Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

IMPROVING THE ADMINISTRATIVE AND LEGAL MECHANISMS OF INTERAGENCY INFORMATION EXCHANGE IN PUBLIC ADMINISTRATION

Tursunov Firdavs Shokir o‘g‘li
Master’s Degree Student at the Law Enforcement
Academy of the Republic of Uzbekistan
Phone: +998900884884
https://doi.org/10.5281/zenodo.23230566

Abstract

This article provides a comprehensive study of the administrative and legal nature, institutional foundations, and practical mechanisms of interagency information exchange in the context of digital public administration. As public administration processes become increasingly digitalized, the integration of information resources and information systems of public authorities is becoming an important prerequisite for improving the efficiency of public services, reducing the administrative burden, eliminating the repeated collection of information, and strengthening the information support of administrative decision-making.

The study analyzes the Laws of the Republic of Uzbekistan “On Electronic Government,” “On Personal Data,” and “On Cybersecurity,” legislation governing administrative procedures, regulatory legal acts regulating electronic cooperation between public authorities, as well as regulatory developments aimed at the digitalization of public services in 2025–2026. Particular attention is paid to the extent to which the existing legal and institutional framework ensures lawful, secure, reliable, and efficient exchange of information between public authorities.

The article conceptualizes the administrative and legal mechanism of interagency information exchange as a combination of three interrelated levels: normative and legal, institutional, and technological-procedural. In addition, the study examines the legal basis for information exchange, the purposes of data use, the delimitation of powers and responsibilities, the reliability and relevance of data, information security, the protection of personal data, the use of interagency integration platforms, liability for data quality, and issues of administrative oversight.

The study also substantiates the need to further improve the administrative and legal mechanisms governing interagency information exchange by strengthening institutional coordination, establishing clear rules for data access and responsibility, ensuring the traceability and reliability of exchanged information, and developing effective mechanisms for protecting the rights and legitimate interests of individuals. The proposed approaches are aimed at ensuring a balance between the efficiency of digital public administration, the lawful use of information resources, and the protection of individual rights.

Keywords: public administration, information exchange, administrative law, electronic government, digital government, interagency electronic cooperation, interoperability, personal data, information security, data governance.

INTRODUCTION

Digitalization is significantly changing the ways in which information is used in public administration. Whereas public authorities previously collected, stored, and processed data mainly

independently, today the possibility of interagency data use is expanding through the integration of various information systems. Such a system makes it possible to reduce the repeated submission of identical documents by citizens and businesses when receiving public services, shorten service delivery periods, and provide administrative decision-making with reliable information.

In Uzbekistan, the legal foundations for electronic cooperation between public authorities have been established. In particular, the Law "On Electronic Government" establishes the general framework for interagency electronic cooperation. Resolution No. 516 of the Cabinet of Ministers dated September 20, 2022 establishes the procedure for electronic cooperation and information exchange through the Interagency Integration Platform. In addition, subsequent regulatory documents aimed at the digitalization of public services have expanded the scope of the use of the "Digital Government" system. At the same time, the technical integration of information systems does not in itself mean that the use of such data is legally justified. Therefore, it is important to study interagency information exchange not only as a technical process but also as an administrative and legal process.

From the perspective of the administrative and legal nature of interagency information exchange, interagency information exchange may be defined as the process by which public authorities and organizations obtain, provide, and process information in accordance with the procedure established by law for the exercise of their powers, the provision of public services, and the performance of administrative functions. Its main elements include:

- entities providing and using information;
- the competence of the relevant public authority;
- the legal basis for information exchange;
- the purpose of using the data;
- the content and volume of the data;
- technical means of exchange;
- information security;
- liability and oversight.

Therefore, it is insufficient to assess interagency information exchange merely as the electronic transmission of data. It is based on the interrelationship of legal, institutional, procedural, and technological elements.

One of the most important requirements in interagency information exchange is to determine the legal basis and purpose for obtaining information. For example, the fact that information concerning a citizen is available to one public authority does not grant another public authority an unrestricted right to use that information. The receiving authority must be able to substantiate why it requires such information and demonstrate that it has the legal authority to obtain it. From this perspective, it would be appropriate to introduce the principle of "competence-based information exchange." According to this principle, a public authority's right to obtain information should arise not from its general status as a public authority, but from a specific administrative function and a specific statutory or regulatory legal competence.

The protection of personal data is of particular importance in interagency information exchange. The Law "On Personal Data" establishes the legal foundations for the collection, storage, use, and protection of such data. Therefore, when exchanging data between public authorities, it is necessary to clarify the following: the existence of a legal basis for obtaining the information; the specific

administrative purpose for which the information is obtained; whether the volume of the requested information is proportionate to that purpose; and whether the transfer and storage of the information comply with security requirements. These requirements serve to ensure a balance between the information needs of public authorities and the citizen's right to protection of personal data.

Another important issue in interagency information exchange is data quality. Information may be transmitted technically quickly and completely; however, if the information itself is outdated or inaccurate, its use may result in an incorrect administrative decision.

Therefore, it is necessary to clearly identify the entities responsible for the accuracy, completeness, relevance, updating, and provenance of data. In this regard, it is proposed to strengthen the institutional accountability mechanism for data quality. For each important government database, a public authority or public official should be designated as responsible for updating data, correcting errors, and ensuring its reliability.

International practice also demonstrates that interoperability should not be understood merely as a technical connection between information systems. According to the OECD's Digital Government Outlook 2026, interoperability is increasingly viewed as a system-level property that must be continuously maintained through governance, common standards, reliable reference data, clearly defined institutional responsibilities, and mechanisms for accountability. The OECD also emphasizes that data quality, interoperability, and data reuse constitute important foundations for effective data-driven government. In this regard, the development of interagency information exchange requires not only technological compatibility but also a coherent governance framework defining who may access data, for what purpose, under what legal basis, and who bears responsibility for the consequences of its use.

Another relevant principle is the "once-only" principle, according to which citizens and businesses should not be required to repeatedly provide the same information to different public authorities where such information is already lawfully available within government information systems. The practical implementation of this principle requires clearly defined legal grounds for data reuse, appropriate data-protection safeguards, interoperable information systems, and mechanisms for verifying the accuracy of previously collected information. Consequently, the once-only principle should be regarded not merely as a technological solution, but as an administrative and legal principle aimed at reducing administrative burdens and improving the quality of public services.

In this context, the concept of authoritative data sources is also important. Where several public authorities rely on the same categories of information, the identification of an official and trusted primary source can reduce discrepancies between databases. Such an approach makes it possible to establish which institution is responsible for maintaining particular data, correcting errors, and ensuring their continued relevance. It can therefore serve as an additional institutional basis for determining liability when inaccurate information leads to an adverse administrative consequence.

It is also important to distinguish between data access and data entitlement. Technical access to an information system should not automatically create a legal entitlement to use all information contained in that system. Access should be structured according to the user's competence, the purpose of processing, the category of information, and the level of sensitivity of the data. Such differentiation is particularly important where personal, financial, social, or other legally protected information is processed.

Another important direction is the development of a risk-based approach to interagency data exchange. Not all categories of information create the same level of risk. The exchange of publicly available or low-risk administrative data may require relatively simple controls, whereas the exchange of sensitive personal or financial information should be subject to enhanced authentication, authorization, logging, security, and oversight requirements. A differentiated approach of this kind would allow public authorities to combine administrative efficiency with an appropriate level of protection of legally protected information. Strengthening oversight over the exchange of information between public authorities also requires the development of a digital audit trail mechanism.

The system should record, for each information request:

- who submitted the request;
- on behalf of which authority the request was made;
- what information was obtained;
- when the information was used;
- what legal basis was relied upon.

Such a mechanism serves not only as a technical control instrument but also as an administrative means of verifying the legality of information use.

The importance of traceability is further reinforced by international practice. The OECD notes that modern data-sharing systems increasingly rely on mechanisms that allow exchanges to be authenticated, authorized, and traced. In some interoperability models, access to data through APIs is linked to authorization mechanisms that create records of data exchanges. This demonstrates that the audit trail should be considered not simply as a cybersecurity feature, but as an element of administrative accountability capable of establishing the circumstances of data access and use.

PROPOSALS

Improving the effectiveness of interagency information exchange should not be

limited to the development of technological infrastructure. The legal grounds for obtaining, using, processing, and providing information to another public authority must be clearly established. From this perspective, the following proposals may be put forward.

First, it is necessary to establish unified legal standards for interagency information exchange. Under existing procedures, the legal basis for information exchange, the composition of data, the purpose of use, and the responsible entities may in some cases be defined differently. Therefore, it would be appropriate to introduce a unified administrative and legal standard establishing general requirements for interagency information exchange. It should clearly specify the grounds for requesting information, the scope of its use, the retention period, data security requirements, and liability. Such a standard should also establish a minimum set of mandatory metadata accompanying each significant data exchange, including the source of the information, the date of its update, the legal basis for access, the purpose of processing, and the responsible institution. This would increase the traceability and legal certainty of interagency data flows.

Second, the principle of “competence-based access” should be strengthened in information exchange.

The fact that a public authority is technically connected to an information system should not mean that it has the right to use the information contained therein for any purpose. The use of each category of

data should be linked to the relevant authority's legally established competence and a specific administrative purpose. This approach would reduce the risk of excessive data collection and unauthorized use.

In addition, access rights should be differentiated according to the functions performed by specific officials or institutions. The principle of least privilege should be applied so that users receive only the level of access necessary to perform their legally defined functions.

Third, it is proposed to clearly establish institutional responsibility for data between public authorities. The institution that creates and maintains the data should be responsible for its relevance, completeness, and accuracy, while the institution using the data should be responsible for its lawful and purpose-specific use. This would provide a clear legal solution to the question: "Who is responsible if the data are incorrect?"

It is also advisable to distinguish between responsibility for data quality and responsibility for data use. Such differentiation would prevent responsibility from being transferred indefinitely between institutions and would allow an error to be traced to the stage at which it actually occurred.

Fourth, it is necessary to develop a digital audit trail as a mandatory element of state information systems. It should be electronically recorded who accessed particular information, when, on what legal basis, and for what purpose. Such a mechanism would make it possible not only to identify unlawful use but also to ensure accountability in the activities of public authorities and establish an evidentiary basis when disputes arise. The audit trail should be protected against unauthorized alteration or deletion and should remain available for the period necessary to ensure legal accountability, security, and administrative review.

Fifth, the practice of repeatedly requesting information should be gradually reduced. If information provided by a citizen is already available within the information systems of public authorities, another public authority should not be permitted to request the same information again, provided that its reuse has an appropriate legal basis. For this purpose, it would be appropriate to systematically apply the "once-only" principle not only to public services but also to interagency administrative procedures.

The implementation of this principle should, however, be accompanied by safeguards ensuring that information is reused only for legally permissible purposes and that citizens retain effective means of correcting inaccurate information.

Sixth, the exchange of personal data should be organized according to the principle of the "minimum necessary data." The ability of a public authority to obtain information that is not necessary for the performance of an administrative function should be restricted. This would not only protect the inviolability of private life but also reduce the risks arising from excessive accumulation of data within information systems. The principle should be operationalized through purpose limitation, data minimization, differentiated access rights, and technical controls that prevent the retrieval of data exceeding the legally defined purpose.

Seventh, it is necessary to strengthen the legal protection of citizens in data exchange. A citizen should have the opportunity to know which public authorities have used information concerning them, the legal basis for such use, and, where appropriate, the purpose for which the information was used. Where a citizen's rights or legitimate interests are violated due to inaccurate information, effective mechanisms should exist for correcting the data and reviewing the administrative decision. In this regard, a citizen-oriented notification mechanism could be introduced for significant categories of personal data

processing. Such a mechanism would enhance transparency and enable individuals to identify and challenge unlawful or inaccurate processing.

Eighth, interagency information exchange should be developed not merely as technical integration but as a unified governance model. It is proposed to establish a system operating according to the following sequence:

legal basis → competence → purpose → scope of data → secure integration → audit → accountability.

This model would serve to harmonize technological capabilities with administrative and legal requirements.

Ninth, a unified classification of data and interoperability standards should be developed. For effective interagency information exchange, public authorities should use common definitions, data formats, identifiers, metadata, and technical standards. Differences in terminology and data structures between institutions can create inconsistencies even where the underlying information is identical.

Therefore, the development of common data standards and interoperable interfaces should form part of the administrative governance framework rather than being treated exclusively as a technical matter. The establishment of authoritative reference data and shared registers would further reduce duplication and inconsistencies between government databases.

Tenth, the concept of “data provenance” should be incorporated into interagency information governance. For legally significant data, it should be possible to determine where the information originated, when it was created or updated, which institution modified it, and through which system it was transferred. Recording data provenance would make it possible to reconstruct the history of information and identify the source of an error when an administrative decision is challenged.

This is particularly important where administrative decisions are based on data received automatically from several interconnected government systems. In such circumstances, the legal reliability of the final decision depends not only on the existence of the information but also on the ability to establish its origin and transformation history.

Eleventh, a risk-based model for interagency information exchange should be introduced. Different categories of information should not necessarily be subject to identical access and security requirements. Information involving sensitive personal, financial, health-related, or other legally protected data should be subject to enhanced authorization, authentication, encryption, logging, and oversight requirements. At the same time, lower-risk administrative information may be exchanged through simplified procedures where legally permissible. Such differentiation would make it possible to avoid both excessive restrictions on legitimate data exchange and insufficient protection of sensitive information.

Twelfth, mechanisms for measuring the effectiveness of interagency information exchange should be established. The effectiveness of information exchange should not be assessed solely by the number of integrated systems or the volume of data transmitted. It should also be evaluated through indicators such as the reduction of repeated requests to citizens, reduction of administrative processing time, accuracy of data, number of corrected data errors, number of unauthorized access incidents, compliance with legal access requirements, and the effectiveness of mechanisms for correcting inaccurate information. Such indicators would allow digital government reforms to be evaluated not merely in terms of technological implementation but also in terms of their actual administrative and legal outcomes.

Overall, the administrative and legal modernization of interagency information exchange should be based on the principle that data interoperability must serve the lawful and efficient exercise of public authority while remaining subject to transparency, accountability, information security, and the protection of individual rights. Accordingly, the development of a unified legal and institutional framework for interagency data exchange can become an important foundation for the further transition of Uzbekistan toward a data-driven, proactive, and human-centred model of digital public administration.

Conclusion

Interagency information exchange is increasingly becoming an essential component of digital public administration. Although the principal legal and technological foundations of this area have been established in Uzbekistan, there remains a need to further improve the legal, institutional, and procedural mechanisms governing information exchange.

The study demonstrates that effective information exchange cannot be ensured solely through the technical interconnection of government bodies' information systems. To this end, issues concerning the authority to obtain data, the purpose of its use, data quality, security, oversight, and accountability should be regulated within a unified system. In this regard, the proposed model of interagency information exchange — "legal basis → competence → purpose → scope of data → integration → audit → accountability" — may contribute to establishing an integrated approach to the regulation of these relations. As a result, interagency information exchange can develop not merely as a technological instrument for accelerating public services, but as an administrative and legal institution that ensures lawful, secure, transparent, and accountable public administration.

References

1. Law of the Republic of Uzbekistan "On Electronic Government," No. O'RQ-395, December 9, 2015.
2. Law of the Republic of Uzbekistan "On Personal Data," No. O'RQ-547, July 2, 2019.
3. Law of the Republic of Uzbekistan "On Cybersecurity," No. O'RQ-764, April 15, 2022.
4. Decree of the President of the Republic of Uzbekistan No. PF-6191, March 23, 2021.
5. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 516, September 20, 2022.
6. Decree of the President of the Republic of Uzbekistan No. PF-157, September 8, 2025.
7. Decree of the President of the Republic of Uzbekistan No. PF-6079, October 5, 2020.
8. OECD. Digital Government Outlook 2026. OECD Publishing, 2026.
9. United Nations. UN E-Government Survey 2024. New York, 2024.
10. OECD. Recommendation of the Council on Enhancing Access to and Sharing of Data. OECD/LEGAL/0463.
11. OECD. Recommendation of the Council on Human-Centred Public Administrative Services. 2024.