

AI for Public Services: Faster, More Transparent, Cheaper

A.T. Svanovich^{1*}, E.V. Petrova²

¹ Department of Computer Science, National Research University, Almaty, Kazakhstan

² Institute for Digital Privacy & Security, Astana, Kazakhstan

Corresponding author: E.V. Petrova, email: e.petrova@idps.kz

Abstract

AI is reshaping how governments deliver services and manage registers. This article maps high-value uses—proactive, event-driven benefits and permits; risk-based inspections; fraud detection; and intelligent queueing—inside a governance frame that embeds privacy-by-design and human oversight. We align with current guidance (OECD digital government, World Bank GovTech Maturity Index, NIST AI RMF, ISO/IEC 31700, EU AI Act), provide a reference architecture coupling registers and event streams with MLOps and policy-as-code, and define KPIs and a phased rollout. The goal is measurable gains in service quality and trust at lower cost.

1. Context and objective

Governments are moving from “apply and wait” portals to **anticipatory** services that act on life-event data with consent. OECD’s new report documents rapid AI uptake in public service design and delivery, while stressing strong data management and accountability.

2. Proactive, event-driven services

Using authoritative registers and event buses (birth, move, expiry), AI pre-fills dossiers, checks eligibility, and pushes consented offers (renewals, benefits) with explanations and audit trails. Estonia’s program illustrates the model: services triggered by life events, offered proactively across agencies.

3. Risk-based inspections

Risk models prioritize **who to inspect, when, and for what**, across tax, customs, food safety, and licensing. Features combine history, networks, seasonality, and anomalies; outputs must be interpretable for inspectors. Under the **EU AI Act**, many public-sector decision systems fall into “high-risk,” requiring quality data, logging, transparency, and human oversight—raising the bar for governance.

4. Anti-fraud and identity assurance

Supervised, unsupervised, and graph methods detect benefit abuse, duplicate identities, procurement collusion, and chargeback rings. Multi-modal signals (device, document, behavior, biometrics where lawful) feed risk scores with strict thresholds and clear redress paths. OECD finds AI most visible in high-volume service domains, but warns that safeguards are essential to avoid undue burden on citizens.

5. Smart queues and service orchestration

Queueing models and reinforcement learning optimize appointment slots, staffing, and routing across channels (web, call center, service hubs). Objectives: lower wait/abandonment, higher first-contact resolution, and accessibility (priority paths for vulnerable users).

6. Data protection and trustworthy AI

Privacy-by-design must run end-to-end: data minimization, purpose limitation, role-based access, encryption at rest/in transit, and verifiable logs. **ISO/IEC 31700-1** sets high-level privacy-by-design requirements; **NIST AI RMF** provides a lifecycle playbook (govern, map, measure, manage). Together with local law, they anchor controls for high-risk public AI.

7. Reference architecture (registers → models → actions)

[Core Registers] Civil | Business | Property | Vehicles | Benefits

| (schema-governed; immutable, signed logs)

[Event Bus] Life events (birth, move, expiry), transactions, alerts

|

[Feature Store] Consented joins; lineage; retention & purpose tags

|

[Model Layer] Eligibility | Risk/Inspections | Fraud/Graphs | Queues

| (MLOps: versioning, drift, audit, approvals)

[Decisioning] Policies-as-code (rules + thresholds + overrides)

|

[Channels] Portal | Mobile | Contact center | Back-office HMI

|

[Controls] RBAC/ABAC, encryption, DPIA, transparency, redress

8. Phased rollout

Phase 1 — Readiness (4–6 wks). Inventory registers and legal bases; consent flows; baseline KPIs; DPIA; adopt NIST AI RMF artifacts (risk policy, model cards).

Phase 2 — Pilot (8–12 wks). One proactive service (e.g., license renewal) + one risk model (e.g., inspections) with human-in-the-loop, explanations, and appeal workflow.

Phase 3 — Scale (12–20 wks). Add payments anti-fraud; roll out smart queues; publish service/model cards; introduce A/B tests and shadow mode.

Phase 4 — Operations (ongoing). Drift and bias monitoring, retraining cadence, external audits, incident and redress SLAs; align high-risk systems to AI Act obligations.

9. KPIs and value

- **Service quality:** time-to-decision, first-contact resolution, abandonment rate.
- **Efficiency:** cost-to-serve, caseworker productivity, backlog clearance.
- **Integrity:** fraud detection/precision, false-positive rate, recovery amount.
- **Trust:** explanation coverage, appeal turnaround, privacy incident rate.
Benchmarking via the **World Bank GTMI** situates progress across registers, services, and enablers.

10. Risks and mitigations

- **Data misuse / over-collection** → purpose limitation, minimization, retention caps, ISO 31700 privacy-by-design controls.
- **Bias / opacity** → interpretable features, adverse-action notices, counterfactual tests, periodic fairness audits.
- **Over-automation** → human override, escalation paths, sampled manual reviews.
- **Security & integrity** → signed events, immutable logs, red-team fraud scenarios; align high-risk deployments to EU AI Act (data quality, logging, oversight).

Conclusion

AI can make public services **proactive, fair, and cost-effective**—provided risk management, privacy-by-design, and human oversight are first-class design elements. By wiring registers and event streams to interpretable models, MLOps, and robust redress, administrations can scale trustworthy AI that measurably improves outcomes for citizens and businesses. OECD’s latest work, the World Bank GTMI, NIST AI RMF, ISO 31700, and the EU AI Act offer a coherent playbook for this journey

Keywords: *E-government, Proactive services, Risk models, Anti-fraud, Smart queues, Data protection*

Selected references (APA 7th)

- European Union. (2024). *Regulation (EU) 2024/1689—Artificial Intelligence Act* (OJ L 12.7.2024). EUR-Lex.
- International Organization for Standardization. (2023). *ISO/IEC 31700-1: Consumer protection—Privacy by design for consumer goods and services*. ISO. [.](#)
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). NIST.
- OECD. (2025). *Governing with Artificial Intelligence* (chapters on public service design & delivery). OECD Publishing.
- World Bank. (2023). *GovTech Maturity Index (GTMI): Methodology and results*. The World Bank.
- Government of Estonia. (2024). *Proactive government services* (life-event services). Ministry of Economic Affairs and Communications.