungen und fehlende wirksame Rechtsbehelfe können Grundrechte beeinträchtigen. Der Beitrag untersucht das Verhältnis zwischen digitaler Verwaltung und Datenschutz aus rechtswissenschaftlicher Perspektive und konzentriert sich dabei auf die rechtlichen und institutionellen Entwicklungsmöglichkeiten Usbekistans. Methodisch werden rechtsdogmatische Analyse, vergleichende Betrachtung und systematische Auswertung internationaler Standards miteinander verbunden. Im Mittelpunkt stehen die Grundsätze der Rechtmäßigkeit, Zweckbindung, Datenminimierung, Transparenz, Sicherheit und Rechenschaftspflicht. Der Beitrag argumentiert, dass eine nachhaltige digitale Transformation nicht allein von technischen Lösungen abhängt. Sie setzt einen klaren gesetzlichen Rahmen, unabhängige Aufsicht, verständliche Verwaltungsverfahren, barrierefreien Zugang und effektiven gerichtlichen Rechtsschutz voraus. Als Ergebnis werden Reformansätze vorgeschlagen, die digitale Innovation und den Schutz der Menschenwürde sowie der Privatsphäre miteinander in Einklang bringen.

Schlüsselwörter

Digitalisierung; öffentliche Verwaltung; Datenschutz; personenbezogene Daten; elektronische Dienstleistungen; Rechtsstaatlichkeit; Usbekistan; Menschenrechte.

Einleitung

Die digitale Transformation gehört zu den bedeutendsten Veränderungen moderner Staatlichkeit. Behörden verwenden zunehmend elektronische Dokumente, Online-Portale, digitale Identifikationssysteme, Register und automatisierte Informationsverarbeitung. Diese Instrumente können Verwaltungsverfahren beschleunigen, Kosten reduzieren und den Zugang zu staatlichen Leistungen erleichtern. Bürgerinnen und Bürger können Anträge elektronisch einreichen, Informationen abrufen und mit Behörden kommunizieren, ohne jede Angelegenheit persönlich erledigen zu müssen.

Die Digitalisierung ist jedoch kein rein technischer Vorgang. Jede digitale Verwaltungsleistung beruht auf rechtlichen Beziehungen: Eine Behörde verarbeitet

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Informationen, trifft Entscheidungen, gewährt oder versagt Leistungen und beeinflusst dadurch die Rechte und Pflichten bestimmter Personen. Deshalb muss die digitale Verwaltung an die Grundsätze der Verfassung, des Verwaltungsrechts und des Datenschutzrechts gebunden bleiben. Die Verwendung moderner Technologien darf die Bindung der öffentlichen Gewalt an Recht und Gesetz nicht schwächen.

Besondere Bedeutung besitzt der Schutz personenbezogener Daten. Staatliche Stellen verfügen häufig über umfangreiche Informationen, etwa zu Identität, Wohnsitz, Bildung, Beschäftigung, Sozialleistungen oder Eigentum. Werden solche Daten ohne klare Rechtsgrundlage gesammelt, zu anderen Zwecken verwendet oder unzureichend geschützt, können Privatsphäre, informationelle Selbstbestimmung und Gleichbehandlung beeinträchtigt werden. Fehlerhafte Daten können außerdem zu falschen Verwaltungsentscheidungen führen.

Für Usbekistan ist dieses Thema im Zusammenhang mit der Modernisierung öffentlicher Dienstleistungen und dem Ausbau elektronischer Verwaltungsinfrastrukturen besonders relevant. Die Verfassung der Republik Usbekistan schützt grundlegende Rechte und Freiheiten; das nationale Recht enthält zudem Regelungen über personenbezogene Daten und elektronische Verwaltungsprozesse. Die praktische Wirksamkeit dieser Garantien hängt jedoch davon ab, wie sie in Behörden, technischen Systemen und gerichtlichen Verfahren umgesetzt werden.

Ziel dieses Beitrags ist es, die rechtlichen Voraussetzungen einer menschenrechtsorientierten digitalen Verwaltung zu untersuchen. Die zentrale Forschungsfrage lautet: Wie kann Usbekistan die Effizienz digitaler Verwaltungsleistungen steigern und zugleich personenbezogene Daten sowie verfassungsrechtlich geschützte Rechte wirksam sichern? Der Beitrag vertritt die These, dass Digitalisierung nur dann rechtsstaatlich legitim ist, wenn jede Datenverarbeitung auf einer nachvollziehbaren Rechtsgrundlage beruht, für einen bestimmten Zweck erforderlich ist und einer wirksamen Kontrolle unterliegt.

Der Beitrag ist in sechs thematische Schritte gegliedert. Zunächst werden Methode und begriffliche Grundlagen erläutert. Danach werden internationale Datenschutzstandards und ihre Bedeutung für die öffentliche Verwaltung betrachtet. Anschließend werden zentrale rechtliche Herausforderungen analysiert. Darauf aufbauend werden Ergebnisse und Reformvorschläge für Usbekistan entwickelt. Abschließend werden die wichtigsten Schlussfolgerungen zusammengefasst.

Material und Methoden

Die Untersuchung verwendet eine qualitative rechtswissenschaftliche Methodik. Erstens wird die rechtsdogmatische Methode eingesetzt, um grundlegende Prinzipien des Verfassungs-, Verwaltungs- und Datenschutzrechts zu bestimmen. Dabei werden insbesondere die Bindung der Verwaltung an das Gesetz, der Schutz der Privatsphäre, Gleichheit vor dem Gesetz und das Recht auf wirksamen Rechtsschutz berücksichtigt.

Zweitens wird eine vergleichende Methode angewendet. Internationale Dokumente und ausgewählte Regelungsansätze, insbesondere die Datenschutz-Grundverordnung der Europäischen Union (DSGVO), dienen als Vergleichsmaßstab. Die DSGVO ist für Usbekistan nicht automatisch verbindlich; sie bietet jedoch ein ausformuliertes Modell für Grundsätze wie Zweckbindung, Datenminimierung, Transparenz, Sicherheit und Rechenschaftspflicht. Auch die

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Leitlinien der OECD zum Schutz der Privatsphäre und grenzüberschreitenden Datenverkehr sowie die Grundsätze des Europarats werden als Orientierung herangezogen.

Drittens wird eine systematische Analyse vorgenommen. Die Digitalisierung wird nicht isoliert als Frage der Datensicherheit betrachtet, sondern als Zusammenspiel von Gesetzgebung, Verwaltungspraxis, technischer Infrastruktur, institutioneller Aufsicht und Rechtsschutz.

Dieser Ansatz ist notwendig, weil ein technisch sicheres System dennoch rechtswidrig sein kann, wenn die Daten ohne ausreichende Rechtsgrundlage erhoben werden. Umgekehrt kann ein gutes Gesetz wirkungslos bleiben, wenn Behörden keine geeigneten Sicherheitsmaßnahmen oder Beschwerdeverfahren bereitstellen.

Die Untersuchung stützt sich auf öffentlich zugängliche normative und wissenschaftliche Materialien. Sie verfolgt keinen empirischen Anspruch und enthält keine eigene statistische Erhebung. Aussagen über die institutionelle Praxis werden daher als rechtliche Bewertung und Reformüberlegung formuliert, nicht als Ergebnis einer repräsentativen Befragung. Die Analyse unterscheidet zwischen geltendem Recht, internationalen Vergleichsstandards und normativen Empfehlungen. Diese Unterscheidung verhindert, dass ausländische Standards fälschlich als unmittelbar geltendes usbekisches Recht dargestellt werden.

Ergebnisse

Digitalisierung als Instrument guter Verwaltung

Digitale Verwaltungsleistungen können mehrere rechtsstaatlich relevante Vorteile schaffen. Erstens erhöhen sie die Zugänglichkeit staatlicher Dienstleistungen. Elektronische Anträge und digitale Informationsangebote können räumliche Hindernisse reduzieren und insbesondere Menschen unterstützen, die weit von Verwaltungszentren entfernt wohnen. Zweitens können standardisierte elektronische Verfahren die Bearbeitungsdauer verkürzen und die Nachvollziehbarkeit einzelner Verfahrensschritte verbessern. Drittens ermöglichen digitale Register einen schnelleren Informationsaustausch zwischen Behörden, sofern dieser Austausch gesetzlich geregelt und technisch abgesichert ist.

Diese Vorteile treten jedoch nicht automatisch ein. Ein Online-Portal ist nicht schon deshalb bürgerfreundlich, weil es rund um die Uhr erreichbar ist. Wenn die Benutzeroberfläche unverständlich ist, keine barrierefreien Alternativen existieren oder eine Person wegen fehlender digitaler Kenntnisse keinen Zugang erhält, kann die Digitalisierung neue Ungleichheiten erzeugen. Gute digitale Verwaltung muss deshalb sowohl Effizienz als auch Inklusion gewährleisten.

Datenschutz als Voraussetzung legitimer Datenverarbeitung

Personenbezogene Daten sind Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Im Verwaltungsbereich können hierzu Identifikationsdaten, Kontaktdaten, Angaben zu Familienstand, Ausbildung, Beschäftigung, Einkommen oder Sozialleistungen gehören. Die Verarbeitung solcher Informationen kann für öffentliche Aufgaben notwendig sein. Sie muss jedoch rechtlich begrenzt bleiben.

Ein erster zentraler Grundsatz ist die Rechtmäßigkeit. Eine Behörde muss erkennen können, auf welche gesetzliche Grundlage sie eine Datenverarbeitung stützt. Der bloße Hinweis auf allgemeine Verwaltungszwecke reicht nicht aus, wenn Umfang und Zweck der Verarbeitung nicht hinreichend bestimmt sind. Der

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

zweite Grundsatz ist die Zweckbindung: Daten, die für eine konkrete Leistung erhoben wurden, dürfen nicht ohne geeignete Rechtsgrundlage für völlig andere Zwecke genutzt werden. Drittens verlangt die Datenminimierung, nur jene Informationen zu erheben, die für die jeweilige Aufgabe erforderlich sind.

Hinzu kommen Richtigkeit, Speicherbegrenzung und Sicherheit. Unrichtige Daten können zu fehlerhaften Entscheidungen führen. Eine unbegrenzte Speicherung erhöht das Risiko von Missbrauch und unbefugtem Zugriff. Behörden müssen daher Verfahren zur Aktualisierung, Berichtigung und Löschung vorsehen, soweit gesetzliche Aufbewahrungspflichten dem nicht entgegenstehen. Sicherheitsmaßnahmen müssen dem Risiko angemessen sein und organisatorische wie technische Vorkehrungen umfassen.

Transparenz und Rechte der betroffenen Personen

Eine Person kann ihre Rechte nur dann wirksam ausüben, wenn sie weiß, welche Behörde ihre Daten verarbeitet, zu welchem Zweck dies geschieht und welche Möglichkeiten zur Berichtigung oder Beschwerde bestehen. Transparenz ist daher kein nebensächlicher Informationsservice, sondern eine Voraussetzung rechtmäßiger Verwaltung.

Digitale Verwaltungsdienste sollten in verständlicher Sprache erklären, welche Daten zwingend erforderlich sind, welche Rechtsgrundlage besteht, ob Informationen an andere Behörden übermittelt werden und wie lange sie gespeichert werden. Die betroffene Person sollte außerdem einen praktikablen Weg haben, unrichtige Angaben berichtigen zu lassen und eine rechtswidrige Verarbeitung anzufechten. Ein formales Recht, das nur über komplizierte oder ausschließlich digitale Verfahren ausgeübt werden kann, ist in der Praxis möglicherweise nicht wirksam.

Automatisierte Entscheidungen und algorithmische Systeme

Mit der Digitalisierung wächst das Interesse an automatisierten Systemen, die Anträge sortieren, Risiken bewerten oder bestimmte Verwaltungsentscheidungen vorbereiten. Solche Systeme können Routineaufgaben unterstützen und eine konsistentere Bearbeitung ermöglichen. Sie können aber auch Fehler systematisch wiederholen oder bestimmte Bevölkerungsgruppen benachteiligen, wenn die zugrunde liegenden Daten unvollständig oder verzerrt sind.

Besonders problematisch sind Entscheidungen mit erheblichen Auswirkungen auf einzelne Personen, etwa bei Sozialleistungen, Bildung, Beschäftigung oder behördlichen Genehmigungen. In solchen Fällen müssen die Kriterien nachvollziehbar sein. Betroffene sollten erfahren können, ob ein automatisiertes System eine wesentliche Rolle gespielt hat, und eine menschliche Überprüfung verlangen können, sofern dies nach dem anwendbaren Recht vorgesehen oder zur Gewährleistung effektiven Rechtsschutzes erforderlich ist.

Ein Algorithmus darf nicht zu einer rechtlichen Blackbox werden. Die Verantwortung für eine Verwaltungsentscheidung bleibt bei der zuständigen Behörde. Sie kann sich nicht allein mit dem Hinweis entlasten, eine Software habe das Ergebnis berechnet. Erforderlich sind dokumentierte Entscheidungswege, Qualitätskontrollen, regelmäßige Prüfungen und klare Zuständigkeiten.

Informationssicherheit und institutionelle Verantwortung

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Die Konzentration zahlreicher Datensätze in digitalen Systemen macht Informationssicherheit zu einer Kernaufgabe des Staates. Unbefugte Zugriffe, Datenverluste oder Manipulationen können nicht nur individuelle Rechte verletzen, sondern auch das Vertrauen in öffentliche Institutionen beeinträchtigen. Informationssicherheit umfasst deshalb Zugangskontrollen, sichere Authentifizierung, Verschlüsselung, Protokollierung, Datensicherung, Mitarbeiterschulungen und Verfahren zur Reaktion auf Sicherheitsvorfälle.

Die Verantwortung darf nicht ausschließlich der technischen Abteilung einer Behörde übertragen werden. Leitungsorgane müssen Risiken bewerten, Zuständigkeiten festlegen und sicherstellen, dass Datenschutz bereits bei der Planung neuer Systeme berücksichtigt wird. Dieses Konzept wird international häufig als „Privacy by Design“ und „Privacy by Default“ bezeichnet. Es bedeutet, dass Schutzmaßnahmen nicht erst nach einem Vorfall ergänzt werden, sondern von Anfang an Bestandteil der Systemgestaltung sind.

Zugangsgerechtigkeit und digitale Inklusion

Ein rechtsstaatlicher Digitalisierungsprozess muss unterschiedliche Lebenslagen berücksichtigen. Nicht alle Menschen verfügen über dieselbe Internetverbindung, dieselben Geräte oder dieselben digitalen Kompetenzen. Menschen mit Behinderungen können auf barrierefreie Gestaltung angewiesen sein. Ältere Personen oder Bewohner abgelegener Gebiete können zusätzliche Unterstützung benötigen.

Daher sollte die digitale Verwaltung alternative Zugangsmöglichkeiten erhalten, solange diese erforderlich sind. Persönliche Beratung, telefonische Unterstützung und zugängliche Servicezentren können digitale Angebote ergänzen. Digitale Transformation darf nicht bedeuten, dass der Zugang zu einem staatlichen Recht faktisch von der Fähigkeit abhängt, eine bestimmte App oder Plattform zu bedienen.

Diskussion

Die Ergebnisse zeigen, dass Datenschutz und Digitalisierung keine gegensätzlichen Ziele sind. Ein angemessener Datenschutz kann das Vertrauen in digitale Dienstleistungen stärken und dadurch ihre Nutzung fördern. Umgekehrt kann eine Verwaltung, die Daten ohne klare Grenzen sammelt, kurzfristig effizient erscheinen, langfristig jedoch das Vertrauen der Bevölkerung verlieren.

Eine zentrale Herausforderung besteht darin, den Begriff des öffentlichen Interesses nicht unbegrenzt auszulegen. Behörden benötigen Daten, um gesetzliche Aufgaben zu erfüllen. Daraus folgt jedoch kein allgemeines Recht, sämtliche verfügbaren Informationen zu sammeln. Jede Verarbeitung sollte auf Erforderlichkeit und Verhältnismäßigkeit geprüft werden. Dabei ist zu fragen, ob das Ziel mit weniger Daten oder mit einer weniger eingriffsintensiven Methode erreicht werden kann.

Ein weiterer Konflikt betrifft den Datenaustausch zwischen Behörden. Interoperabilität kann Doppelarbeit vermeiden und Verwaltungsleistungen beschleunigen. Gleichzeitig steigt das Risiko, dass Daten über ihren ursprünglichen Zweck hinaus verwendet werden. Ein sicherer Datenaustausch benötigt daher klare gesetzliche Zuständigkeiten, protokollierte Zugriffe und Regeln über die Weitergabe. Technische Vernetzung darf die rechtlichen Grenzen einzelner Behörden nicht aufheben.

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

Die DSGVO bietet einen nützlichen Vergleichsrahmen, insbesondere durch ihre Grundsätze der Rechenschaftspflicht und des Datenschutzes durch Technikgestaltung. Dennoch sollte eine Rechtsordnung nicht lediglich ausländische Normen kopieren. Regelungen müssen zur Verfassungsstruktur, Verwaltungspraxis, technischen Leistungsfähigkeit und gesellschaftlichen Situation des jeweiligen Staates passen. Für Usbekistan ist deshalb eine schrittweise Umsetzung sinnvoll, die klare Mindestgarantien mit realistischen institutionellen Anforderungen verbindet.

Von besonderer Bedeutung ist die unabhängige oder jedenfalls funktional wirksame Aufsicht. Datenschutzrechte bleiben schwach, wenn dieselbe Stelle, die Daten verarbeitet, allein über Beschwerden gegen diese Verarbeitung entscheidet. Eine Aufsichtsstruktur sollte über ausreichende Fachkenntnisse, klare Untersuchungsbefugnisse und transparente Berichtsmechanismen verfügen. Zugleich müssen Zuständigkeiten zwischen Datenschutzaufsicht, Cybersicherheitsorganen, Verwaltungsbehörden und Gerichten eindeutig geregelt sein.

Auch die gerichtliche Kontrolle muss mit der technischen Entwicklung Schritt halten. Gerichte sollten Zugang zu den Informationen erhalten können, die erforderlich sind, um die Rechtmäßigkeit einer automatisierten oder datenbasierten Entscheidung zu prüfen. Dazu können Verfahrensprotokolle, die verwendete Rechtsgrundlage, die entscheidungsrelevanten

Daten und eine verständliche Beschreibung des Systems gehören. Geschäftsgeheimnisse dürfen nicht pauschal dazu führen, dass staatliche Entscheidungen jeder Kontrolle entzogen werden.

Schließlich ist Datenschutz nicht nur eine Frage individueller Ansprüche. Er hat eine demokratische Dimension. Wenn Menschen befürchten müssen, dass jede digitale Handlung unbegrenzt erfasst und verknüpft wird, kann dies ihre Bereitschaft beeinträchtigen, öffentliche Dienstleistungen zu nutzen oder ihre Rechte auszuüben. Datenschutz schützt somit nicht nur persönliche Geheimnisse, sondern auch Autonomie, Würde und gesellschaftliches Vertrauen.

Empfehlungen für Usbekistan

Auf Grundlage der Analyse lassen sich mehrere Reformrichtungen formulieren.

Erstens sollte jede Behörde ein vollständiges und regelmäßig aktualisiertes Verzeichnis ihrer Verarbeitungstätigkeiten führen. Dieses Verzeichnis sollte Zweck, Datenkategorien, Rechtsgrundlage, Empfänger, Speicherfristen und verantwortliche Stellen enthalten. Eine solche Dokumentation erleichtert interne Kontrolle und externe Aufsicht.

Zweitens sollten Datenschutz-Folgenabschätzungen für besonders risikoreiche Projekte eingeführt oder konsequent angewendet werden. Vor der Einführung eines neuen zentralen Registers, eines biometrischen Systems oder eines algorithmischen Entscheidungstools sollte die Behörde mögliche Auswirkungen auf Grundrechte untersuchen. Die Bewertung sollte Risiken, Schutzmaßnahmen und verbleibende Gefahren dokumentieren.

Drittens müssen Informationspflichten verständlich und zugänglich gestaltet werden. Datenschutzhinweise sollten nicht ausschließlich aus langen juristischen Texten bestehen. Kurze Erläuterungen in klarer Sprache, ergänzt durch ausführliche rechtliche Informationen, können die tatsächliche Verständlichkeit

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

verbessern. Wo sinnvoll, sollten Informationen in den in Usbekistan gebräuchlichen Sprachen angeboten werden.

Viertens sollten Betroffene über einfache Verfahren verfügen, um Auskunft zu erhalten, unrichtige Daten berichtigen zu lassen und Beschwerden einzureichen. Für Personen ohne zuverlässigen Internetzugang müssen alternative Wege bestehen. Fristen und Zuständigkeiten sollten gesetzlich oder durch klare Verfahrensregeln bestimmt werden.

Fünftens ist eine wirksame Kontrolle automatisierter Verwaltungsentscheidungen erforderlich. Bei Entscheidungen mit erheblichen Auswirkungen sollten Behörden dokumentieren, welche Rolle automatisierte Systeme gespielt haben. Es sollte eine verantwortliche menschliche Stelle geben, die Einwände prüft und die Entscheidung begründen kann. Systeme müssen regelmäßig auf Fehler und diskriminierende Auswirkungen getestet werden.

Sechstens sollten öffentliche Stellen verbindliche Mindeststandards für Informationssicherheit anwenden. Dazu gehören rollenbasierte Zugriffsrechte, starke Authentifizierung, Verschlüsselung, regelmäßige Sicherheitsprüfungen, Mitarbeiterschulungen und ein klarer Plan für Sicherheitsvorfälle. Bei erheblichen Vorfällen sollten zuständige Stellen und betroffene Personen nach klaren Regeln informiert werden.

Siebtens sollte die Ausbildung von Verwaltungsmitarbeitenden gestärkt werden. Datenschutz ist nicht allein Aufgabe von Juristen oder IT-Fachleuten. Beschäftigte, die täglich mit Bürgerdaten arbeiten, müssen Grundkenntnisse über Vertraulichkeit, Zweckbindung, sichere Kommunikation und den Umgang mit Anfragen besitzen.

Achtens sollte die Gesetzgebung technologieneutral und zukunftsorientiert formuliert werden. Zu detaillierte technische Vorgaben können rasch veralten. Das Gesetz sollte daher grundlegende Rechte, Pflichten, Verantwortlichkeiten und Kontrollmechanismen festlegen, während technische Standards regelmäßig aktualisiert werden können.

Neuntens muss digitale Inklusion als Bestandteil guter Verwaltung verstanden werden. Elektronische Angebote sollten barrierefrei, mobil nutzbar und möglichst einfach gestaltet sein. Gleichzeitig sollten persönliche Unterstützungsangebote erhalten bleiben, damit niemand allein wegen fehlender technischer Fähigkeiten von staatlichen Leistungen ausgeschlossen wird.

Zehntens sollte die internationale Zusammenarbeit ausgebaut werden. Erfahrungsaustausch mit Staaten und internationalen Organisationen kann helfen, bewährte Praktiken zu übernehmen. Dabei ist stets zu prüfen, welche Modelle mit den nationalen verfassungsrechtlichen und institutionellen Bedingungen vereinbar sind.

Schlussfolgerung

Die Digitalisierung der öffentlichen Verwaltung bietet Usbekistan erhebliche Chancen, staatliche Dienstleistungen zugänglicher, schneller und transparenter zu gestalten. Ihr Erfolg darf jedoch nicht allein an der Zahl elektronischer Portale oder der Geschwindigkeit der Datenverarbeitung gemessen werden. Entscheidend ist, ob digitale Verfahren die Rechte der Menschen achten und die öffentliche Gewalt weiterhin an Recht und Gesetz binden.

Die Untersuchung hat gezeigt, dass ein wirksamer Datenschutz auf mehreren miteinander verbundenen Elementen beruht: einer klaren gesetzlichen Grundlage,

© 2026 Arabian International Conference on Science,Technology and Innovation. All rights reserved.

bestimmten Verarbeitungszwecken, Datenminimierung, Transparenz, Informationssicherheit, wirksamer Aufsicht und effektivem Rechtsschutz. Bei automatisierten Entscheidungen kommen zusätzliche Anforderungen hinzu, insbesondere Nachvollziehbarkeit, Dokumentation und die Möglichkeit einer angemessenen Überprüfung.

Für Usbekistan empfiehlt sich ein ganzheitlicher Ansatz. Datenschutz sollte bereits bei der Planung digitaler Verwaltungsprojekte berücksichtigt werden. Behörden benötigen klare Verantwortlichkeiten und ausreichende Fachkompetenz. Bürgerinnen und Bürger müssen verständliche Informationen und praktikable Beschwerdewege erhalten. Besonders risikoreiche Systeme sollten vor ihrer Einführung und während ihres Betriebs regelmäßig überprüft werden.

Die zentrale Schlussfolgerung lautet: Eine moderne digitale Verwaltung ist nicht nur eine Verwaltung, die Technologien verwendet, sondern eine Verwaltung, die Technologien rechtmäßig, transparent, sicher und menschenorientiert einsetzt. Wenn Usbekistan diese Prinzipien konsequent miteinander verbindet, kann die digitale Transformation sowohl die Leistungsfähigkeit des Staates als auch das Vertrauen der Bevölkerung stärken.

Danksagung

Der Beitrag wurde ohne die Angabe einer institutionellen Förderung oder individueller Unterstützungsleistungen vorbereitet. Falls im Rahmen der endgültigen Einreichung eine Förderung, Betreuung oder fachliche Unterstützung vorliegt, sollte diese hier konkret und wahrheitsgemäß angegeben werden.

Literaturverzeichnis

1. Council of Europe. (1981). Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108). https://www.coe.int/en/web/data-protection/convention108
2. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. Organisation for Economic Co-operation and Development. (2013). The OECD privacy framework. OECD Publishing. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
4. United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights
5. United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/ins truments-mechanisms/instruments/international-covenant-civil-and-political-rights
6. Republic of Uzbekistan. (2019). Law No. ZRU-547 on personal data (as amended). National legislation database, LexUZ. https://lex.uz/docs/4396419
7. Republic of Uzbekistan. (2023). Constitution of the Republic of Uzbekistan. National legislation database, LexUZ. https://lex.uz/