

DOI <https://doi.org/10.32782/2956-333X/2026-7-2>

PERSONAL RESPONSIBILITY IN UKRAINE'S MINISTRY OF JUSTICE: A CONCEPTUAL MODEL

Roman M. Roman,

Carpathian Professional College of the University "Ukraine", Khust, Ukraine

<https://orcid.org/0009-0000-1117-0687>

r.romanm1225@gmail.com

Summary. Public institutions frequently state that managers and public servants bear personal responsibility, yet such clauses often fail to show how responsibility should be attributed in multistage, collegial, and digitally mediated decision-making. The aim of this article is to develop a conceptual model of personal responsibility for managers and public servants within the system of the Ministry of Justice of Ukraine and to identify the legal, organisational, human-resource, and digital conditions required for its implementation. The study draws on the Constitution of Ukraine, legislation on civil service, administrative procedure, access to public information, personal data protection, public electronic registers, electronic identification, and performance evaluation, together with scholarship on public accountability, digital government, and algorithmic accountability. The methods include system design, functional modelling, doctrinal legal analysis, risk analysis, and scenario testing. The proposed model is structured as a closed six-link cycle consisting of mandate, decision preparation and adoption, protected digital trace, multi-criteria assessment, proportionate consequence, and organisational learning. Its normative core is the principle of symmetry between lawful authority, available resources and information, controllable risk, and the scope of personal responsibility. For collegial and technology-mediated decisions, the model introduces distributed role attribution while preserving the identifiable contribution of each participant. Practical instruments include a process responsibility passport, a material-decision record, version and approval logs, recorded professional dissent, quality indicators, graduated responses, and mandatory after-action review. Scenario testing demonstrates the model's applicability to drafting normative acts, adopting individual administrative acts, enforcement proceedings, and algorithm-supported decisions. The article argues that digital records should be minimally sufficient, tamper-evident, role-accessible, and retention-limited, while transparency must remain compatible with personal data protection and procedural confidentiality. The novelty of the study lies in integrating legal individualisation, managerial accountability, and digital traceability into a single learning-oriented cycle designed to strengthen responsibility without creating a blame culture and to support consistent institutional improvement over time.

Keywords: accountability, digital traceability, administrative decision-making, public service, organisational learning, role attribution, procedural safeguards, algorithmic governance.

1. Introduction

Personal responsibility becomes a principle of governance only when it influences process design before a violation occurs. A formula stating that a manager or public servant "bears personal responsibility" does not explain which part of collective work the person is responsible for, which resources are available, which risks are under that person's control, how the decision can be explained, or what the organisation will change after an error. In the system of the Ministry of Justice of Ukraine, this problem is intensified by the large number of legal regimes, territorial units, registers, and professional actors.

Digitalisation simultaneously facilitates and complicates the attribution of individual responsibility. An electronic system can accurately record the author of an action, the time, the document version, and the approval route. However, a decision may depend on an automated check, an external register, software configuration, or an artificial intelligence model. In such a situation, the traditional logic that "the person who signs is the person responsible" does not reveal the contribution of the rule designer, data owner, system administrator, and public official. Algorithmic mediation creates a risk of diffusion of responsibility and an illusion of technological neutrality (Busuioc, 2021; Wirtz et al., 2019).

Public accountability theory treats information, discussion, assessment, and consequences as necessary components of a complete accountability process (Bovens, 2007; Brandsma & Schillemans, 2013). At the same time, mechanically increasing transparency does not guarantee better governance: excessive openness may undermine confidentiality, encourage defensive behaviour, and reduce the quality of internal professional deliberation (Bannister & Connolly, 2011). A conceptual model must therefore combine traceability with data minimisation, the public's right to information with protection of participants in the procedure, and individual consequences with analysis of systemic causes.

The Organisation for Economic Co-operation and Development describes digital government as digital by design, data-driven, government as a platform, open by default, user-driven, and proactive (OECD, 2020a). For personal responsibility, these dimensions mean that controls should be embedded in the process, data should have a designated owner, shared components should have clear responsibility for quality, and the user should receive an understandable decision and a route for appeal. Integrity likewise requires systemic management of risks, standards, learning, and response (OECD, 2020b).

The purpose of this article is to develop a conceptual model of personal responsibility for managers and public servants within the system of the Ministry of Justice of Ukraine and to determine the legal, organisational, human-resource, and digital conditions for its implementation. The model is intended to meet four requirements: to establish each person's contribution to a multistage decision; to preserve the institutional responsibility of the public body; to ensure procedural fairness; and to transform consequences into a source of organisational learning. The research hypothesis is that a closed accountability cycle is more effective than isolated control and disciplinary measures.

2. Materials and Methods

The normative corpus included the Constitution of Ukraine, the laws On Civil Service, On Administrative Procedure, On Access to Public Information, On Protection of Personal Data, On Public Electronic Registers, and On Electronic Identification and Electronic Trust Services, as well as the Regulation on the Ministry of Justice of Ukraine and the procedure for evaluating civil servants' performance. These provisions were compared with the Principles of Public Administration and the OECD Public Integrity Handbook (OECD, 2020b; SIGMA, 2023).

System design was used to construct a closed cycle in which the output of each link serves as a verifiable prerequisite for the next. Functional modelling made it possible to distinguish the roles of initiator, drafter, adviser, approver, decision-maker, implementer, controller, and owner of the digital system. Doctrinal legal analysis was applied to the limits of authority, the grounds for consequences, and procedural safeguards. Risk analysis covered role diffusion, retrospective changes to standards, excessive surveillance, automation bias, and blame culture.

The model was tested using four scenarios typical of the justice system: preparation of a normative legal act; adoption of an individual administrative act; implementation of a decision in enforcement proceedings; and the use of an automated check or recommendation algorithm. The scenario testing did not reproduce specific cases and did not contain personal data. For each scenario, the analysis asked whether it was possible to establish the mandate, individual contribution, data used, reasons, assessment forum, possible consequence, and required process change.

The quality criteria for the model were defined as legal certainty, completeness of traceability, proportionality, feasibility, protection of rights, resistance to manipulation, and capacity for learning. The model is considered incomplete if it creates a record without competent assessment, imposes a consequence without a pre-existing standard, personalises responsibility without an adequate mandate, or provides transparency without information protection. A limitation of the study is its conceptual nature; the quantitative effectiveness of the proposed instruments must be established during pilot implementation.

3. Results and Discussion

The proposed model takes the form of a closed cycle: mandate – decision – digital trace – assessment – consequence – learning. Closure means that findings generated through assessment modify the next mandate, regulation, competency requirement, or technical rule. If the cycle ends only with a sanction, the organisation does not eliminate causes. If it ends only with a recommendation that has no responsible owner, change may not occur. Each link must therefore have a defined output, an identifiable personal role, and documentary evidence.

The normative core of the model is the principle of symmetry: the scope of personal responsibility should correspond to the scope of lawful authority, the resources and information available, the degree of control over risk, and the ability to act through due procedure. The constitutional principle of legality prevents responsibility from being created by an internal instruction outside legal competence, while

the individual nature of legal liability requires personal grounds to be established (Verkhovna Rada of Ukraine, 1996). Symmetry does not guarantee a positive outcome, but it makes assessment fairer and more predictable.

The first link is the mandate. It answers who must act, for what purpose, within which limits, and with which resources. For continuing activities, the sources are legislation, the regulation governing the body, the job profile, and internal rules; for a specific task, the source is a resolution or another formal instruction. The mandate should specify the expected result, deadline, limits of discretion, required approvals, access to data, and the method for escalating an obstacle. An oral instruction that materially changes the task or risk should be formally confirmed without delay.

The instrument for this link is a process responsibility passport. It identifies the owner of the end-to-end result and separates individual roles without confusing their subject matter. The process owner is responsible for integrity, deadlines, interaction, and correction of systemic defects; the drafter is responsible for the prepared content; the adviser for the opinion within the relevant professional field; the approver for the defined check; the decision-maker for the final choice; and the implementer for proper execution. The passport should be approved before a specific dispute arises.

The second link is decision preparation and adoption. The Law of Ukraine On Administrative Procedure requires relevant circumstances to be examined, the person concerned to be involved, impartiality and proportionality to be observed, and the administrative act to be reasoned (Verkhovna Rada of Ukraine, 2022). For internal accountability, these requirements are insufficient if the origin of a material position cannot be identified. The model therefore proposes a material-decision record containing the problem, legal basis, factual data, alternatives considered, risks to rights and resources, professional reservations, reasons for the final choice, and the actor accepting the residual risk.

The record should not create a separate bureaucratic document for every standard operation. Materiality criteria include significant impact on individual rights, a new legal approach, high financial or reputational risk, departure from established practice, the use of an automated recommendation, or the overriding of a negative professional approval. For high-volume standard procedures, structured fields and exception controls should be embedded in the information system. This differentiation preserves proportionality in the administrative burden.

Professional dissent is a separate element of the second link. A public servant should be able to record a legal, ethical, technical, or resource-related risk, propose an alternative, and escalate the matter to the appropriate level. A reservation does not create a right to block a lawful decision, but a manager who rejects it accepts responsibility for the corresponding residual risk and should provide reasons for that choice. This protects professional integrity while preserving the manageability of the hierarchy.

The third link is the protected digital trace. Its purpose is to reconstruct a legally significant history rather than to establish total surveillance of an employee. The minimum record should include the identified role, time, version, material amendment, subject of approval, reservation, signature, transfer for implementation, and completion. Legislation on electronic identification provides means to authenticate the actor, while the law on public electronic registers establishes requirements for register information and interoperability (Verkhovna Rada of Ukraine, 2017, 2021).

The quality of the digital trace is determined not by the volume of records but by their evidentiary fitness. A record should be protected against undetected alteration, while corrections should preserve history; access should be granted according to official roles; events should use a consistent time reference and clear semantics; and retention periods should correspond to the purpose and possible appeal periods. The owner of the information system is responsible for technical integrity and access rules but not for the legal substance of every decision. A user is responsible for the accuracy of data entered within the interface and permissions provided.

Openness and personalisation are not identical. The Law of Ukraine On Access to Public Information supports transparency of public bodies, while the Law of Ukraine On Protection of Personal Data requires a lawful purpose and an appropriate processing regime (Verkhovna Rada of Ukraine, 2010, 2011). Public disclosure should cover the information necessary to understand competence, procedure, reasons, and result; internal personal logs should be disclosed only to the extent justified by law and the rights

of participants. Bannister and Connolly (2011) appropriately warn that decontextualised transparency may harm good governance.

For automated and algorithm-supported decisions, the digital trace should additionally record the name and version of the system, data source, role of the algorithm, threshold rule, instances of manual override, and the responsible public official. A system that merely sorts materials has a different influence from a system that provides an automated recommendation or effectively determines the outcome. Busuioc (2021) shows that algorithmic accountability is impossible unless the organisation can explain the role of the system and preserve human competence. A technology supplier cannot replace the public authority as the bearer of obligations towards the individual.

The fourth link is multi-criteria assessment. A single binary evaluation of "completed/not completed" cannot distinguish legality, procedural quality, integrity, performance, and learning behaviour. Five groups of criteria are proposed: legal criteria – competence, procedure, reasoning, and proportionality; temporal criteria – compliance with deadlines and response to delay; performance criteria – achievement of the controllable result; integrity criteria – conflicts of interest, impartiality, and use of resources; and learning criteria – detection of error, reporting, correction, and prevention of recurrence.

The criteria should be established before the assessment period and aligned with the official role. Civil service legislation and the procedure for performance evaluation already provide for tasks and key indicators to be defined (Verkhovna Rada of Ukraine, 2015; Cabinet of Ministers of Ukraine, 2017). The model proposes supplementing them with process-quality indicators without reducing evaluation to a mechanical score. A low number of annulled decisions, for example, may be a positive signal, but without considering case complexity, changes in practice, and access to appeal, it does not prove personal effectiveness.

The assessment forum should correspond to the subject matter. A court or administrative appeal body assesses the legality of an act; a disciplinary body assesses a culpable breach of official duty; a manager assesses organisation and task performance; an anti-corruption unit assesses conflicts of interest and integrity; and a technical audit assesses system integrity. The accountability cube demonstrates the need to balance information, discussion, and consequences (Brandsma & Schillemans, 2013). A single universal controller cannot competently cover all these subjects.

The fifth link is the proportionate consequence. The model distinguishes five types of cause: a good-faith error despite proper process; a deficit of knowledge or skill; an organisational defect; negligence; and an intentional violation. Different responses correspond to these causes: professional review and clarification of the standard; training or mentoring; modification of a regulation, resource, or system; disciplinary proceedings; or referral to the competent authority. Legal qualification should occur only in the procedure established by law.

This approach counteracts blame culture. If every negative outcome triggers personal punishment, employees are encouraged to conceal mistakes, avoid non-standard decisions, and create unnecessary approvals. If consequences are absent even in cases of intentional misconduct, accountability loses credibility. Balance is provided by a pre-existing standard, evidence-based attribution, the right to be heard, a reasoned conclusion, proportionality, and appeal. Acknowledging one's own error and promptly mitigating harm should be treated as positive behaviour, but should not automatically eliminate a legal consequence.

The sixth link is organisational learning. After a significant breach, a successful appeal, a systemic delay, or a near miss, an after-action review should be conducted without duplicating disciplinary proceedings. It should answer what happened; which individual and systemic factors were involved; which controls worked or failed; which rule, process, competence, or technical component should be changed; and who is responsible for the change and by what deadline. The result should be de-identified to the extent necessary for learning by other units.

The cycle is closed when the findings of the review are incorporated into a new mandate, process passport, training programme, control rule, or information system. The manager is responsible for implementing the agreed change, while the process owner is responsible for verifying its effect. Personal responsibility therefore extends not only to the initial error but also to inaction after a reliable signal of systemic risk has been received. This corresponds to the preventive logic of public integrity (OECD, 2020b).

Scenario testing confirmed the functional applicability of the model. In the preparation of a normative act, it distinguishes the policy objective, authorship of the text, legal review, and acceptance of residual risk. In an individual administrative case, it connects the authorised official with evidence, participation of the addressee, and reasoning. In enforcement proceedings, it distinguishes the enforcement officer's own actions from external constraints and technical availability. For algorithmic support, it adds the responsibilities of the data owner, system or model owner, and human decision-maker.

Normative implementation of the model requires the principle of symmetry and procedural safeguards to be embedded in the relevant legal framework. The Regulation on the Ministry of Justice and internal rules should distinguish political, organisational, procedural, and professional responsibility (Cabinet of Ministers of Ukraine, 2014). Special procedures should define criteria for a material decision, professional dissent, and after-action review. An internal act cannot create a new legal sanction, but it can specify managerial and learning responses.

Human-resource support should include competency profiles covering the ability to reason decisions, work with evidence, report risks, use data, and conduct causal analysis. Assessment of managers should include the quality of delegation, response to reservations, correction of systemic defects, and psychological safety for reporting errors. Assessment of public servants should include procedural quality, timeliness, substantiation, and learning behaviour. Responsibility without competency development increases fear rather than capacity.

Digital support should include role-based identification, a log of legally significant events, version control, preservation of reasons, linkage to deadlines, exception notifications, access segregation, and retention controls. The system should not automatically infer culpability from a single indicator. An algorithm may flag a risk or deviation, but the final assessment must be made by a competent person who considers context and the right to explanation. This preserves the human-centred character of digital government.

Phased implementation should begin with one process that has a high impact on individual rights and one internal managerial process. The first stage should describe roles and baseline indicators; the second should establish the digital trace and a channel for professional reservations; the third should test assessment and after-action review; and the fourth should independently evaluate the results. Pilot criteria should focus not on the number of persons sanctioned but on fewer undefined handovers, stronger reasoning, timely correction, and a reduction in recurring errors.

4. Conclusions

A conceptual model of personal responsibility for managers and public servants within the system of the Ministry of Justice of Ukraine has been developed as a closed six-link cycle consisting of mandate, decision preparation and adoption, protected digital trace, multi-criteria assessment, proportionate consequence, and organisational learning. Its difference from a conventional disciplinary approach lies in embedding responsibility into the governance process before a violation occurs and in requiring findings to be fed back into the next cycle.

The principle of symmetry requires personal consequences to be aligned with lawful authority, available resources, accessible information, controllable risk, and due procedure. For multistage, collegial, and algorithm-mediated decisions, distributed role attribution is proposed: each participant is responsible for a defined subject, while the public authority retains its external obligation towards the individual. A signature is important but is not the sole evidence of personal contribution.

The practical toolkit of the model consists of a process responsibility passport, a material-decision record, recorded professional dissent, version and approval logs, a profile of quality indicators, graduated consequences, and after-action review. The digital trace should be minimally sufficient, protected against undetected alteration, accessible by role, and limited by retention periods. An automated system may support analysis but must not replace a competent assessment forum or the individual's right to provide an explanation.

Implementation requires coordinated legal, organisational, human-resource, and digital measures. Pilot implementation should be evaluated by the quality of role allocation, the quality of reasoning, timely correction, and the reduction of recurring errors rather than by the number of sanctions imposed. A promising

direction for further research is empirical testing of the model across different processes within the Ministry of Justice system and identification of the minimum set of digital events sufficient for fair attribution without excessive administrative burden.

References:

1. Bannister, F., & Connolly, R. (2011). The trouble with transparency: A critical review of openness in e-government. *Policy & Internet*, 3(1), 1-30. <https://doi.org/10.2202/1944-2866.1076> [in English].
2. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), 447-468. <https://doi.org/10.1111/j.1468-0386.2007.00378.x> [in English].
3. Brandsma, G. J., & Schillemans, T. (2013). The accountability cube: Measuring accountability. *Journal of Public Administration Research and Theory*, 23(4), 953-975. <https://doi.org/10.1093/jopart/mus034> [in English].
4. Busuioc, M. (2021). Accountable artificial intelligence: Holding algorithms to account. *Public Administration Review*, 81(5), 825-836. <https://doi.org/10.1111/puar.13293> [in English].
5. Cabinet of Ministers of Ukraine. (2014). Pro zatverdzhennia Polozhennia pro Ministerstvo yustytzii Ukrainy [On approval of the Regulation on the Ministry of Justice of Ukraine] (Resolution No. 228). <https://zakon.rada.gov.ua/go/228-2014-п> [in Ukrainian].
6. Cabinet of Ministers of Ukraine. (2017). Pro zatverdzhennia Poriadku provedennia otsiniuvannia rezultativ sluzhbovoi diialnosti derzhavnykh sluzhbovtiv [On approval of the procedure for evaluating the results of civil servants' performance] (Resolution No. 640). <https://zakon.rada.gov.ua/go/640-2017-п> [in Ukrainian].
7. *The OECD digital government policy framework: Six dimensions of a digital government*. OECD Public Governance Policy Papers, 2. <https://doi.org/10.1787/f64fed2a-en> [in English].
8. *OECD public integrity handbook*. OECD Publishing. <https://doi.org/10.1787/ac8ed8e8-en> [in English].
9. *The principles of public administration*. OECD. https://www.sigmaweb.org/en/publications/2023/11/the-principles-of-public-administration_5e68f805.html [in English].
10. 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> [in English].
11. Verkhovna Rada of Ukraine. (1996). Konstytutsiia Ukrainy [Constitution of Ukraine] (No. 254k/96-VR). <https://zakon.rada.gov.ua/go/254к/96-вр> [in Ukrainian].
12. Verkhovna Rada of Ukraine. (2010). Pro zakhyst personalnykh danykh [On protection of personal data] (Law of Ukraine No. 2297-VI). <https://zakon.rada.gov.ua/go/2297-17> [in Ukrainian].
13. Verkhovna Rada of Ukraine. (2011). Pro dostup do publichnoi informatsii [On access to public information] (Law of Ukraine No. 2939-VI). <https://zakon.rada.gov.ua/go/2939-17> [in Ukrainian].
14. Verkhovna Rada of Ukraine. (2015). Pro derzhavnu sluzhbu [On civil service] (Law of Ukraine No. 889-VIII). <https://zakon.rada.gov.ua/go/889-19> [in Ukrainian].
15. Verkhovna Rada of Ukraine. (2017). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On electronic identification and electronic trust services] (Law of Ukraine No. 2155-VIII). <https://zakon.rada.gov.ua/go/2155-19> [in Ukrainian].
16. Verkhovna Rada of Ukraine. (2021). Pro publichni elektronni reiestry [On public electronic registers] (Law of Ukraine No. 1907-IX). <https://zakon.rada.gov.ua/go/1907-20> [in Ukrainian].
17. Verkhovna Rada of Ukraine. (2022). Pro administratyvnu protseduru [On administrative procedure] (Law of Ukraine No. 2073-IX). <https://zakon.rada.gov.ua/go/2073-20> [in Ukrainian].