TERMS OF REFERENCE

for developing the e-Contravention Case Management System within the Ministry of Internal Affairs

Chisinau 2023

Contents

Introduction

An effective, professional and accountable law enforcement system is an important element for sustainable development. Having recognized the importance of this, the Government of the Republic of Moldova has been engaged since 2010 in a comprehensive reform of its internal affairs and law enforcement systems. The Strategy for Internal Affairs Development for 2022-2030 places particular emphasis on advancing structural change in the field of internal affairs, aiming to build by 2030 a modernized and resilient internal affairs system capable of responding promptly and professionally to the needs of the people it serves. Digitization is one of the key factors supporting these efforts. Digital transformation is essential for the police service to remain relevant, effective and responsive in its approach to protecting and serving the public. Digital transformation has the potential to streamline every part of the policing process, changing the way police work, leverage data, exploit available technologies, collaborate with partner organizations, and organize themselves.

As part of its mandate to maintain public order and safety, the police is the main law enforcement agency responsible for detecting and investigating offences. To date, although efforts have been made to digitize the contravention proceedings, all activities carried out by the competent authorities are paper-based. The documentation of the offence is carried out on paper, with the involvement of the human factor (the reporting officer, the offender, etc.), through the accumulation of material evidence, which is likely to be compromised by lack of knowledge, negligence or malice, creating imminent risks that the report of the offence will be annulled by the court for reasons other than those relating to the legality of the decision to impose a penalty. This state of affairs affects both the operational performance of the Ministry of Internal Affairs in the area of the contravention proceedings and the image of the institution.

Currently there is no electronic case management system capable of assisting the reporting officer in the procedural actions taken by the officer, to ensure the follow-up of the execution of the tasks within the deadlines, to provide timely, complete and truthful information to support the decision-making process, to facilitate collaborative work between different participants in the process for a prompt response to contravention cases. The IT solution owned by the MIA, which ensures the maintenance of the contravention register (AIS REC), is outdated and unscalable. The application uses outdated proprietary technology, has architectural flaws that make it vulnerable to security risks and lacks scalability.

Recognizing the importance of digital transformation in ensuring effective and transparent policing and the delivery of justice for all, the UNDP project "Supporting e-transformation of policing processes related to contravention cases" aims to create the enabling conditions and support the capacity development (at managerial and user level) needed to modernize police operations in contravention cases. Building on MIA's aspirations to digitize internal processes and improve the quality of service delivery, the project will strengthen institutional capacities, facilitate inter-institutional dialogue and interoperability, update (to the extent necessary) the regulatory framework and develop a modern and scalable software solution to enable an environment to foster next generation police operations, supported by skills, knowledge and tools in line with modern-style policing concepts.

The achievement of the overall objective of the Project is to be realized with the commitment of the Ministry of Internal Affairs, the General Inspectorate of Police, the e-Government Agency and other stakeholders in the digitization of processes related to contravention cases, to ensure the development and implementation of the electronic contravention case management system. The new software solution will equip the police service with digital tools to support more efficient and transparent work across the public safety system, while taking advantage of the opportunities offered by digital technologies. It will ensure increased quality and simplify the

work of the police service and other public officials in contravention cases by eliminating or significantly reducing the flow of paper documents used or produced in contravention proceedings.

1. Procurement background

By providing financial support for the development of the e-Contravention Case Management System software solution, the Donor aims to create a high-performance, scalable and sustainable tool that will be used by all competent authorities to resolve contravention cases.

Taking into account the complexity of the area to be automated (the contravention proceedings and related activities) and the fact that the workflows for all authorities competent to deal with contravention cases are to be digitized, each of them having its own specificity, the Donor together with the Beneficiary (Ministry of Internal Affairs of Moldova) agreed on the development and implementation of the software solution in stages.

In the first stage, the activities of the General Police Inspectorate of the Ministry of Internal Affairs of Moldova in the management of contravention and related cases will be digitized.

In this regard, the Donor contracted the implementation unit of the UNDP project "Supporting e-transformation of policing processes related to contravention cases" to organize the procurement and provide support to the Beneficiary in the process of setting the task, organizing the development work, implementation and post-implementation support, as well as developing the internal capacities of the Beneficiary to e-transform the contravention proceedings.

2. Procurement purpose

The immediate purpose of the procurement is to purchase services for the design, development, configuration and implementation of the e-Contravention Case Management System software solution in accordance with the functional and non-functional requirements specified in Annex A "Terms of reference for the development of the e-Contravention Case Management AIS within the Ministry of Internal Affairs".

3. Procurement object

The Ministry of Internal Affairs and the UNDP project "Supporting e-transformation of policing processes related to contravention cases" are interested in identifying an information technology service provider capable of proposing an experienced team to develop the e-Contravention Case Management AIS based on the Agile methodology in accordance with the functional and non-functional requirements described in Annex A "Terms of reference for the development of the e-Contravention Case Management AIS within the Ministry of Internal Affairs".

The e-Contravention Case Management AIS is to be implemented by a competitive team of specialists who meet the requirements specified in Chapter 9 of these specifications. The specialists proposed by the tenderers must be available full-time during the project activities (depending on the project stage, the specialists assigned to the specific stage activities must work exclusively for the e-Contravention Case Management AIS and must not be assigned in parallel to other projects of the developing company) so that the activities in the implementation plan run without interruptions.

The effort required for the design, development and implementation of the e-Contravention Case Management AIS is estimated at 2100 man/days and carried out by 13 key experts according to the estimates stipulated in Table 1 of Chapter 10 of these specifications. The development and implementation period is 18 calendar

months during which the developing company will ensure the availability and involvement of the requested experts.

In addition to the design, development and implementation of the e-Contravention Case Management AIS, part of the original contract is to provide warranty, maintenance and support services for the applications of the computerized system provided for a term of 12 months from the date of final acceptance of the computerized system. Part of the maintenance and support services is the provision by the provider of 100 man-days of development services. These development services do not cover the removal of shortcomings and errors related to the developed functionalities.

The estimates stipulated in Table 1 of Chapter 10 are preventive, so that depending on the evolution of the project the planned effort of some categories of experts may be allocated to others but will not exceed the total amount of 1820 man-days.

4. Development approach

The development of the solution will follow the principle of iterative and agile development.

As there are several methodologies for agile software development and to avoid misunderstandings, this section provides key principles to be followed in the design, development and implementation of the IT solution.

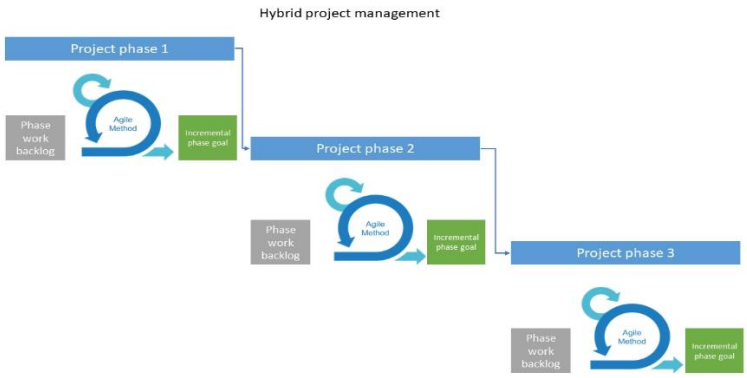
Detailed requirements regarding project management processes and project milestones are presented in Annex B "Requirements for the implementation of the e-Contravention Case Management System". The following is a summary of the approach for the project management process for the development of the e-Contravention Case Management System software solution:

~~1~~ 4.1. Iterative development

Unlike the waterfall development approach, the solution will be developed in iterations called *sprints*. This means that the implementation of system functionality will be done in stages, with some modules in production while others are still under development. The priority of the tasks to be included in a sprint will be determined by the Beneficiary. The duration of the sprint will be determined by the Beneficiary together with the Software Solution Provider.

4.2 ~~1~~. Hybrid approach for development

Agile principles will be applied in the development process. The Agile methodology promotes an iterative and incremental approach to software development. The schematic development of a software product according to the Agile methodology is shown in the figure below.



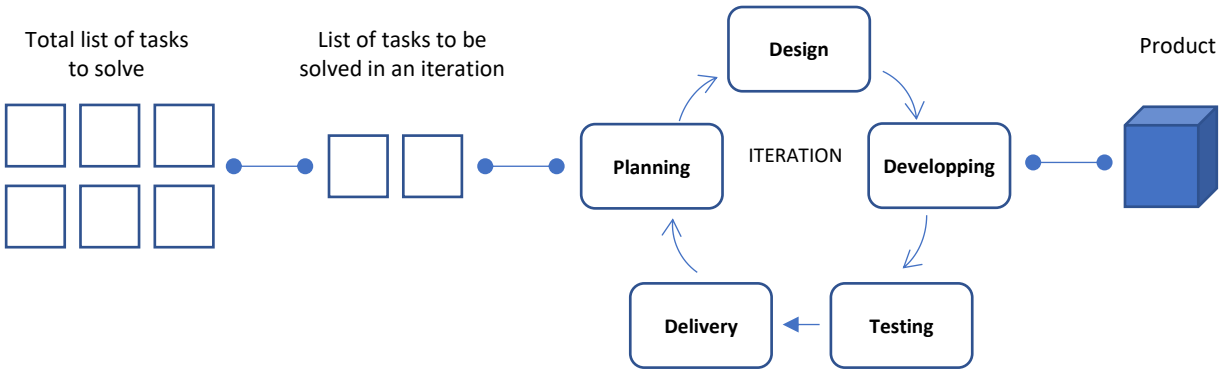


Figure 1. Indicative description of the Hybrid development cycle/process.

Generally speaking, software development according to the Hybrid approach for project implementation involves the following stages (phases):

1. Project initiation: At this stage, arrangements are made for the organization of the project, experts are appointed, the project management organization chart is established, the Project Initiation Document is drafted and agreed with the Beneficiary.
   The objectives and high-level vision of the product to be developed are concretized, the project plan is drawn up, priorities are set and available resources are assessed.
   The requirements for the project initiation stage are presented in Annex B chapterB.3.
2. Project analysis and definition (Product Discovery): At this stage, starting from the generic requirements set out in this specification, the Provider will carry out a detailed analysis of the automation needs and agree with the Beneficiary the *solution backlog (total list of tasks to be solved).*
   The identified requirements included in the backlog are detailed and clearly defined so that they can be understood by the Beneficiary and estimated by the development team. Each requirement is described in user terms (user story) and includes acceptance criteria, initial estimates of required resources and other details.
   Once requirements are detailed and estimated, they are prioritized. The beneficiary prioritizes the requirements in the backlog.
   The beneficiary is free to manage its backlog, adding, deleting or changing the order of items in the backlog as it wishes provided that they fall within the functional scope defined in the specification.
   The detailed requirements for the analysis and definition stage of the project are presented in Annex B Chapter B.4.1.
3. Sprint Planning: This stage involves selecting priority requirements from the product backlog, setting objectives for each sprint and estimating the effort required to implement them. At the beginning of each sprint, the most important items that fit into a sprint are selected and a sprint backlog is created from them. The items in this sprint backlog are further detailed by the Provider, coordinated with the Beneficiary to approve the implementation model and distributed to the developers for implementation. The sprint backlog does not change during the sprint development process.
   The detailed requirements for the sprint planning stage are given in Annex B Chapter B.4.2.
4. Sprint implementation: The joint development team (Provider and Beneficiary specialists) works during a sprint to implement the priority requirements established in the sprint planning. At this stage, the requirements are broken down into smaller tasks and assigned to team members for implementation. Close

communication and collaboration between team members is essential to ensure progress and resolve any issues that arise.

Each sprint ends with a functional product, which is presented to the Beneficiary for acceptance on the last day(s) of the sprint. The functional product will meet the agreed criteria. The delivered product shall be fully functional and tested, accompanied by relevant unit tests, accompanied by relevant documentation if applicable, full source code provided, etc.

The detailed requirements for the sprint planning stage are given in Annex B Chapter B.4.3.

5. Sprint Retrospective: At the end of each sprint, the Provider carries out an analysis of the objections and additional requirements formulated by the Beneficiary in order to complete the backlog. New requirements/functionalities/features are introduced into the backlog after coordination with the Beneficiary. As the introduction of new requirements/functionalities/characteristics may influence the order of priorities all changes to the backlog are coordinated with the Beneficiary.
6. The detailed requirements for the sprint planning stage are presented in Annex B Chapter B.4.3.

Other aspects of organizing the process according to Agile:

- If the deliverables contain defects for reasons not attributable to the Beneficiary, the Provider will remove them without any schedule changes or costs, including possible visits to the Client.
- Functional deliverables resulting from different sprints may be combined at the discretion of the Beneficiary into a production release. Any incidents reported by the Beneficiary after release will be handled by the Provider in accordance with the Service Level Agreements (SLA) defined in Annex B, chapter3.3. The level of services related to e-Contravention Case Management System (service level).
- In order to ensure timely delivery of products by the development team, a representative of the Beneficiary, usually called "*Product Owner*" in Agile methodologies, will be permanently available to the team to answer questions from the team, thus avoiding slowing down the development and implementation process.
- The Provider will have in the project team people in the role of "*Business Analyst*" who will perform all the analysis, detail design and coordination of the implementation solution with the Beneficiary. The Business Analyst will be responsible for the initial development of the backlog of the e-Contravention Case Management System, coordinating it with the "*Product Owner*" to establish development priorities.
- *The Business Analyst* together with the development team will analyze the area under automation and propose optimal implementation solutions. The Beneficiary will ensure the correct understanding of the requirements towards the solution and will guide the Provider in the design and implementation process of the computerized system.
- The Provider together with the Beneficiary will regularly update the product backlog to reflect the prioritized list of desired functionalities to be implemented.

4.3 2. Beneficiary involvement

Unlike the waterfall model commonly used in the procurement and implementation of government IT systems, the person designated by the Beneficiary - the "*Product Owner*", will be heavily involved in the development process. The Product Owner will be permanently available to answer clarification questions from the development team, thus avoiding complex and formal communication within the project. In order to get a working product at the end of the sprint, it is extremely important that the team has all the necessary information at the right time.

The responsibilities of the Product Owner are described in Chapter 8.

In accordance with the principles of Agile project management methodology, the Beneficiary will develop the Product Vision Statement and Product Roadmap to monitor progress and ensure proper product development.

4.4 ~~3~~. Warranty

The developed solution will have a 12-month warranty. The warranty period starts after the final production release of the e-Contravention Case Management System. During the warranty period the Provider will eliminate all identified defects.

The requirements for warranty, maintenance and post-implementation support are described in Annex B, Chapter3.

5. Expected deliverables

As part of the activities required to meet the objectives stipulated in this specification the Provider shall provide the following deliverables:

1. High-level architecture document of the e-Contravention Case Management System (e-Contravention Case AIS Concept). The Provider will develop a high-level architecture document of the future IT solution including the main implementation aspects (implementation objectives, architecture, technology stack, deployment infrastructure, functional components, mock-ups of the main interfaces, etc.). Based on the High-level Architecture Document approved by the Beneficiary the development and implementation sprints of the e-Contravention Case Management System will be started.
2. A fully functional information system (e-Contravention Case Management System) in accordance with the functional and non-functional requirements defined in Annex A "Terms of Reference for the development of the e-Contravention Case Management System" within the Ministry of Internal Affairs", including:
    - source code, third-party libraries and tools, licenses, if applicable.
3. Initial data population and data migration from the REC and RAR AIS systems into the e-Contravention Case Management System.
4. Technical documentation and end-user documentation prepared in accordance with the Beneficiary's requirements contained in Annex B.
5. Training sessions and materials developed in accordance with the Beneficiary's requirements set out in Annex B.
6. Continuity (maintenance) plan for the e-Contravention Case Management System

6. Reporting requirements

All the reports specified in Annex B “Requirements for implementation of the e-Contravention Case Management System” and “Requirements for warranty, maintenance and post-implementation support” will be presented during the activity, such as:

1. Reports related to the development and implementation stage of the e-Contravention Case Management System:
    - Project Initiation Document (PID);
    - Project Discovery and Project Backlog Definition Report;
    - Sprint Plan, which includes the list of tasks and their priorities (Sprint Backlog), resources the Provider expects from the Beneficiary and/or actions to be taken by the Beneficiary;
    - Weekly project progress reports and project records maintained and updated as per the Project Initiation Document

- End Sprint Reports including description of achieved results and retrospective report;
- Stage Completion Reports including: overview of completed stage, presentation of project plan for the next period, risk analysis, project problem setting, project quality level record
- Exception reports, which will contain as a minimum: description of causes of deviations in the project, impact produced, proposed solutions to resolve and overall impact on the project, options recommended by the Project Manager or Supplier
- Reports on acceptance testing results for all types of tests performed (unit testing, system testing, integration testing, stress testing, load testing, penetration testing, etc.)
- Report on the completion of the piloting stage of the e-Contravention Case Management System
- Training reports, including: Evaluation results of participants.
- Report on the assessment of risks and their impact carried out as part of the definition of the Continuity Plan

2. Reports related to the maintenance and post-implementation support stage:
    - Service Level Reports;
    - Incident debugging reports;
    - Continuity Plan Testing Report
    - Development request review reports related to perfective maintenance

7. Project implementation deadlines

The tasks listed in this document are estimated to be completed in 30 months: 18 months for design/development/ migration/implementation and 12 months for warranty, maintenance and technical support. Although, the main purpose of the warranty period is to identify and fix bugs, if the Beneficiary identifies new functionalities during the warranty period that need to be implemented, they can be implemented in additional iterations, depending on the available budget.

In case of satisfactory performance, the contract may be extended on the basis of the same contractual provisions.

8. Institutional arrangements

8.1. Beneficiary:

The Beneficiary of this procurement is the Ministry of Internal Affairs.

The Beneficiary is responsible for all administrative and procedural aspects, contract and financial management, including acceptance and payment for deliverables/ reports under the Contract, general project-related responsibilities and effective coordination with stakeholders.

The Beneficiary will designate the Product Owner, who will coordinate and make decisions on all aspects of the technical elements of the Contract. The Product Owner will issue the administrative note on the Contract implementation start date and other tasks.

The Beneficiary shall ensure the following:

- infrastructure resources for the test and production environment;
- source code repositories, problem identification and management system, continuous integration and delivery (CI/CD) environment, task management system.
- training facilities.

The Beneficiary will ensure the delegation of at least the following specialists

#	Name of expert's competence	Responsibilities
1.	Product owner	• The Product Owner represents the Beneficiary within the development team and in relation to other stakeholders. He/she must clearly communicate and share the requirements, objectives and priorities of the Beneficiary and ensure transparency and understanding within the project. • The Product Owner is responsible for defining and clarifying the Beneficiary's requirements and expectations for the product. • The Product Owner maintains the product backlog. The Product Owner together with the Business Analyst will regularly update the product backlog to reflect the prioritized list of desired functionalities to be implemented. • The Product Owner responds to developer questions. The Product Owner will be permanently available to answer clarification questions from the developer team, thus avoiding complex and formal project communication. In order to get a working product at the end of the sprint, it is extremely important that the team has all the necessary information at the right time. • Product Owner accepts milestone/sprint deliverables. Milestone/sprint deliverables are presented to the Beneficiary at the end of each sprint for acceptance. The Beneficiary via the Product Owner will accept the milestone/sprint deliverables or inform the Provider of identified defects until the completion of the next sprint. • Although not strictly necessary, the Product Owner may attend the development team meetings to be informed about progress and possible blocking factors for a prompt reaction to them. • The Product Owner also makes the decision on the product release according to the release plan.
2.	Project Manager from MIA	• The MIA Project Manager organizes and coordinates the project activities of the MIA team and ensures their execution within the agreed terms; • Leads the MIA Project Team and is primarily responsible for fulfilling MIA's responsibilities under the Project; • Monitors the timely execution of operational commitments made by MIA project team members (e.g. provision of information, review of deliverables, etc.); • Organizes the secretarial work of the MIA Project Team (handling correspondence, information exchange, document storage, etc.); • Informs his/her team about the activities and events produced within the Project, ensures good communication and collaboration within the MIA project team; • Ensures good communication, coordinates and mediates the interaction and collaboration between the project team on the MIA side and the project team on the Provider side; • Organizes project meetings and working meetings; • Reports to the CDP on project progress, risks, deficiencies and exceptions encountered.
3.	Project coordinator from the institution (GPI,STI)	• Represents in the Project the institution of which he/she is a part; and in the Project;

		• Ensures the follow-up and achievement of the Project objectives at the level of the institution of which he/she is part; • Proposes the nominal composition of the members of the project team within the institution he/she represents and ensures their delegation according to the needs of the project; • Organizes, coordinates and supervises the appropriate participation of the responsible persons within the institution in the project activities; • Ensures complete, accurate and timely provision of information related to the institution; • Reviews and validates project deliverables relevant to his/her institution.
4.	Business area specialist (GPI employees)	• Provides timely, accurate and complete information on the business model of the institution of which he/she is a part; and • Is the point of contact between the project and other managers of the institution, if the situation requires their involvement in the project at the level of the operational business model; • Reviews and validates the deliverables produced within the project relevant to the business model of the institution of which he/she is part.
5.	ICT Specialist (STI employees)	• Provides timely, accurate and complete information on the ICT environment of the institution of which he/she is a part; and • Is the point of contact between the project and other managers of the institution, if the situation requires their involvement in the ICT environment of the project; • Reviews and validates project deliverables relevant to the ICT environment of the institution of which he/she is a part.
6.	MIA testing/pilot team	• This team is responsible for testing and evaluating the software to ensure that it meets the requirements and expectations of the beneficiary. • The testing/pilot team evaluates the user experience and usability of the software. They review workflows, user interface and functionalities to ensure they are intuitive and easy to use. • The testing/pilot team involves real users in testing and evaluating the software product. This approach allows to get direct feedback from users and identify their needs and suggestions for further improvements.

8.2. Provider:

The Provider is the company or consortium that has been awarded the contract following the tender and is to carry out the work in accordance with these specifications.

The Provider shall be responsible for the management of the project in accordance with the project plan and practices agreed with the Beneficiary. The Provider is responsible for identifying and mobilizing the resources required to carry out the activities in its area of responsibility set out in the project management plan to the agreed quality level.

The detailed requirements for the Provider's responsibilities related to the project management procedures are described in Annex B "Requirements for the implementation of the e-Contravention Case Management System".

8.3. Purchaser of the IT system

The UNDP project "Supporting e-transformation of policing processes related to contravention cases" ensures the procurement of the design, development, implementation, warranty, maintenance and technical support of the e-Contravention Case Management System according to the requirements of this ToR.

9. Qualification requirements

1.2. Qualification requirements for the development company

The Provider shall provide supporting documentation (including information on completed contracts and contact details of clients from whom references may be requested or whom the Beneficiary may, if necessary, visit to familiarize itself with the systems put into operation by the Provider) to satisfy itself that the Provider satisfies the experience requirements below:

1. Has been operational for the last 5 years, with the bulk of the work being in the development of IT systems.
2. Has experience of implementing projects similar in scope and complexity developing applications, demonstrated by at least 2 contracts with development stage completed in at least 3 years. For ongoing projects, copies of acceptance documents for the entire software solution will be submitted.
3. Software development experience using Agile principles (as described in the scope and approach section of the ToR) will be an advantage. This will be demonstrated by presenting the project methodology describing the role of the Provider.
4. Demonstrated experience in the use of the technology stack and holding the relevant technology stack, quality assurance processes and information security certifications will be an advantage.

1.3. Qualification requirements for the Consultant staff

The Consultant will propose a team of the following key experts:

#	Category	Name of experts competence	units
1.	Key Expert	Project manager/ Scrum master	1
2.	Key Expert	System architect	1
3.	Key Expert	Business analyst	2
4.	Key Expert	Software developer	4
5.	Key Expert	Database Developer/Administrator	1
6.	Key Expert	Integration Specialist/Developer	1
7.	Key Expert	Specialist Quality Assurance/Trainer	3
8.	Non Key Experts	Non Key Experts (UI Designer, Subject Domain expert, Technical writer, Trainer, etc.)	*

For the proposed key experts, CVs demonstrating that they meet the minimum qualification requirements will be submitted as follows:

9.1. Key Expert 1. Project manager/ Scrum master

The Project Manager/Scrum Master leads the project team on behalf of the Provider and is primarily responsible for fulfilling the Provider's responsibilities for the Project. He/she ensures the availability of the required experts from the Provider in accordance with the Project Work Plan, organizes and coordinates the project activities of the Provider's team and ensures their execution according to the requirements and within the agreed terms. Ensures good communication, coordinates and mediates the interaction and collaboration between the project team on the Provider side, the project team on the Beneficiary side, as well as coordination with external

partners. Organizes project meetings and working meetings, and reports to the project steering committee on project progress, risks, shortcomings and exceptions.

The expert in the role of Project Manager/Scrum Master must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 7 years' experience in software development;
- at least 5 years of demonstrated experience in team/project management applying Agile methodology, with at least 2 projects implemented in the last 3 years;
- at least 2 successfully completed projects with public authorities, experience in implementing projects within public authorities in the Republic of Moldova will be considered an advantage.
- holding the following certifications or equivalent: CSM / CSPO, PMI-ACP, PMP, Prince2, SAFE5
- the following certifications will be an advantage: ISO 27001 Lead Auditor, CISM, ITIL, ISO 20000, ISO 9001
- experience in systems analysis;
- communication skills in English and Romanian.

9.2. Key Expert 2. System Architect

The System Architect is responsible for designing and defining the architecture of the software system. His role is to ensure that the system is designed in a coherent, efficient and scalable way, in accordance with the requirements and objectives of the creation of the e-Contravention Case Management System. The System Architect works with the development team to design and define the structure and components of the software system. This involves identifying and selecting the most appropriate technologies, platforms and frameworks to meet the project requirements. During software development, the system architect oversees the implementation of the defined architecture and ensures that the software components are integrated correctly and that the system works as intended. The System Architect must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 5 years of experience in software development, with at least 2 projects implemented in the last 3 years;
- minimum 3 years of experience in IT systems architecture, including large-scale systems architecture;
- holding certifications in any technology in the required technology stack will be considered an advantage;
- communication skills in Romanian.

9.3. Key Expert 3. Business Analyst

The Business Analyst is responsible for identifying the Beneficiary's needs and requirements and "translating" them into clear and achievable specifications for the development team. He/she works closely with the Beneficiary team and other stakeholders to identify the specific needs of each group. He/she uses various techniques and tools to translate the stated requirements into functional specifications to be realized in Agile sprints and jointly prioritizes them with the Beneficiary based on the value added. The Business Analyst is primarily responsible for ensuring that all parties involved in the project, both Provider and Beneficiary, have a clear understanding of the requirements and that the information is correctly interpreted and applied during development. The Business Analyst participates in the testing and validation process of the functionality developed to ensure that requirements and expectations are met and that the final product complies with the established needs and standards.

The Business Analyst expert must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 5 years of experience in software development;
- at least 5 years of demonstrated experience in business analysis with Agile methodology, with at least 2 projects implemented in the last 3 years;
- holding certifications in any technology in the required technology stack will be considered an advantage and project management processes;
- experience in unit testing, continuous integration, DevOps;
- experience in systems analysis;
- communication skills in Romanian and Russian.

9.4. Key Expert 4. Software Developer

Key category of developer responsible for implementing DevOps mechanisms in the development and implementation process of the e-Contravention Case Management System and involvement in critical development processes. This category of experts must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 5 years of experience in software development;
- participation in at least 2 software development projects in the last 3 years applying the Agile methodology;
- demonstrated experience in unit testing, continuous integration, DevOps;
- holding certifications in any technology in the required technology stack will be considered an advantage;
- communication skills in Romanian.

9.5. Key Expert 5. Database Developer/Administrator

Developer category responsible for the design and administration of the database related to the e-Contravention Case Management System. By virtue of the held position, the given category of experts is to define the data structures related to the e-Contravention Case Management System, implement the stored procedures of the e-Contravention Case Management System, configure the rights and privileges at database level for all categories of e-Contravention Case Management System users, implement the database backup mechanism, implement the data migration mechanism and the initial population of the e-Contravention Case Management System database.

Development/Administration is responsible for migrating data from the existing REC and RAR AIS systems, preparing and uploading the primary data sets required for the operation of the e-Contravention Case Management System.

The Database Developer/Administrator must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 5 years of experience in software development;
- at least 3 years of experience in developing/administering an Enterprise level DBMS (MS SQL, Oracle, etc.);
- participation in at least 2 projects implemented in the last 3 years applying Agile methodology;
- holding certification in any technology in the required technology stack will be an advantage;
- proven experience in database design, development and optimization;

- communication skills in Romanian.

9.6. Key Expert 6. Integration Specialist/Software Developer

Key category of developer responsible for integrating and coordinating individual software components to create a functional and cohesive solution. The Integration Specialist is responsible for bringing together the various software components developed by team members and ensuring their interoperability. He or she works to properly connect and interact software modules and systems to achieve the desired functionality. The Integration Specialist designs and configures data exchange via ESB (Enterprise Service Bus), messaging, web services and other tools to enable communication and data exchange between software components.

This category of experts must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 5 years of experience in software development;
- demonstrated experience working with WSO2 middleware platform technology. Experience working with MConnect will be an advantage;
- participation in at least 2 software development projects in the last 3 years applying Agile methodology;
- demonstrated experience of unit testing, continuous integration, DevOps;
- holding certifications in any technology in the required technology stack will be considered an advantage;
- communication skills in Romanian.

9.7. Key Expert 7. Specialist Quality Assurance/Software Tester/Trainer

Key expert responsible for ensuring the quality of the development and implementation processes of the e-Contravention Case Management System (functional and non-functional testing of the e-Contravention Case Management System including through automated means), drafting the user documentation of the e-Contravention Case Management System and conducting training for the categories of users mentioned in these specifications. It is also responsible for training the users. This type of expert must meet the following qualification requirements:

- higher education in ICT or other relevant field;
- at least 3 years of experience in software testing in projects of similar complexity;
- demonstrated experience in software testing analysis and design;
- demonstrated experience in performance testing (load and stress) and security testing;
- demonstrated experience in automated testing;
- certification in any technology in the required technology stack would be an advantage;
- experience in conducting training sessions for end users and IT specialists;
- experience of writing technical and end-user documentation;
- communication skills in Romanian.

9.8. Non Key Experts

The Provider may also include other experts in the project team as required. The involvement of these specialists will be coordinated with the Beneficiary. The total man/hours for which these specialists will be involved will not exceed 300 man/hours.

10. Estimation of project effort

Table 1 contains a pre-assessment of the effort required to design, develop and implement the e-Contravention Case Management System for all categories of experts requested in Chapter 8 of this ToR.

Table 1. Estimated effort for the implementation of the e-Contravention Case Management System

#	Name of the expert's competence	man/days	units	Total (man/day)
1.	Project manager/ Scrum master	180	1	180
2.	System Architect	60	1	60
3.	Business Analyst	150	2	300
4.	Software Developer	205	4	820
5.	Database Developer / Administrator	80	1	80
6.	Integration Specialist /Developer	180	1	180
7.	Specialist Quality Assurance/Software Tester/Trainer	60	3	180
8.	Non Key Experts (UI Designer, Domain expert, Technical writer, Trainer, etc.)		*	300
TOTAL			13*	2100

The experts in the development team will work within the effort limit included in Table 1. Considering the Agile development methodology, if necessary, the Beneficiary may reallocate the workload reserved to the experts involved in the e-Contravention Case Management System development project, so that the effort not used by some experts can be distributed to others.

~~Payment will be made on a quarterly basis based on the actual effort made by the Provider's experts jointly agreed with the Beneficiary during the planning stage of project SPRINTs and deliverables accepted by the Beneficiary.~~

Annex A

Specifications of the software requirements for the e-Contravention Case Management System in the Ministry of Internal Affairs

1. Generalities

1.1. Purpose and destination of the Annex

This annex "Software Requirements Specification for the e-Contravention Case Management System in the Ministry of Internal Affairs" is intended to present the objectives and expectations of the system implementation by providing a detailed description of the functionalities, features and requirements that the software product must meet. This annex serves as a reference for the product backlog. The functional and non-functional requirements described in this annex are mandatory unless expressly stated otherwise.

The document is intended for the solution developer, the implementation unit and other stakeholders such as sponsors, stakeholders, end beneficiaries, etc.

1.2. Notions and abbreviations

The following notions and abbreviations are used in this document:

RO – Reporting Officer
BD – Database
CC – Contravention Code
CPC – Criminal Procedure Code
GD – Government Decision
MIA – Ministry of Internal Affairs of the Republic of Moldova
IDNO – Identification number of the legal entity, unique 13-digit number.
IDNP – Identification number of the natural person, unique 13-digit number.
GPI – General Police Inspectorate of the MIA
Chief RO – Chief of the Reporting Officer
RCFI – Register of Criminological and Forensic Information
ToR – Terms of Reference
CIO – Criminal Investigation Officer

information system – the totality of information resources, information and communication technologies, together with associated organizational structures, interacting in an organized manner to collect, process, store and deliver information in order to achieve predetermined objectives.
information resource - the totality of data and information stored in an organized manner in information systems, in accordance with established requirements and applicable legislation;
automated information system (AIS) – synonym for information system;
information service – a data delivery service, developed and made available by the data provider through the interoperability platform, which meets the needs of multiple data consumers;
Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) - as defined by Government Decision No 128 of 20.02.2014 on the Common Government Technology Platform (MCloud)

information object – the virtual reflection of the object of record within the information resource, presented through the sets of characteristics that define it and the values assigned to those characteristics;
CARE[1] (Community database on Accidents on the Roads in Europe) - Community statistical database on road accidents resulting in death or injury. Established under Council of Europe Decision 93/704/EC of 30.11.1993.
CADaS[2] (Common Road Accident Data Set) – is a framework standard promoted by the Council of Europe for the unification of road accident statistics within the CARE framework. It defines a common set of data elements (statistical variables and values) describing the phenomenon and their taxonomy.
MoReq2010 (Modular Requirements for Records Systems) – Document of specifications recommended by the European Commission for the acquisition/development of Electronic Records Management Systems.

2. The purpose and objectives of the creation of the e-Contravention Case Management System

2.1. Purpose

The purpose of the creation of the e-Contravention Case Management System information resource is to provide an efficient centralized configurable platform to digitally support the contravention case management and related activities carried out by the reporting officers of the various authorities empowered to deal with contravention cases.

2.2. General objectives:

- Digitization of the contravention process
- Facilitating citizens' access to information of interest to them and to public services
- Increasing transparency: A computerized system for managing contraventions should ensure greater transparency in the process of handling contravention cases and increase citizens' confidence in the authorities' ability to enforce the law and protect their interests.
- Increased efficiency and effectiveness: A computerized contravention management system can help to increase the efficiency and effectiveness of the process of documenting and managing contravention cases. By using electronic documents and excluding manual processes, enforcement authorities can save time and resources and process more cases in a shorter time.
- Ensure probity and improve accuracy: A computerized contravention management system can reduce human error and the possibility of data manipulation in the process of handling contravention cases. This would help increase accuracy and precision in the documentation of contravention cases and reduce the number of challenges and the risk of the contravention report being overturned by the court for reasons other than the legality of the penalty decision.
- Improved communication: A computerized contravention management system can improve communication between the different authorities involved in handling contravention cases. This can help eliminate redundancies and increase the efficiency of case management processes.
- Improved capacity for monitoring and analyzing data on contravention cases: A computerized contravention management system should allow for the collection of statistics and the generation of detailed reports, which can help to identify trends, recurring problems and behavioral patterns of offenders. This will help in the development of public policy and strategies in the areas of law

[1] https://ec.europa.eu/transport/road_safety/specialist/observatory/methodology_tools/about_care_en
[2] https://ec.europa.eu/transport/road_safety/sites/roadsafety/files/cadas_glossary_v_3_6.pdf

enforcement, respect for human rights and freedoms and the overall improvement of law enforcement approaches to the management of contravention cases.

- Increased data security: A 'secure by design' contravention management IT system can help increase the security of personal data. This is ensured by implementing strong security controls, encrypting sensitive data and other measures required by regulations, standards and best practices in the field of personal data protection and cyber security.
- Strengthen ICT service management and information security systems. Capacity building based on digital tools will contribute to meeting consumer demands and continuously improving processes and delivery of online public services. At the same time, achieving the objective involves minimizing cyber security risks related to information attacks on institutional resources and confidential data in order to prevent unauthorized damage, modification or even deletion and to protect departmental and state information resources.

2.3. Specific objectives:

- Implementation of the electronic contravention case file;
- Ensuring a unified country-wide record of contravention cases and the follow-up of the enforcement of sanctions imposed, in order to make the operational and tactical activities of law enforcement agencies more efficient in the process of detecting and combating contraventions and ensuring the rule of law and creating conditions for better identification of continuous and repeated contraventions;
- Improving accuracy and precision - a computerized contravention management system can help the reporting officer to make more informed decisions and reduce the risk of errors, ambiguities and data manipulation in the process of managing contravention cases, by automating certain activities, digitizing information and replacing physical documents with electronic ones.
- Efficient documentation of contravention cases: The system should allow for fast and accurate documentation of contravention cases so that relevant information can be accessed and updated accordingly.
- Processing and Tracking: The system must allow for tracking the progress of cases, as well as notification and scheduling of hearings and other events relevant to those cases.
- Process automation: The system should be able to automate processes such as notification generation and scheduling of hearings in order to reduce case processing time and optimize resources.
- Reporting and analysis: The system should be able to generate relevant reports and analysis on contravention cases in order to evaluate the effectiveness of the system and the case management process.
- Integration with other systems: The system should be able to integrate with other systems such as police databases, online payment system, etc. for more efficient case management.
- Accessibility and security: The system must be accessible to all authorized users, but also provide adequate security to protect confidential information and personal data.
- Ensuring compliance: the system must comply with legal regulations and standards and allow proper administration and management of personal data.
- Flexibility and extensibility: The system must have the capabilities to design, configure and deploy new information objects and IT services without source code intervention and programmer involvement. The contravention process is a complex set of activities involving many stakeholders. The automation of activities related to the contravention process is to be carried out in a stepwise manner for each authority competent to deal with contravention cases. It is expected that the definition of entities, registers and register objects, workflows, tasks, document templates, case management rules and

related decision trees, screen forms, APIs and other application components and services required to automate the contravention case management activities related to each stage can be achieved without the involvement of programmers and the need for development of application source code.

- Providing information support to the authorities competent to deal with contravention cases, other central administrative authorities and local public administration authorities in order to increase the efficiency of public policy making in the field of law enforcement and respect for human rights and freedoms;
- Ensuring that citizens' rights and freedoms are not violated due to lack of information about actions and/or decisions of other authorities competent to deal with contravention cases.
- Ensuring efficient and secure data exchange with competent authorities dealing with contravention cases and other parties holding data relevant to the management of contravention cases or consumers of data related to the field of automation;

2.4. Expected effects:

The implementation of the e-Contravention Case Management System **will allow**:

- implement the contravention case file in electronic format;
- the creation and development of a single information resource for enforcement bodies;
- ensure probity and improve the quality of the work of the reporting officer;
- facilitate the development of standards of reporting officer activity, through automated performance evaluation and the establishment of monitoring mechanisms;
- ensure an adequate level of protection of personal data;
- digitizing the infringement process;
- bringing the contravention process in line with Community standards;
- automation of processes;
- exclusion of the human factor and corruption phenomena in the documentation of the contravention and the adoption of the decision;
- the correct legal qualification of the offence;
- improving forms of control over the work of the reporting officer;
- optimizing the activities of the subdivisions of the Ministry of Internal Affairs in which reporting officers work;
- improving discipline and institutional control over the contravention process;
- improving the quality of data produced in the activities of the contravention procedure;
- creating the conditions for the exchange of data in electronic form between the Ministry of Internal Affairs and other legal bodies with responsibilities in the field of contraventions (e.g. Prosecution, courts, other public authorities in which reporting officers work, etc.);
- reducing the number of court decisions to the detriment of the state institution;
- improving the quality of justice.

The implementation of the e-Contravention Case Management System **will ensure**:

- the creation of a unified computerized support for the management in a consolidated form of the data and information required to support the decision during the activities of the contravention procedure, planning, coordination and management of the actions of the reporting officer;

- the implementation of a modern system for managing data and their life cycle, with the possibility of recording and displaying online the dynamic evolution of the contravention file, including the descriptive details of events;
- real-time exchange of information during the contravention procedure, operational transmission of information and its chronological recording.
- the implementation of the application will provide a computer platform integrating information technology applications through which the management of the Ministry and other structures of the Ministry of Internal Affairs with competences in the management of contravention processes will benefit from:
- creation of a database at the central level of the Ministry of Internal Affairs on the progress of contravention procedure activities and centralized storage of procedural documents in electronic format;
- implementation of analysis and evaluation tools allowing the operational production of summaries and reports necessary for decision making;
- the development of periodic predefined reports on the progress of activities on the contravention cases or activities in their dynamics;
- judicious planning of human and material resources in the process of planning the activities of the contravention procedure and implicitly during their development;
- simplification of the process of logging data and information during the course of contravention proceedings;
- creating a flexible mechanism for recording, storing and archiving data and information, both in terms of event reporting and documents related to the contravention process and action management.

3. Reference regulatory framework for the new computerized system

The regulatory framework of reference for the e-Contravention Case Management System is composed of national legislation, international treaties and conventions to which the Republic of Moldova is a party. These can be grouped into the following areas:

1. Normative acts regulating the field of activity subject to automation;
2. Normative acts governing the ICT sector and information security;
3. Normative acts institutionalizing Shared Government Platform IT Services and AIS relevant to the field of automation
4. Normative acts institutionalizing MIA information resources to be integrated/taken over in the e-Contravention Case Management System;
5. ICT standards and standards relevant to the field of automation

The following regulatory acts are considered the most relevant to the creation and operation of the e-Contravention Case Management System:

1. The normative acts regulating the field of activity subject to automation:
   - Contravention Code No 218 of 24.10.2008
   - Criminal Procedure Code approved by Law No. 122 of 14.03.2003
   - Law no.320 of 27.12.2012 on the activity of the Police and the status of the police officer
   - Law No. 216 of 08.08.2003 on the fully automated information system for the registration of offences, criminal cases and offenders;

- Law No. 412 of 09.12.2004 on official statistics;
- Law No. 414 of 22.12.2006 on compulsory third party liability insurance for damage caused by motor vehicles;
- Law No. 45 of 01.03.2007 on preventing and combating domestic violence
- Law No. 131-XVI of 07.06.2007 on road traffic safety
- Law No. 50 of 22.03.2012 on preventing and combating organized crime
- Law No. 68 of 14.04.2016 on forensic expertise and the status of the forensic expert
- Government Decision No. 547 of 12.11.2019 on the organization and functioning of the General Police Inspectorate;
- Government Decision No. 778 of 20.11.1995 on the approval and implementation of the merchandisable types of driving licenses and registration certificates for means of transport;
- Government Decision No.1047 of 08.11.1999 on the reorganization of the Automated Information System of Search "Automobile" in the State Register of Transport and the introduction of testing of motor vehicles and their trailers;
- Government Decision no. 493 of 14.08.2009 approving the Regulation on the record of traffic offences and ensuring the access of the driving license holder to information on penalty points.
- Government Decision No. 684/2018 approving the Regulation on the evaluation, administration and recovery of criminal assets (seized);
- Joint Order of the Prosecutor General, the Minister of Internal Affairs, the Director General of the Customs Department, the Director of the Centre for Combating Economic Crimes and Corruption No. 121 / 254 / 286-O / 95 of 18.07.2008 on the single register of offences, criminal cases and offenders.
- MIA Order No. 325 of 30 August 2002 on the improvement of the normative-legal regulation of the activity of the Road Traffic Safety Service of the Traffic Police of the General Police Inspectorate of the MIA of the Republic of Moldova.
- MIA Order No.195 of 17.04.2020 on the establishment of competences in the field of detection/examination of contraventions assigned to the reporting officers of the Ministry of Internal Affairs
- MIA Order No. 172 of 23.04.2021 on the amendment of the Annex to MIA Order No. 195 of 17.04.2020
- MIA Order No. 85/2019, "Instruction on how to register and record contraventions, the persons who committed them and the results of the examination of contravention cases";
- Order of the General Inspectorate of Border Police No 650 /2013, on the Instruction on the recording and examination of contravention cases by border police officers.
- GPI Order No. 85 of 02.03.2022 on the approval of standard forms of procedural documents drawn up by Police employees in the contravention process, as well as following the examination of other information on offences and incidents.
- Order of the Minister of Health No. 99 of 27.06.2003 on the approval of the Regulation on the forensic assessment of the severity of bodily injury;
- Joint Order of the Minister of Internal Affairs, Minister of Transport and Road Administration, Minister of Health, Director General of the National Bureau of Statistics No. 160/64/214/38 of 24 May 2006
- Joint Order of the Ministry of Internal Affairs, Ministry of Transport and Road Administration, Ministry of Health, National Bureau of Statistics with no.335/224/827/81 of 26.10.2016 on the record of road accidents;
- GPI Order No. 562 of 31.12.2021 on the approval of the Operational Procedure for the receipt, registration, recording, examination and archiving of complaints.
- GPI Order No. 93 of 28.03.2023 on the approval of the methodological instruction on police intervention in preventing and combating cases of domestic violence.

2. The normative acts governing the ICT sector and information security

- Law No. 982 of 11.05.2000 on access to information;
- Law No. 1069 of 22.06.2000 on information technology
- Law No. 467 of 21.11.2003 on computerization and state information resources;
- Law No. 71 of 22.03.2007 on registers;
- Law No. 133 of 08.07.2011 on the protection of personal data
- Law No. 305 of 26.12.2012 on the re-use of public sector information
- Law No. 91 of 29.05.2014 on electronic signature and electronic document;
- Law No. 142 of 19.07.2018 on data exchange and interoperability
- Law No. 234 of 23.12.2021 on public services
- Government Decision No. 840 of 30.07.2004 on the creation of the Telecommunications System of Public Administration Authorities
- Government Decision No. 562 of 26.05.2006 on the creation of automated state information systems and resources
- Government Decision No. 1123 of 24.12.2010 on the approval of the Requirements for ensuring the security of personal data when processing personal data in the framework of personal data information systems
- Government Decision No. 330 of 04.05.2010 on the creation and administration of the single government portal of public services
- Government Decision No. 188 of 06.04.2012 on the official pages of public administration authorities in the Internet network
- Government Decision No. 656 of 05.09.2012 on the approval of the Interoperability Framework Program;
- Government Decision No. 822 of 09.11.2012 on the services of the electronic mail system of public administration authorities
- Government Decision No. 886 of 08.11.2013 approving the Methodological Rules for the implementation of Law No 305 of 26 December 2012 on the re-use of public sector information
- Government Decision No. 201 of 07.04.2017 on the approval of the mandatory minimum requirements for cyber security
- Government Decision No. 1141 of 20.12.2017 approving the Regulation on the application of the electronic signature on electronic documents by officials of public legal entities in their electronic circulation.
- Government Decision No. 153/2021 approving the Concept of the information system "Register of State Information Resources and Systems" and the Regulation on how to keep the Register of State Information Resources and Systems.
- Government Decision No. 491/2022 on the approval of the manner of recognition of qualified electronic signatures created using a qualified public key certificate issued by a trust service provider of a Member State of the European Union
- MDI Order No. 78 of 01.06.2006 on the approval of the technical regulation "Software lifecycle processes" RT 38370656 - 002:2006.
- MDI Order No. 94 of 17.09.2009 on the approval of some technical regulations (the way of electronic public services registration, provision of electronic public services, ensuring information security in the provision of electronic public services, determining the cost of development and implementation of automated information systems)
- MIA Order No. 195 of 04 July 2016 on the implementation of centralized management practices of Information and Communication Technology services within MIA

- MIA Order No. 401/2016 on the implementation of the Indicator of documents and their retention terms
- MIA Order No. 243 of 18.08.2017 on the Information and Communication Technology Services Management System within MIA
- MIA Order No. 244 of 18.08.2017 on the Information Security Management System within MIA
- MIA Order No. 247 of 03.08.2016 on the application of personal data protection practices in the implementation of Information and Communication Technology services within MIA;
- MIA Order No. 31 of 14.12.2017 on the approval of the Regulation on the general control of information systems maintained by the MIA IT Service

3. The normative acts institutionalizing Shared Government Platform IT Services and AIS relevant to the automation domain:
   - Government Decision No. 1323 of 29.12.2000 on the approval of the lists of national and local (county) public roads;
   - Government Decision No. 1058 of 06.08.2002 on the creation of the automated information system "State Register of Vehicle Drivers";
   - Government Decision No. 1518 of 17.12.2003 on the creation of the automated information system "State register of administrative-territorial units and streets of localities in the territory of Moldova
   - Government Decision No. 770 of 06.07.2004 on the Integrated Automated Information System for the Recording of Offences, Criminal Cases and Offenders
   - Government Decision No. 1202 of 27.10.2006 on the approval of the Concept of the Integrated Information System of Law Enforcement Agencies
   - Government Decision No. 65 of 21.05.2007 on the approval of the Concept of the Automated Information System "Fingerprint Register”
   - Government Decision No. 188/2012 on the official pages of public administration authorities in the Internet;
   - Government Decision No. 133 of 27.02.2012 on the approval of the Technical Concept of the State Automated Information System in the field of compulsory civil liability insurance for damage caused by motor vehicles;
   - Government Decision No. 965 of 27.11.2014 on the approval of the Regulation on the organization and operation of the Automated System of Road Traffic Supervision "Traffic Control" and amendment of the Concept of the Automated System of Road Traffic Supervision "Traffic Control";
   - Government Decision No 329 of 01.06.2012 on the Government Electronic Payment Service (MPay)
   - Government Decision No. 1090 of 10.01.2013 on the Government Electronic Authentication and Access Control Service (MPass)
   - Government Decision No. 128 of 25.02.2014 on the Common Government Technology Platform (MCloud)
   - Government Decision No. 405 of 02.06.2014 on the integrated electronic governmental electronic signature service (MSign)
   - Government Decision No. 708 of 05.09.2014 on the electronic government logging service (MLog)
   - Government Decision No. 701 of 29.08.2014 on the approval of the Methodology for the publication of open government data
   - Government Decision No. 414 of 08.05.2018 on measures to consolidate data centers in the public sector and streamline the administration of state information systems;
   - Government Decision No. 211/2019 on the interoperability platform (MConnect);

- Government Decision No. 376/2020 on the approval of the Concept of the Government Electronic Notification Service (MNotify) and the Regulation on the operation and use of the Government Electronic Notification Service (MNotify);
- Government Decision No. 712/2020 on the Government Electronic Payment Service (MPay);
- Government Decision No. 375/2020 approving the Concept of the Automated Information System "Register of Powers of Attorney on the basis of electronic signature" (MPower) and the Regulation on how to keep the Register of Powers of Attorney on the basis of electronic signature;
- Government Decision No. 746/2020 on the procedure for providing information on administrative fines to the State Tax Service
- Government Decision No. 323/2021 approving the Concept of the "Semantic Catalogue" Information System and the Regulation on how to keep the Register formed by the "Semantic Catalogue" Information System
- Government Decision No. 413/2020 approving the Regulation on the use, administration and development of the Governmental Citizen

4. The normative acts institutionalizing MIA information resources to be integrated/taken over in the e-Contravention Case Management System:
   - Law No. 185 of 11.09.2020 on the Automated Information System for recording contraventions, contravention cases and offenders
   - Government Decision No. 693 of 21.06.2007 on the approval of the Concept of the Automated Information System "State Register of Road Accidents".
   - Government Decision No. 517 of 22.07.2022 on the approval of the Concept of the Automated Information System for the registration of contraventions, contravention cases and offenders and the Regulation on the single registration of contraventions, contravention cases and offenders

5. ICT standards and standards relevant to the field of automation
   The design, development and implementation of the *e-Contravention Case Management System* must be carried out in accordance with national standards and methodology as well as established ICT sector recommendations and requirements. Thus, the following regulations and standards should be taken into account:
   - The Republic of Moldova Standard SM ISO/IEC/IEEE 15288:2015, "Systems and software engineering. System lifecycle processes".
   - Standard SM 12207:2005 "Software life cycle processes";
   - Standard SM SR ISO 15489:2016 "Information and documentation - Documentation management".
   - Technical regulation "Software life cycle processes" RT 38370656-002:2006; Official Gazette No. 95-97/335 of 23/06/2006.
   - SM RM ISO 14641 Electronic document management - Design and operation of electronic document storage information system - Specification;
   - World Wide Web Consortium (W3C) recommendations (http://www.w3c.org) on the quality of Web page content, the possibilities of accurate information viewing using widely used Internet browsers, and compatibility with different computer platforms;
   - W3C Recommendations (http://validator.w3.org) on the testing of Web pages. All web pages generated by the e-Contravention Case Management System will be tested according to these recommendations.
   - SDMX standard (Statistical data and metadata exchange standard - http://sdmx.org)
   - SM ISO/IEC 111791:2018 "Information technology - Metadata registries (MDR)”

4. Stakeholders and business roles

4.1. Stakeholders involved in the implementation of the e-Contravention Case Management System

Identifying stakeholders and their needs is important for the conceptualization of the IT system. The information and functionality needs of these entities are to be considered for the definition of the information objects and functional capabilities of the e-Contravention Case Management System.

Stakeholders in the implementation of the e-Contravention Case Management System are defined by the legislative acts regulating the management of contravention cases, the creation and use of state information resources, access to information, cyber security and protection of personal data, as well as other legislative acts related to the field of automation and can be grouped as follows:

A. Participants in the contravention process:
   1. The authorities competent to deal with contravention cases in accordance with Article 393 of the Contravention Code are:
      a) the court;
      b) the public prosecutor;
      c) the administrative commission;
      d) the reporting officer (specialized bodies specified in art. 400–423[12]).
   2. The person in respect of whom the contravention proceedings have been brought;
   3. The victim
   4. The witness
   5. The specialist
   6. The expert
   7. The interpreter
   8. The defender
   9. The probation counsellor

B. The subjects of the legal relations relating to the creation and maintenance of departmental state registers, such as: **Register of contraventions, contravention cases and offenders**. In accordance with Government Decision No. 517/2022 approving the Concept of the Automated Information System for recording contraventions, contravention cases and offenders and the Regulation on the single record of contraventions, contravention cases and offenders, the subjects of legal relations are:

   1. The State - as the Owner of the information resource.
   2. Ministry of Internal Affairs - as the Possessor of the information resource.
   3. Information Technology Service of the Ministry of Internal Affairs - as the Holder of the information resource.
   4. National Administrator, who has access to all information/counts in the System;
   5. Local Administrator, depending on his/her functional competences, has access to the following accounts:
      - The "Automated record of contraventions and persons who have committed them" outline;

- The "Record of penalty points awarded for traffic offences" outline;
- The "Automated record of persons and cars reported as wanted" outline;
- The "Generation of personalized statistical reports" outline;
- The "Management of records documents" outline;
- The "Management of retrieved documents" outline;

6. The Registrar (the person responsible for recording contraventions), depending on his/her functional competences, has access to the following accounts:
   - The "Automated record of contraventions and persons who have committed them" outline;
   - The "Record of penalty points awarded for traffic offences" outline;
   - The "Automated record of persons and cars reported as wanted" outline;
7. The view user, who has access to the following outlines, with the restriction to enter some data and modify the data entered:
   - The "Automated record of contraventions and persons who committed them" outline;
   - The "Record of penalty points awarded for traffic offences" outline;
   - The "Automated record of persons and cars reported as wanted" outline;
   - The "Generation of personalized statistical reports" outline.
8. The data providers are:
   1) Public Services Agency;
   2) the courts;
   3) participants in the System, according to Law No 185/2020 on the Automated Information System for recording contraventions, contravention cases and offenders;
   4) natural or legal persons of private or public law who submit to the participants' data on the information objects of the System in the manner established by the regulatory framework.

State Register of Road Accidents. In accordance with the Government Decision No 693/2007 on the approval of the Concept of the automated information system "State Register of Road Accidents", the following subjects of the legal relations related to the creation and maintenance of the "State Register of Road Accidents" are nominated:

1. The State - as the Owner of the information resource.
2. Ministry of Internal Affairs - as the Possessor of the information resource.
3. Information Technology Service of the Ministry of Internal Affairs - as the Holder of the information resource.
4. Registrars:

   a) Ministry of Internal Affairs (police stations), in terms of records:
   - the occurrence of road accidents;
   - means of transport involved in the accident;
   - persons involved in the accident;
   - witnesses to road accidents;
   - administrative reports drawn up on the accident;
   - criminal cases initiated as a result of the accident;

- topological data on the scene of the accident;
- conclusions based on forensic, auto-technical and trace investigations;

b) Ministry of Health (health institutions, Forensic Medicine Centre) regarding the records:

- persons who died as a result of the accident;
- persons seriously injured as a result of the accident;
- persons slightly injured as a result of the accident;
- conclusions based on forensic investigations;

c) Ministry of Justice (National Centre for Forensic Expertise) regarding the records:

- conclusions on the basis of forensic, auto-technical and tracing investigations.

Register of Emergency Restriction Orders. Law 45/2007 on preventing and combating domestic violence and GPI Order 93/2023 provide for the following stakeholders:

1. Ministry of Internal Affairs - as the Possessor of the information resource.
2. Information Technology Service of the Ministry of Internal Affairs - as the Holder of the RICC AIS.
3. Guard Service/Police Inspectorate - as responsible for the registration of the Emergency Restriction Order in the Central Data Bank (RICC AIS).
4. Head of Community Interaction Service/Principal Officer - responsible for systematizing and recording emergency restriction orders issued by the Police in respect of domestic abusers.
5. Subdivision Secretary - as the person responsible for keeping the record of the register of emergency restriction orders in accordance with the MIA Order No. 401/2016 on the implementation of the Indicator of documents and their retention terms.
6. The police officer - as the issuer of the emergency restriction order
7. Other authorities and institutions empowered to prevent and combat domestic violence according to Law no. 45/2007, as well as:
   - central specialized state bodies (Ministry of Labor and Social Protection, Ministry of Health, Ministry of Education and Research, Ministry of the Internal Affairs, Ministry of Justice);
   - local public administration authorities and specialized local public administration authorities;
   - centers/services for assistance and protection of victims of domestic violence and their children and centers/services for assistance and counselling for family abusers;
   - - other organizations with specialized activities in this field.

C. The subjects of the legal relationships relating to the creation and maintenance of internal registers, such as:

1. Register of persons and means of transport announced as wanted.
2. Register of blank forms of strict record.
3. Register of issued e-Contravention record.

Subjects of the legal relations related to the creation and maintenance of the internal registers are:

1. Ministry of Internal Affairs - as the Possessor of the information resource.
2. Information Technology Service of the Ministry of Internal Affairs - as Holder of the RICC AIS.
3. Subdivisions of the MIA with police functions - as Registrars and Recipients of the internal register data

D. In addition to the participants explicitly defined by the Contravention Code and the regulations for keeping departmental state registers related to the contravention process, as interested parties shall also be considered:
   1. Law enforcement bodies - as authorities responsible for ensuring the rule of law in accordance with the roles assigned by Government Decision No 1202 of 27.10.2006 on the approval of the Concept of the Integrated Information System of Law Enforcement Bodies.
   2. International partners under police cooperation agreements, such as Interpol, Europol, etc.
   3. Authorities with control functions are public authorities responsible for law enforcement at all stages of the life cycle of the information resource, from conceptualization to destruction. This category also includes authorities responsible for GDPR, cybersecurity, etc.
   4. The citizen to be the ultimate beneficiary of all public policies.

4.2. Business roles

According to the tasks set out in the regulatory framework on the management of contravention cases, electronic record keeping, creation and use of state information resources, access to information, cybersecurity and personal data protection, and other legislation related to automation, stakeholders can be grouped as follows:

1. Entities with direct powers.

   Entities with direct powers are the stakeholders empowered by law to set up, own, manage and use the information resource e-Contravention Case Management System. Entities in these roles are interested in and will be involved in the process of conceptualization, development and use of the e-Contravention Case Management System.

   The entities with direct powers are:

   - Entities with administrative powers - these are public authorities that have administrative roles, established by law, in relation to the application but by virtue of which they do not use it;
   - Users of the e-Contravention Case Management System - authorities whose employees directly use the application to perform their duties.

2. Authorities with control functions

   Authorities with control functions are public authorities responsible for ensuring compliance at all stages of the information resource life cycle, from conceptualization to destruction. This category also includes authorities responsible for GDPR, cyber security, etc.

3. Beneficiaries without direct access – these are entities that are not direct users of the e-Contravention Case Management System:
   - use information from the e-Contravention Case Management System (e.g. via the MConnect interoperability platform and/or public services such as: MCabinet, MDoc, date.gov.md, services.gov.md, MPay, etc.);
   - can benefit from statistics and depersonalized data from it;
   - they are data providers for the e-Contravention Case Management System.

The involvement of these entities at the conceptualization and development stage of the e-Contravention Case Management System is important. The information needs of these entities are to be considered for the definition of the information objects of the e-Contravention Case Management System.

4.2.1. ENTITIES WITH DIRECT POWERS IN ADMINISTRATIVE ROLES:

OWNER

The owner of the state information resources, in this case the e-Contravention Case Management System and the electronic records kept in the e-Contravention Case Management System, is ***the State***. The owner determines the possessors, holders, technical administrators and users of state information systems, and in the case of departmental state registers the register possessor, register holder, registrar and sub-registrar.

POSSESSOR of the e-Contravention Case Management System:

The role of the possessor of the e-Contravention Case Management System is assigned to the Ministry of Internal Affairs by Law 185/2020. The possessor ensures the legal, financial and organizational conditions for the establishment, administration, maintenance and development of state information systems.

The MIA is also the implicit possessor of the departmental state registers to be created and kept in electronic format in the e-Contravention Case Management System:

1. State Register of Contraventions
2. Register of road accidents
3. Register of emergency restriction orders.
4. Register of protection orders
5. Register of persons and means of transport announced as wanted.
6. Register of blank forms of strict record
7. Register of Contravention Records.
8. Other electronic registers part of the e-Contravention Case Management System.

Other possessors of the departmental state registers to be created at later stages may be other authorities competent to deal with contravention cases which will use the e-Contravention Case Management System. Their possessors are to be determined by the Owner's decision in accordance with the provisions of the Law No 71/2007 on registers.

The MIA as the possessor shall designate and determine the duties of the holder, the technical administrator and the users of the state information systems (AIS) and the duties concerning the manner of keeping the departmental state registers held electronically.

HOLDER:

The IT Service of the MIA, as a specialized subdivision of the MIA responsible for the management of corporate information resources, according to the Government Decision no. 517/2022 and has the role of *holde*r of the e-Contravention Case Management System.

The IT Service of the MIA, as holder of the e-Contravention Case Management System, is also the *holder* of the registers kept in electronic format in the e-Contravention Case Management System.

TECHNICAL ADMINISTRATOR:

The IT Service of the MIA, as a specialized subdivision of the MIA, is responsible for the management of corporate information resources and is the technical administrator of the e-Contravention Case Management System.

The technical administrator is responsible for managing the technical infrastructure (hardware and software), maintenance and development of the information system; security implementation.

Although the technical administrator has the role of super administrator of the software according to the law, the technical administrator does not have the right to use its data, except in the cases provided for by law.

OTHER ADMINISTRATIVE ROLES:

- The Information Technology Service of the MIA is responsible for organizing the protection of personal data within the e-Contravention Case Management System;
- Responsible for cyber security is the Information Technology Service of the MIA according to the MIA Order no. 244 of 18.08.2017 on the information security management system of the MIA.

4.2.2. ENTITIES WITH DIRECT POWERS WITH ROLES OF SYSTEM USERS:

ROLE OF ADMINISTRATORS OF THE E-CONTRAVENTION CASE MANAGEMENT SYSTEM

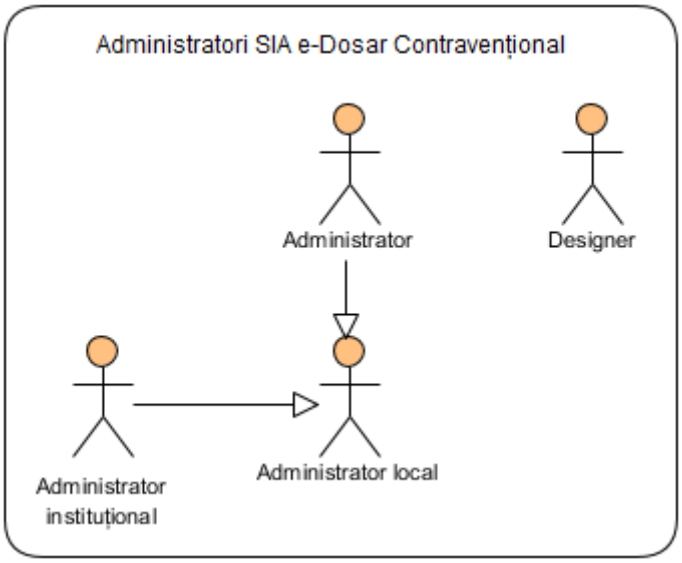


Figure 1. Roles of administration of the e-Contravention Case Management System

National Administrator

The IT Service of the MIA, as a specialized subdivision of the MIA, is responsible for the management of corporate information resources and is the technical administrator of the e-Contravention Case Management System.

The technical administrator is responsible for managing the technical infrastructure (hardware and software), maintenance and development of the information system; security implementation.

Although the technical administrator has the role of super administrator of the software according to the law, the technical administrator does not have the right to use its data, except in the cases provided for by law.

Institutional Administrators

Every authority competent to deal with contravention cases that will use the e-Contravention Case Management System will designate its own administrators who are responsible for setting up the institution's working environment.

The administration of the institution's working environment includes the customized configuration for a given institution of all IT services offered by the e-Contravention Case Management System, roles and access rights to these services.

Local Administrators

In turn, each authority competent to deal with contravention cases may delegate the functions of administration according to competence and territorial distribution to its subdivisions.

In the case of the MIA the following level of hierarchy regarding the administration of users and access rights is established:

1. General Police Inspectorate;
    - Information Technology and Communications Division
2. General Inspectorate of Border Police
3. Migration and Asylum Inspectorate
4. Operational Management Inspectorate
5. General Inspectorate for Emergency Situations

ROLES OF USERS OF THE E-CONTRAVENTION CASE MANAGEMENT SYSTEM

The users and administrators of the e-Contravention Case Management System are presented in the figure below

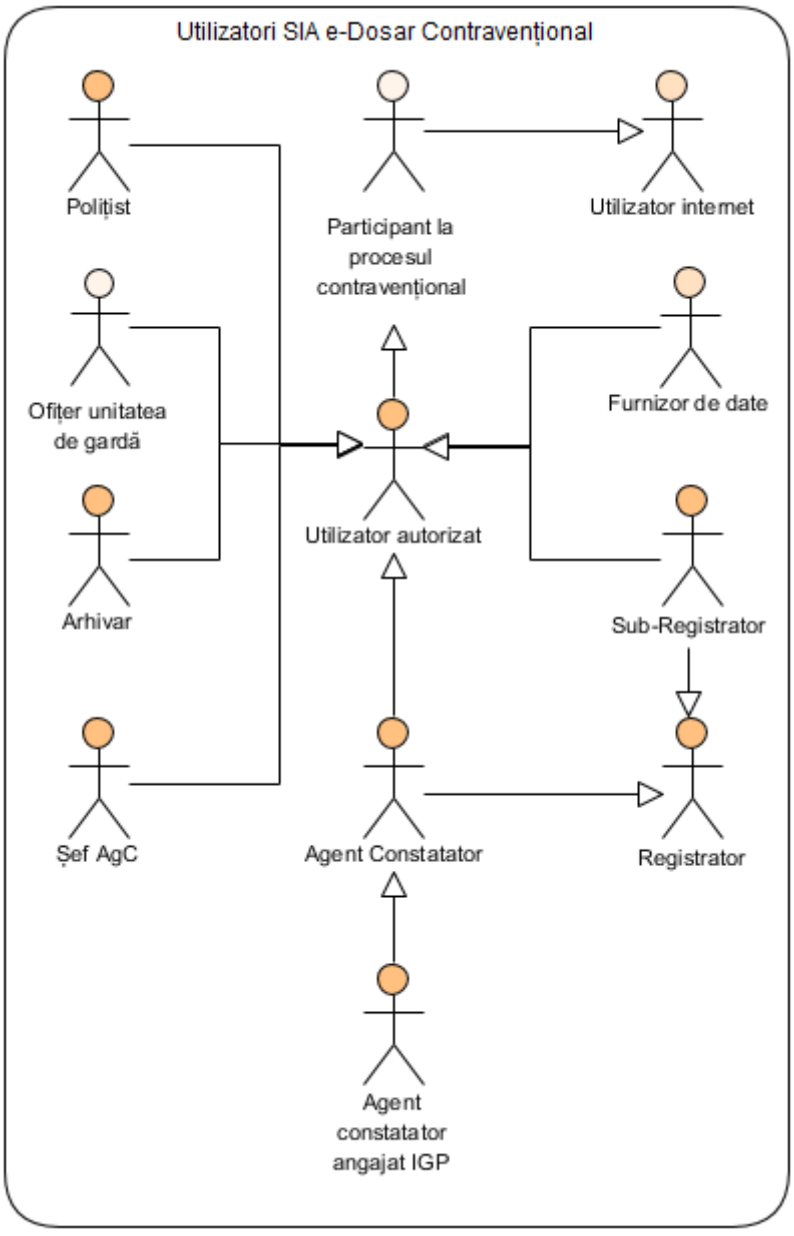


Figure 2. Human users of the e-Contravention Case Management System

INTERNET USERS

Internet user is a generic role that defines any person that through the Internet can have access:

- to public information disseminated through the Web portal of the MIA or the public data portal servcii.gov.md,
- can access specialized services through which the e-Contravention Case Management System communicates with non-user process participants (e.g. via MNotify, MCabinet, MDoc, MPay)
- can access specialized services offered by the platform of the e-Contravention Case Management System, such as: on-line notifications, e-Contravention Record, etc.

AUTHORIZED USERS

A generic role corresponding to any authorized user of the e-Contravention Case Management System and specifying all user interface facilities provided by the System to all categories of authorized users. The given stakeholders have access to the following functionalities:

- has access to the Personal Dashboard through which they access functionalities according to their assigned role;
- has access to the workspace of the user group to which they belong;
- adds new documents/files and processes them within workflows;
- performs tasks within workflows;
- explores the collection of documents stored in the e-Case, data from the records kept in the e-Contravention Case Management System and data from external AIS;
- manages agenda events;
- sends and receives notifications;
- generates documents and reports specific to his/her job duties.

The following describes the types of authorized user roles.

REPORTING OFFICER

The users of the e-Contravention Case Management System with the role of the Reporting Officer are the employees of the authorities competent to deal with contravention cases specified in art. 400–423[12] of the Contravention Code of the Republic of Moldova no. 218/2008, empowered to establish the contravention and/or to sanction it.

REPORTING AGENT EMPLOYEE OF THE GPI

Given the fact that the implementation of the e-Contravention Case Management System will be carried out in several stages and taking into account that this specification refers to the digitization of the activities of the GPI of the MIA, at this stage only the employees of the GPI of the MIA will be considered as users with the role of Reporting Officer.

The list of the groups of MAI GPI employees having the duties of a reporting officer and their specific duties are defined by the MIA Order no. 195 of 17.04.2020 on the establishment of competences in the field of detection/examination of contraventions assigned to the Ministry of Internal Affairs' reporting officers.

CHIEF OF THE REPORTING OFFICER

Chief of the Reporting Officer - is the employee of the authority empowered to deal with contravention cases responsible for distributing referrals, redistributing cases and monitoring their resolution. The Chief of the Reporting Officer has no right to interfere in the work of the reporting officer.

REGISTRARS:

Law 71/2007 on registers sets out in general terms the rights and obligations of Registrars. The duties of the users of the e-Contravention Case Management System who act as Registrars are laid down for each individual register.

The Registrars of the registers to be implemented at this stage of the development of the AIS are established as follow:

Registrars of the *"State Register of Contraventions"* are the participants of the System established by Government Decision No. 517/2022, namely "Registrars of the Register are the participants of the System, according to the Law No. 185/2020 on the Automated Information System for the Recording of Contraventions, Contravention Cases and Offenders and the Contravention Code of the Republic of Moldova No. 218/2008, the competent authorities to resolve contravention cases are:

1. The Court;
2. The Prosecutor;
3. Administrative Commission;
4. Reporting Officer (specialized bodies specified in art. 400–423[12]).

Registrars of the *"State Register of Road Accidents"* are established by Government Decision No 693/2007 on the approval of the Concept of the Automated Information System "State Register of Road Accidents", namely:

1. Ministry of Internal Affairs (police stations)
2. Ministry of Health (medical institutions, forensic medicine center)
3. Ministry of Justice (National Centre for Forensic Expertise)

Registrars of the *"Register of emergency restriction orders"*:

1. Employees of Police Stations or the criminal prosecution officer.

Registrars of the *"Register of protection orders"*:

1. Employees of the Police Inspectorate responsible for the case;

Registrars of the *"Register of persons and means of transport announced as wanted"* are established by Government Decision No 517/2022, i.e. the authorities competent to deal with contravention cases:

1. The Court;
2. The Prosecutor l;
3. Administrative Commission;
4. Reporting Officer (specialized bodies specified in art. 400–423[12]).

Registrars of the *"Register of blank forms of strict record"* are established by Government Decision No. 517/2022, i.e. the authorities competent to deal with contravention cases:

1. The Court;
2. The Prosecutor l;
3. Administrative Commission;
4. Reporting Officer (specialized bodies specified in art. 400–423[12]).

Registrars of the *"Register of issued Contravention Records"*:

1. Employees of the Information Technology Service of the MIA responsible for issuing contravention records;

SUB-REGISTRARS:

According to Law 71/2007 the Registrar is entitled to delegate functions of direct data entry in the Register to the sub-registrar on a territorial basis or according to competence.

The role of sub-registrar is to be applied only in the case of the "Register of blank forms of strict record". The role of sub-registrar is assigned to the employees of the subordinate institutions of MIA responsible for the distribution and registration of the blanks of the strict record forms.

DATA PROVIDERS:

Starting from the fact that the e-Contravention Case Management System is a platform that includes several information resources, such as: the contravention case file and registers, the data providers include a multitude of natural and legal persons who provide data for each information resource, namely:

Data providers for the e-Contravention Case Management System are participants in the contravention process defined by the Contravention Code who are data providers:

1. The person in respect of whom the contravention proceedings have been initiated;
2. The victim
3. The witness
4. The specialist
5. The expert
6. The interpreter
7. The defender
8. The probation counsellor
9. The reporting officer who is the representative of the public authority indicated in art.400-423[12] of the Contravention Code and designated as competent to settle the contravention case and to impose sanctions.
10. The prosecutor
11. The court;
12. The administrative commission

Data providers for the *"State Register of Contraventions"* are provided in the Government Decision 517/2022 and namely:

1. Public Services Agency;
2. Courts;
3. Participants in the System, according to the Law no. 185/2020 on the Automated Information System for recording contraventions, contravention cases and offenders;
4. Participants in the formation of the state information resource "Register of Road Accidents" according to the tasks established by Government Decision No. 693/2007;
5. Natural or legal persons of private or public law who submit to the participants the data on the information objects of the System in the manner established by the regulatory framework;

Data providers of the *"State Register of Road Accidents"* are provided in the Government Decision 517/2022 and namely:

1. Ministry of Internal Affairs (police stations)

2. Ministry of Health (medical institutions, forensic medicine center)
3. Ministry of Justice (National Centre for Forensic Expertise)

Data providers of the *"Register of protection orders"* are:

1. The courts issuing the protection orders;

Data providers of the *"Register of persons and means of transport announced as wanted"* are:

1. Participants in the System, according to the Law no. 185/2020 on the Automated Information System for recording contraventions, contravention cases and offenders;

Data providers of the *"Register of blank forms of strict record"* are:

1. Participants in the System, according to the Law no. 185/2020 on the Automated Information System for recording contraventions, contravention cases and offenders;

Duty Unit Officer

The Duty Unit Officer is responsible for receiving, recording and qualifying alerts. The user in the role of Duty Unit Officer is also the Registrar for the Register of offence referrals (R1) and the Register of other information on offences and incidents r (R2).

Archivist

The employee in the role of Archivist is responsible for the management of the data held in the archive. From the point of view of the e-Contravention Case Management System, access to data and documents in the digital archive will only be allowed to users in the role of Archivist.

DATA PROVIDERS AS INTEROPERABILITY PARTNERS:

The following possessors/holders of public registers the information objects of which are reused in the e-Contravention Case Management System are data providers:

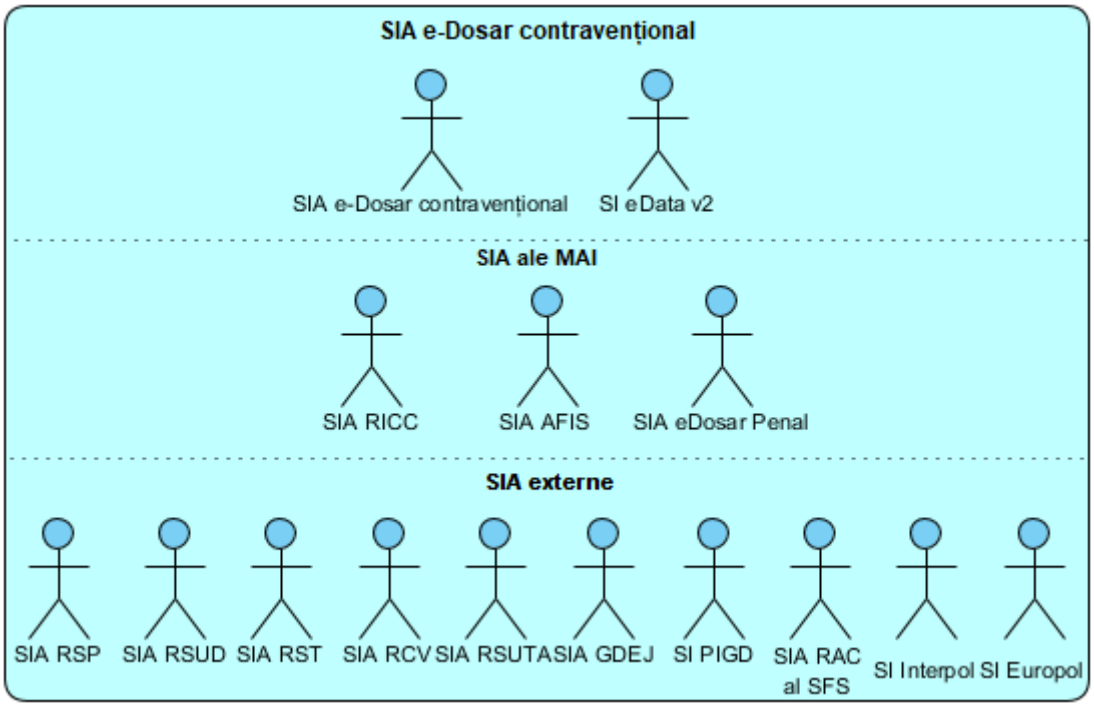


Figure 3. Users of IT systems

1. The Public Services Agency as holder of the state registers provides data from:

- AIS State Register of Population - data on individuals, home address and documents, which have been issued to them;
- AIS State Register of Legal Entities - data on all categories of legal entities, constituted on a legal basis, legal address, rights to exercise various licensed activities;
- AIS "State Register of Transport" - data on means of transport (including units with identification numbers), their owners and other authorized persons, documents and registration numbers;
- AIS "State Register of Vehicle Drivers" - data on the right of the natural person to drive the corresponding means of transport;

2. Ministry of Justice as possessor of:
   - AIS "Management of judicial expertise files" (SIGDEJ) - expert reports drawn up by or with the participation of judicial experts;
   - Integrated Case Management System - court decisions and judgments on contravention cases;
3. The IT Service of the MIA as holder of the MIA's AIS provides data from:
   - AFIS (Fingerprinting Register);
   - RICC AIS (Forensic and Criminological Information Register);
   - AIS e-Criminal Case (once implemented);
4. Land Relations and Cadaster Agency
   - AIS State Register of Administrative-Territorial Units and Addresses - data on administrative-territorial units, streets, buildings and flats when registering residence
   - National Geospatial Data Fund
5. State Tax Inspectorate
   - AIS "Register of administrative fines", part of the Information System of the State Tax Service - to provide information on administrative fines to the State Tax Service in accordance with the provisions
6. Interpol/Europol
   - As an IT service provider for automated exchange of DNA, fingerprinting and vehicle registration data;

4.2.3. AUTHORITIES WITH CONTROL ROLES

Public authorities whose competences are related to the development of new state information resources and/or data contained in the RSDG. These may include:

1. The public institution Electronic Governance Agency (EGov);
2. Public institution Information Technology and Cyber Security Service (STISC);
3. National Centre for Personal Data Protection (CNPDCP);
4. The Ministry of Interior's IT Service as responsible for the MIA's ICT architecture and responsible for the implementation of cyber security within the MIA.

4.2.4. OTHER BENEFICIARY ENTITIES WITHOUT DIRECT ACCESS

Other beneficiaries of the e-Contravention Case Management System, other than users of the system are the following:

1. The citizen must be the ultimate beneficiary of all public policies. The e-Contravention Case Management System is a tool to facilitate communication between the citizen and law enforcement authorities, providing a quicker and more efficient way to check the status of the case and receive notification of penalty decisions, in particular, and to ensure greater transparency of the law enforcement process, giving the citizen the possibility to access information on contravention cases and check how they are handled, in general.

   The citizen will be able to access information from the e-Contravention Case Management System as follows:

   1. Publicly accessible information through the data.gov.md portal, the MIA web portal and other public data sources;
   2. Personalized information by:
      - Requesting a public service offered by the MIA (e.g. e-Contravention Record)
      - Through the citizen portal MCabinet.

2. The State - The e-Contravention Case Management System is the state information resource used for the purpose of managing contravention cases, including thematic departmental electronic registers and electronic document archive related to contravention cases. Through the implementation of the information resource, the State aims to: streamline the process of managing contravention cases, reduce the costs and time required to manage contravention cases, ensure compliance with national and international regulations, increase transparency by enabling citizens to check how contravention cases are managed by facilitating citizen confidence in the correctness of decisions and trust in law enforcement authorities.

3. Public authorities (other than those who have users of the e-Contravention Case Management System)- will benefit from improved communication and access to public and detailed information, if the law so provides on contraventions and related facts.

   Public authorities without direct access will access the information in the e-Contravention Case Management System in the following way:

   1. Detailed information and personalized data, if provided for by law, by addressing requests for information to authorized users of the e-Contravention Case Management System by their areas of competence;
   2. Publicly accessible information through the data.gov.md portal, the MIA web portal and other public data sources;

5. Reference model for the architecture of the MIA's information systems and principles for the development of the e-Contravention Case Management System

5.1. Reference model for the architecture of the MIA's information systems

The MIA future ICT architecture document defines the *reference architecture model for the MIA Automated Information Systems (MIA AIS)* as part of the MIA Integrated Information System (MIA IIS). The MIA IIS reference model is a technology-neutral architecture model based on the principles of SOA (*Service Oriented Architecture*), the architecture principle applied to the implementation of large-scale government architecture. Applications with such an architecture are characterized by the ability to be operated independently of others, to benefit from the functionality offered by other applications and to be replaced by other applications provided that the services offered meet the technical requirements set. A Service Oriented Architecture (SOA) starts from the business model and uses technology to design, develop and deliver IT services based on open standards, thereby improving the reusability of delivered IT components and creating agility to respond to change.

The *MIA IIS* is designed as a set of embedded services and micro-services designed to explore various types of digital content, regardless of where and how it was created and stored, across numerous use cases, by different groups of MIA and external users, realized through a set of integrated platform programs, separate applications that share common APIs and data repositories, and co-opted and reused content service components. The MIA IIS architecture is shown in the figure below:

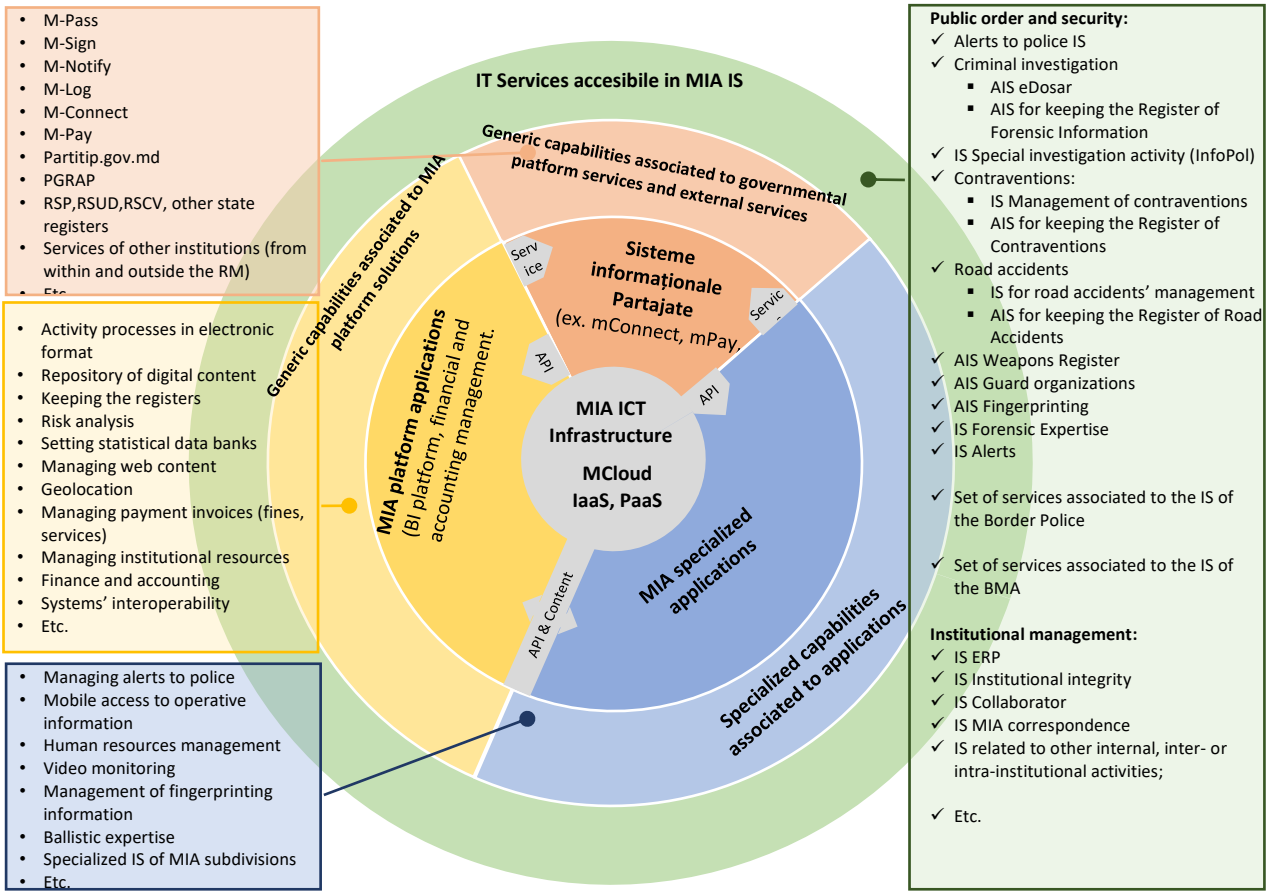


Figure 4. Architecture of the Integrated Information System of the MIA

MIA's IIS is described through functional levels, which are shown in the diagram in the form of concentric circles. Each level has associated specific functions within the IIS of MIA.

Level 1: ICT Services – this functional level represents the IT services used by the MIA in its activities or for the purpose of providing services to third parties. It is how the IIS of the MIA is perceived from the perspective of the MIA's business processes. ICT services can be logically grouped in order to form Automated Information Systems, relevant from the perspective of MIA users and activities. ICT services support MIA's activities and processes in a flexible, business-oriented and technology-independent manner.

Two types of ICT services related to MIA's IIS are identified:

1. ICT services for users, intended for MIA employees or authorized external users (citizens, employees of other institutions and third parties);
2. ICT services for applications, intended to be accessed by other applications in order to enrich their functionality and ultimately deliver ICT services to users. ICT services for applications can be accessed by applications inside or outside the MIA.

ICT services are built by orchestrating and aggregating ICT capabilities accessible within the IIS of the MIA.

Level 2: ICT Capabilities – ICT Capabilities represent the functional characteristics of the IIS of the MIA. ICT capabilities can be orchestrated and aggregated to build ICT services. One or more aggregated capabilities form an ICT service from the perspective of MIA's business processes. ICT capabilities are associated with applications in the MAI application architecture, or ICT services provided by third parties. The orchestration and aggregation of ICT capabilities is done by configuring, adapting and integrating applications from the MIA application architecture. The development of new ICT capabilities involves the acquisition and implementation of new applications or the development of existing ICT systems. Alternatively, MIA may contract external ICT services that will provide the ICT capabilities required by MIA.

Level 3: Application Architecture - includes all application components (application platforms, distinct applications and components thereof) owned by MIA or accessible to MIA for use. The functional and non-functional features of MIA applications constitute the ICT capabilities on the basis of which ICT services are produced. In the context that a MIA information system presents a logical grouping of different ICT capabilities, MIA information systems may be based on one or more applications from the MIA application architecture. MIA's application architecture has a modular structure, which ensures flexibility to respond to MIA's needs while facilitating the re-use of existing components. All applications support unique standards for technical interoperability. Integration of applications is implicitly ensured through the MIA interoperability platform. Data exchange with applications outside the MIA application architecture is by default carried out through the government interoperability platform.

The following major groups of applications form the application architecture of the MIA:

1. MIA platform applications: have ICT capabilities that meet the common needs of several MIA processes and activities. This facilitates the re-use of platform applications to produce distinct ICT services;
2. Specialized MIA applications: have ICT capabilities needed to support particular MIA activities and processes. Specialized capabilities are developed when they cannot be provided by orchestrating generic capabilities. They are also associated with applications already deployed and that will continue to be used
3. Government and third party IT services: have ICT capabilities characteristic of government services and intended for common use by public authorities. They may also meet the needs of the MIA, in which case they are co-opted and treated as an integral part of the MIA's application architecture.

The applications in the MIA application architecture (including government services) are interoperable.

MIA develops, implements and operates applications as part of MIA's IIS in order to provide the ICT capabilities required to produce ICT services. Whenever MIA identifies the need for new ICT capabilities that cannot be provided by MIA's current application architecture, it takes the following actions, in the following order:

1. Analyses the possibility of obtaining the required capabilities by integrating available government services into the MIA application architecture.
2. Analyses the possibility of developing current platform applications. New ICT capabilities can be provided by implementing new functionalities of the platform applications.
3. Analyses the rationale for the development of new specialized or platform applications.

Level 4: Technology Architecture – includes technology infrastructure components to ensure the ICT environment necessary for the efficient and secure operation of the applications in the MIA application architecture, as well as their accessibility by users and other applications. The technology architecture includes: data centers, data processing and storage equipment, communication networks, operating environments and system software.

5.2. Principles for the development of the e-Contravention Case Management System

The process of conceptualizing an automated solution starts with the definition of principles, the use of which will ensure the achievement of the set objectives and the development of a solution that is efficient, easy to use and maintain, secure and adaptable to future changes. The following principles define the approach to be taken in the design and development of the e-Contravention Case Management System.

5.2.1. General architectural principles

Prevalence of principles - The only way for MIA and MIA's subdivisions to benefit from quality ICT services aligned with business needs is to consistently and unambiguously apply a single set of ICT architecture principles. The ICT architecture principles apply to all ICT development projects and to MIA's subdivisions when managing the ICT domain.

Maximizing the benefit - Decisions relating to the ICT domain are made with a view to maximizing the benefit produced for MIA as a single entity. This principle is based on the concept of "MIA benefit first". The benefits pursued at the level of the MAI bring more long-term value than the benefits pursued at the level of a single subdivision of the MIA. The application of this principle, however, should not prevent the MIA subdivisions from exercising their key functions.

Everyone's responsibility for ICT - All stakeholders participate in ICT decision-making and implementation. All sub-divisions of the MIA are stakeholders in ICT decisions at MIA level. Business experts and ICT experts from MIA subdivisions should form joint teams to address MIA needs and implement ICT projects aligned to these needs.

Business continuity - MIA must be able to continue its key operational activities in the event of the failure of ICT systems. The implementation of ICT systems brings multiple benefits for MIA and MIA subdivisions, at the same time it increases the operational dependency of processes on ICT systems. To ensure business continuity this dependency must be managed on two dimensions: preventive; reactive.

Preventive: ICT systems must be reliable and have a high level of resilience to incidents (internal and external) that could affect them. Continuity and security requirements must be considered at the planning stage of ICT systems (application systems and infrastructure systems). Then, it must be ensured that these requirements are correctly implemented, work and remain current over time. The MIA must provide the necessary capabilities to ensure the above.

Reactive: The MIA must plan in advance how it will continue key operational activities in the event of the failure of ICT systems. The deployment of new IT systems must be accompanied by the development of an appropriate Continuity Plan.

Service orientation - MIA's large-scale ICT architecture must be oriented towards the delivery of ICT services to MIA's business processes. Service orientation at the ICT architecture level allows MIA to be more agile in adjusting business processes to new needs, enables the implementation of new processes and supports the implementation of unrestricted information flows inside and outside MIA.

Compliance and legality - MIA will manage and use the ICT domain in compliance with applicable legal regulations, including those related to intellectual property protection. All activities of MIA and MIA's subdivisions are carried out strictly in accordance with applicable legal regulations. Activities related to the ICT domain must adhere to this practice.

Principle of applying best practice and industry standards ensures that the solution developed is modern, has high reliability because it is based on the experience of other similar solutions and is compatible with existing systems both in the country and abroad that comply with industry standards;

Principle of extensibility, according to which the components of the e-Contravention Case Management System provide facilities for adjusting and extending the existing functionalities in order to ensure compliance with constantly changing needs;

Principle of progressive development, according to which the development of the system and the continuous modification of its components are carried out in accordance with advanced technologies;

Principle of consecutiveness, which involves the development and implementation of the system in stages;

Principle of operational efficiency, which implies optimizing the quality-cost ratio;

Principle of simplicity and user-friendliness: this involves designing and implementing all user-friendly program components based on exclusively visual, ergonomic and logical design principles;

Principle of system auditing, which involves recording information about changes that occur in the system, so that it is possible to reconstruct the history of a document or its condition at a previous stage;

Principle of personal responsibility – which provides for the personal liability in accordance with the legislation in force of all persons having access to the e-Contravention Case Management System for unauthorized access, use and actions. In this sense, access to data is personalized and any action to use the system is logged with the application of non-repudiation;

Principle of information security states that information is protected on the basis of integrity, availability, confidentiality, incontestability and authenticity. All information is subject to a security assessment based on these 5 factors. The traceability approach to security includes the initiation and proper application of audit system and monitoring tools. The availability of information sharing and disclosure should be balanced with the need to limit the availability of confidential, proprietary and sensitive information;

Principle of security by design is an approach in software and hardware development that aims to make systems as free as possible from vulnerabilities and impervious to attack using such measures as continuous testing, authentication guarantees and adherence to good programming practices;

5.2.2. Principles for data architecture

Data sharing - Data is shared within MIA and used in common to fulfil duty tasks. Timely access to truthful information can significantly improve the decision-making process and the effectiveness of MIA activities. It is simpler and more rational to maintain the quality of data in one source and then share it, than to control the quality of the same data in different sources. Also, the timeliness of the data depends on the path the

data takes from the source that created it to the entity that consumes it. This path must be minimal. The speed at which data is collected, created, transmitted and consumed depends on the ability of MIA to share the data.

Data accessibility - Data is accessible to users for the fulfilment of duty tasks. Broad access to data allows for more effective activities and more efficient decision-making. MIA employees must take part in the processes of creating, modifying, transmitting and accessing data within the application systems, if their duties involve such activities with data (the practice of data being created by one employee and recorded by another is not encouraged). This assumes that users within the MIA are adequately trained and can use data and application systems in a responsible manner. Employees will be primarily responsible for the accuracy of data created and modified and for justifying access to data as required by the service.

All data have a Data Trustee - For each type of data, a Data Trustee is designated within MIA who will be primarily responsible for the completeness and accuracy of the data at MIA level. All activities related to data collection, recording, modification, storage and access will be coordinated centrally with the involvement of the data holder. In this way, uniform and effective mechanisms can be implemented to ensure control over data quality. To align with other principles, the data holder should not decide who has access to the data, only how access is controlled to meet data quality standards. This principle applies both to data held by the MIA and to data provided by external entities.

Data has a single primary reference source - One reference source is established and used for any data type, and only one. For the same data set to have the same content for all entities consuming it (people, systems), there must be only one primary data source. The primary data source must guarantee the completeness and correctness of the data, and it shall be referenced in all cases involving the type of data concerned.

Principle of unique identification - stipulates that each copy of the information object is assigned a unique system-wide identification code by which it can be located and accessed;

Principle of secure data – stipulates that data is entered into the e-Contravention Case Management System only on the basis of records from trusted information sources and that data is entered into the system only through authorized and authenticated channels;

Prevalence of data in electronic form - Whenever data can serve its purpose in electronic form, it will not be reproduced on paper. Whenever data must exist in paper form, there will be a copy of the data in electronic form. The use of data in electronic form in business processes has obvious advantages: it can be processed automatically, the quality of the data is higher, the data is more accessible, the costs are lower. If there is a need to have data in paper form, translating it into electronic form will also provide a significant part of the benefits listed.

Common data definition vocabulary - Data are fully defined at the level of the MIA and definitions are easily understandable and available to all stakeholders. Data managed by different applications, including applications that are in development, must use the same data definition vocabulary. In this way, applications will be able to integrate and share data (ensuring interoperability). In addition, a common data vocabulary is also needed to facilitate communication between the responsible persons.

Principle of semantic interoperability capability – states that the RSDG AIS data model is semantically and syntactically aligned at national and international level. Common semantic assets promoted at European and international level are used to define the local vocabulary;

Data security - Data is protected against unauthorized use and disclosure. Data will be protected proportionate to its sensitivity. Data accessibility and shared use of data within MIA must be balanced against data security requirements. The legal regulations applicable to data protection, including personal data, are mandatory and are to be implemented in the e-Contravention Case Management System.

Minimization of the personal data set - data processing systems should be designed and selected according to the purpose of collecting and processing as little personal data as possible.

5.2.3. Principle for applications' architecture

Alignment with large-scale government architecture – implies unreserved compliance with the principles and architecture established in large-scale architecture, such as: service-based architecture (SOA), interoperability, reusable services and components, portability, flexibility, etc. If large-scale government architecture is good for the whole of government then it is good for the MIA. Large-scale architecture will provide MIA with opportunities to control and reduce complexity as well as develop new, simpler and better solutions. MIA will also draw on the knowledge and experience of the government.

SOA Architecture - The ICT architecture is developed with the application of specific principles of a service-oriented system architecture. A well-managed SOA environment will enable MIA to respond quickly to the tasks at hand, increase the agility of operational processes and consolidate existing IT resources through reuse. Application components will be able to be deployed without rigid mutual dependencies. Components will interact through external interfaces implemented on the basis of open, technology-independent standards. This gives flexibility of choice of technologies and independent lifecycles for the Information Systems used by MIA. It will also allow stakeholders to select alternative technology options for data entry and access capabilities;

Ensuring interoperability - The interoperability framework is established and implemented at the MIA application architecture level. It is aligned to the government interoperability framework. Adoption of the government interoperability framework provides an opportunity to reduce the number of interactions between systems by establishing a single set of working arrangements and a single technical way of interconnection.

Autonomous service orientation - The application architecture is oriented towards autonomous IT services (functional and institutional). Complex services can be easily composed if there are stand-alone services that will simplify interactions and respond to citizens' needs and allow faster changes or subsequent substitution of technologies. Interoperability is achieved by providing partners with public interaction interface.

Weak dependencies at the application architecture level - Applications and application components are developed with minimal dependencies on other applications and application components. Adherence to this principle in the implementation of the Interoperability Framework helps to reduce the following dependencies: communication protocol dependencies, syntax and format dependencies, semantic, temporal, behavioral and organizational dependencies.

Independent from technology platform - states that preferably application solutions should be independent from specific technology options and therefore be able to operate on a variety of technology platforms. Technological independence enables application solutions to be developed, updated and operated in the most efficient and timely manner. Otherwise technology, which is subject to continuous ageing and vendor dependency, becomes paramount to the detriment of user requirements.

Application Re-use and Shared Use - MIA will re-use or share to the maximum extent possible MIA-owned or government-owned applications within the shared government platform.

User-friendly applications - Applications are easy and convenient for users to use. The present technologies are transparent to users. User-friendly apps will allow users to focus on performing tasks in exchange for understanding the technologies on which the app is based. Rapid user training is another rationale.

5.2.4. Principles for technology architecture

Long-term focus for technology architecture - Given that infrastructure investments are quite significant, decisions need to be based on a long-term strategy, even if this may be at the expense of short-term profitability. It is important to identify business plans and objectives for both the short and medium term as well as the long term, which will allow for tailored planning and design that will ensure scalability and flexibility in the future.

Use of open technologies in the technology architecture - Open technologies enable the implementation of an efficient and flexible technology infrastructure. By using the open technology stack, technical diversity will be controlled, which will reduce the complexity of the architecture and consequently of the deployed infrastructure, allowing for more efficient management and flexibility. Open technologies and architectures also allow to take advantage of industry trends and future technologies. Such an approach provides a higher return on investment by extending the useful life of infrastructure components, which facilitates the portability of applications to smaller or larger platforms without the need for extensive re-engineering and will increase the likelihood that replaced hard components can be used effectively elsewhere within the institution.

Scalability, adaptability and flexibility for the technology platform - The technology architecture must take into account the future needs of the organization to ensure business continuity. The architecture must be identified/defined in such a way that it is easy enough to modify it in order to increase the capacity of the resources made available, the speed of response to possible changes and to raise the level of availability of the services delivered from it. To this end, it is important to identify how to scale each component part of the infrastructure.

Use of the common government platform - Whenever the common government platform - MCloud, can serve the purpose, it will be selected for the provision of the technological platform necessary for the implementation of the application systems of the MIA and subordinate subdivisions.

Virtualization of resources at the technology architecture level - Virtualization of resources enables their efficient use and ensures the scalability of systems. The use of separate physical resources results in servers being used at a capacity not exceeding 50% of the total computing resource. Virtualization of resources allows their management for various business purposes and the separation of physical and virtual resources for various systems and services, which allows optimization of IT processes and procedures, more efficient spending and management of resources, better control and simplified management of IT services.

Technology architecture security - Regardless of how resources are used and how data is managed, security is a key area in IT infrastructure management, which is why it is very important to identify the security aspects of each area, starting with physical security (at the physical level), network security, application security and data security. It is strictly necessary to use the concept of "least privilege" in managing access to resources and data and to continuously monitor all activities related to this domain.

Reliability of the corporate network - In the context of implementing a large-scale corporate architecture, applications and IT services rely on the corporate network to communicate. MIA's corporate network will ensure a high level of reliability, resilience and security for data, video and voice transport.

6. Architecture of the e-Contravention Case Management System

6.1. Architecture components of e-Contravention Case Management System

The architecture of the e-Contravention Case Management System is established on 4 dimensions:

1. *Functional (business) architecture* – describes how the software product will function, how it will be used to perform business activities and support the organization's business processes, and how the various components of the system interact with each other to provide this functionality. Compared to the IIS reference model MIA includes the ICT Services to be provided by the IT solution.
2. *Data architecture* - includes information artifacts and the set of rules, policies, standards and models that govern and define the type of data collected and how it is used, stored, managed and integrated within an organization and its database systems. Provides a formal approach to creating and managing the flow of data and how it is processed across an organization's IT systems and applications. The purpose of defining data architecture is to ensure that data is managed efficiently and effectively across the system, while ensuring its integrity, confidentiality and security.
3. Application Solution Architecture – defines the list of capabilities that must be owned by the application components required to provide digital support for the business functionalities and information resources with which the e-Contravention Case Management System is to interact. It includes a reference model that is intended to guide and ensure a clear understanding of the application architecture of the e-Contravention Case Management System to be implemented.
4. Technology architecture - contains information and artefacts related to the technology components that ensure the proper functioning of the e-Contravention Case Management System application components (operating environments, support services, DBMS, server hardware, data storage hardware, local and corporate networks, data center premises). The role of the technology architecture is to ensure appropriate technology platforms for the proper functioning of the business applications and ICT services at the parameters required by the business.

6.2. Functional (business) architecture

6.2.1. Business processes and functions to be automated

The following business processes and functions are to be supported digitally in the e-Contravention Case Management System:

6.2.1.1. The process of recording the alerts.

The process includes performing the following key business functions

- Receipt of the reports received through different channels, such as:
  - Referrals submitted to the units on duty (referrals and other information);
  - Referrals submitted online;
  - Self-reporting, including self-reporting from AIS Traffic Control;
  - Alerts received by telephone (via dispatchers, duty units or hotlines);
  - Referrals received by official correspondence (sent via the Registry);
  - Prosecutor's order to reclassify a criminal case as a contravention case
  - Referrals on cases forwarded by other authorities according to their competence
  - Alerts sent via the 112 service.
- Management of alerts:

- Primary recording of alerts and forwarding to the head of the subdivision for qualification of the fact and determination of the person responsible for examination
- Recording in the information about the referral in the Register of offence referrals (R1);
- Recording in the Register of other information on offences and incidents (R2);

- Concluding reports on registered alerts
- Keeping track of electronic documents/copies of paper documents collected in the process of alert registration;
- Interoperability with the AIS:
  - AIS 112 - for the purpose of receiving alerts received by the 112 service
  - AIS e-Criminal Case File - for the purpose of registering self-reporting and tracking the status of the criminal case;
  - AIS e-Contravention Case - for the purpose of registering self-reporting and tracking the status of the contravention case;
  - Mobile solution to support the work of the RO for the detection of violations in flagrante delicto - for the purpose of registering self-reporting
- Archiving the referral of offences and other information on offences and incidents

Workflow associated with the process of registration of referrals

The workflow associated with the process of registration of referrals is defined by GPI Order No 562/2021 on the approval of the Standard Operating Procedure for the receipt, registration, recording, examination and archiving of referrals. The Standard Operating Procedures for the receipt, registration, recording, examination and archiving of complaints are set out in Annex A1

6.2.1.2. The activity of establishing infringements by the reporting officer in flagrante delicto (self-reporting).

The process includes performing the following key business functions:

- Accessing data from approved mobile devices for the purpose of establishing infringements. At least the following approved mobile devices are to be integrated:
  i. LTI 20/20 ,,TruCAM" (laser) speed measuring device for vehicles;
  ii. Drager Alcotest 7510 breath ethanol concentration analyzer;
  iii. Drager Alcotest 6820 breath ethanol concentration analyzer.
- Taking photo, video and audio images from non-approved mobile devices for use as evidence. Smartphones and tablets are considered as non-approved mobile devices.
- Video/photo recording of the moment of reading/signing the contravention report by the offender. It is expected that the recording can be used as evidence in the case of contesting the fact
- Sound recording of the fact of the communication of the person's rights by the Reporting Officer (or photo/video recording of the fact that they were made aware of them - alternatively, a tick can be requested on each point on the tablet with a photograph of the moment).
- Automatic reading of QR code information from ID documents (it is expected that ID card, driving license and other documents will contain QR codes).
- Legitimizing the person
- Access to information about the person (natural/legal) and objects (e.g. car, property, weapon, etc.) in electronic state registers, information systems held by the MIA and by external bodies.
- Registration of the location where the contravention took place.

- Generation and self-completion of the "self-report form". The "self-report form" is created:
  - By the system, automatically:
    1. On receipt of the structured message with the pre-filled "self-report form" fields from an infringement detection AIS (e.g. Traffic Control AIS)
    2. Based on a predefined scenario selected by the reporting officer (e.g. road accident, speeding, etc.). Scenario includes pre-completed templates of the "Self-report form".
  - At the deliberate indication of the reporting officer:
    1. The system generates a "self-report form" in which the system metadata (system number, document name, data of the investigating officer, date and time of creation, etc.) are filled in. The system assists the reporting officer in filling it in by suggesting different information according to what has been filled in (e.g. when filling in the IDNP, the person data will be extracted from the SRP, when filling in the CC article number, the text will be suggested, etc.)
- Transmission to the Alert registration process the "self-reporting form" and evidence
- Identification of the person based on facial image, including:
  - Capturing the face image;
  - Searching the person in the SRP based on facial image using PSA facial recognition solution;
- Keeping records of activities involving the processing of personal data in connection with the carrying out of citizens' identification and self-checks by employees of the Ministry of Internal Affairs and its subordinate institutions

6.2.1.3. The process for managing contravention cases and related activities.

The process includes performing the following key business functions:

- Receipt of referral or self-report
- Distribution of referrals to the reporting officer by the Chief of Reporting Officer
- Acceptance of the distributed contravention case by the Chief of the Reporting Officer;
- Recusal of the reporting officer
- Finding of contravention or lack thereof,
- Forwarding the case according to jurisdiction
- Examination of the contravention:
  - Identification of persons
  - On-site search
  - Search
  - Collection of objects
  - Filling in procedural action forms
    - Retention
    - Forced apprehension
    - Removal from driving the vehicle
    - Removal and bringing the vehicle to the car park
    - Suspension of the right to use the vehicle
    - Seizure

  - Application of restriction orders
  - Hearing procedural parties (witness, victim, suspect, etc.)
  - Ordering the carrying out of technical-scientific findings and expertise
  - Summoning the parties
  - Documentation of the road accident
  - Dispatching the contravention case according to jurisdiction
  - Proposal to reclassify the contravention case as a criminal offence
  - Conclusion of cooperation agreement
  - Completion of exit letters
  - Etc.
- Entering completed paper procedural documents at the crime scene

- Taking of the sanction decision
  - Establishing the sanction
- Sending the decision on the contravention case to the bailiffs for enforcement
- Recording of penalty points awarded for committing traffic offences;
- Activities related to the suspension of the exercise of the special right to drive vehicles in case of accumulation of 15 penalty points, including:
  - Proposal for applying the suspension of the exercise of the special right to drive vehicles to the chief, deputy chiefs and heads of territorial subdivisions of the National Public Security Inspectorate.
  - Taking action as decided by the head, deputy heads and heads of territorial subdivisions of the National Public Security Inspectorate.
  - Collecting the driving license and forwarding it for storage.
- Attending the trials for contested, reassessed or appealed cases
- Placing the contravention case file in the archives
- Collecting statistics and completing reports
- Data exchange and collaborative work with process partners via their AIS.
- Access information from official and operational sources, including State Registers, AIS held by the MIA and process partners
- Document signing and verification with:
  - qualified electronic signature
  - electronic holographic signature
- Sending notifications
- Handling of incoming and outgoing correspondence related to case management, including:
  - Completion and coordination of outgoing letters
  - Recording outgoing correspondence
  - Recording incoming correspondence
  - Monitoring of response submission deadlines
- Interacting with participants in the process (witness, suspect, victim, etc.) who have a role in the contravention process via MCabinet and MNotify

- Sending documents to MDoc
- Viewing documents, notifications and other messages in MCabinet
- Receiving electronic documents from MConnect, email
- Notifying participants via MNotify

- IT service for generating payment accounts for fines and payment tracking (Billing), including:
  - Management of treasury accounts associated with fine types.
  - Generation of payment account for fines and forwarding the account to MPay
  - Fine payment tracking
- Monitoring enforcement discipline. The function includes activities such as:
  - Monitoring procedural deadlines and compliance with tasks ordered by the Chief.
  - Identifying the need to Reassign the contravention case
  - Monitoring individual performance and workload of the reporting officer.

Workflow associated with the contravention case management process and related activities

The workflow associated with the "Contravention case management process and related activities" is regulated by the Contravention Code of the Republic of Moldova (CC) - Law No 218 of 24.10.2008 and a number of internal instructions. The workflow diagram of the contravention process is presented in Annex No. A2

6.2.1.4. Activities related to the maintenance of departmental state registers related to the contravention process.

The process includes the performance of the following key business functions:

- Carrying out registration, amendment and deletion of records activities - activities are carried out within the "contravention case management and related activities" workflow. The registration, signing of confirmatory documents, as well as the occurrence of events (e.g. cancellation of penalty points on expiry of the deadline) within the workflow serve as the basis for the registration/modification/deletion of records from the registers.
- Deletion scheduling service - refers to the ability to hold deletion rules for records in accordance with retention rules. A record cannot be retained if the legal basis under which it was made has expired. The deletion schedule is used to manage the life cycles of records according to established legal procedures. Similarly, the service ensures that on disposal a residual record remains for the lifetime of the system. The residual record, demonstrates not only that a record was once active, but more importantly, that the record was properly disposed of in accordance with an appropriate disposal protocol.
- Retention service - the ability to prevent a record's deletion rule from being applied in the event of a recurring reason. Record removal does not always mean destruction. According to Law 133/2011 the disposal of records can be: by archiving, de-personalization, or destruction.
- Search, retrieval and presentation of data - the ability to retrieve and present records and metadata in response to queries.

The following departmental state registers associated with the contravention process are to be managed in the e-Contravention Case Management System:

1. State Register of Contraventions;
2. Register of traffic accidents;
3. Register of emergency restriction orders;

4. Register of restriction orders
5. Register of persons and means of transport announced as wanted;
6. Register of issued contravention records

Workflow associated with the process of keeping departmental state registers related to the contravention process

The generic workflow associated with the " Process of keeping departmental state registers related to the contravention process " is presented in Annex No. A3.

At the same time, the digitization of the "Process of keeping departmental state registers related to the contravention process" will take into account the specificities laid down in the Regulations for keeping each individual register.

The following aspects specific to the keeping of each register are considered critical and will be taken into account when designing and developing the e-Contravention Case Management System:

1. State Register of Contraventions (established by Government Decision no. 517/2022).
   - The registration/modification of data in the register is based on the following events:
     - Signing within the workflow of the following documents:
       1. decision on the examination of the contravention on the basis of the personal finding of the reporting officer
       2. decision on the contravention case
       3. the minutes of the contravention
       4. other documents configurable by the administrator
     - Recording of documents in the e-Contravention Case:
       1. court decision on the case
       2. appeal, recourse
       3. Prosecutor's order on the prosecution of a contravention, in relation to the non-prosecution or termination of prosecution
2. Register of Road Accidents (established by Government Decision no. 693/2007). The process includes the following key business functions:
   - The recording/modification of data in the register is based on the following events:
     - Recording of the "referral" / "self-report" on the road accident
     - Signing within the workflow of the following documents:
       1. decision on the examination of the contravention on the basis of the personal finding of the reporting officer
       2. decision on the contravention case
       3. 3. the minutes of the contravention
       4. 4. other documents configurable by the administrator
     - Recording of documents in the e-Contravention Case:
       1. court decision on the case
       2. appeal, recourse
       3. Prosecutor's order on the prosecution of a contravention, in relation to the non-prosecution or termination of prosecution
     - Dissemination of statistical information, including:
       - Generation of statistical reports for internal use;
       - Dissemination of statistical data of a public nature;

- Reporting to CARE (Community database on Accidents on the Roads in Europe) in accordance with the requirements of CADaS (Common Framework of Data on Road Traffic Accidents in Europe).

- Receipt of documents from data providers:
  - Ministry of Health (health institutions, Forensic Medicine Centre)
  - Ministry of Justice (National Forensic Expertise Centre)

3. Register of emergency restriction orders.
   The procedure for the formation and keeping of the Register of emergency restriction orders is defined by GPI Order No. 93 of 28.03.2023 on the approval of the methodical instruction on police intervention in preventing and combating cases of domestic violence.
   The process includes performing the following key business functions:
   - Recording/modifying data in the register, which is carried out based on the following events:
     - ordering the issuance of the emergency restriction order against the abuser by the reporting or prosecuting body;
     - assignment of the record number in accordance with the Classification of the Codes of the Regions of the Territorial Subdivisions of the Police, used for entry into the Central Data Bank, in accordance with Interdepartmental Order No 121/254/286-0/95 of 18 July 2008 on the Single Record of Offences, Criminal Cases and Offenders.
   - Systematization and record keeping of emergency restriction orders issued by the Police in respect of domestic abusers by the Head of Community Interaction Service/Principal Officer;
   - Keeping the register of records of emergency restriction orders which is provided by the Secretariat of the subdivision, according to the provisions of the Order of the Minister of Internal Affairs No. 401/2016 on the implementation of the Indicator of documents and their retention periods;
   - Supervision of the execution of the measures imposed by the emergency restriction order, which involves:
     - initiation of the accumulation file (record sheet) of the tertiary prevention work by the employee of the Police Sector, within the radius of the aggressor's domicile;
     - processing explanations from the victim, family members, neighbors or other persons who come into contact with the family members, from the offender and confirmatory materials.
4. Registration of persons and means of transport announced as wanted – Register of persons and means of transport announced as wanted;
   The process includes performing the following key business functions:
   - registration of persons and means of transport in orientation;
   - registration of incoming information from other law enforcement bodies and process partners - data providers (including import of incoming data in electronic format);
   - dissemination of information to recipients of information (including in electronic format);
5. Register of offence referrals (R1);
   The process includes performing the following key business functions:
   - Primary recording of data in the register is based on:
     - referrals (denunciation or complaint) lodged
     - self-reporting by the reporting officer or criminal prosecution officer
   - Change of data based on events (e.g. assignment of case to reporting officer/prosecution officer in case of referral, proposal to refuse to prosecute, etc.)
   - Entry of records in the archive;
6. Register of other information on offences and incidents (R2);
   The process includes performing the following key business functions:

- Primary recording of data in the register is based on:
  - Alerts about offences or other breaches received verbally, via telephone, 112, etc. to the duty unit
- Change of data according to events
- Entry of records in the archive;

6.2.1.5. Activities for managing the blank forms of strict record keeping

The process includes performing the following key business functions:

- Generation of unique numbers of the record forms and their assignment according to the hierarchical structures of the reporting officers;
- Allocation of unique numbers according to distributed blanks
- Keeping track of the use of unique numbers of records, including redrawn records.

6.2.1.6. E-Contravention Record Service

- Requesting the Contravention Record and validating the right of access
- Keeping the register of issued Contravention Records, including:
  - Workflow related to registration, modification and deletion activities. The primary registration of data in the register is done based on the request of the natural or legal person
  - The basis for the documentary registration is the e-Record issued as requested
- management of the series and numbers of the blanks used for printing the Contravention Record and the keeping of the records drawn up.

6.2.1.7. Management of documents and files in the electronic archive:

The transfer of the Contravention Case Files, documents and records from the registers to the archive shall be carried out in accordance with the provisions of MIA Order No. 401/2016 on the implementation of the Document Indicator and the terms of their retention

The process includes carrying out the following key business functions:

- Transferring the e-file of the contravention case to the archive
- Transition of records from departmental state registers to the archive
- Workflow related to requesting access to documents stored in the electronic archive Workflow related to requesting access to documents stored in the electronic archive

6.3. Data architecture

The data architecture of the e-Contravention Case Management System is represented by the totality of information artefacts contained in the AIS, organized according to the needs of the application solution. Given that the e-Contravention Case Management System includes several functional components using different data sets and models, the architecture of the e-Contravention Case Management System is formed by the totality of the data architectures of the constituent components. The data architectures of the functional components of the e-Contravention Case Management System and the particular requirements are presented in the annexes describing these components. This chapter describes the general approach and requirements to be considered when designing and operating the data architecture of the whole system as well as in particular for each functional component.

At least the following information artefacts are to be identified:

1. System documents and their structure

2. List of data flows with external systems (interoperability model) and description of message structure.
3. List of electronic registers kept in the e-Contravention Case Management System
4. List and description of the information objects held in the registers
5. List of information objects describing the workflow.
6. List and content of system nomenclatures

All information objects contained.

6.3.1. Conceptual data model associated with the workflows in the e-Contravention Case Management System

The data model associated with the workflow management component - is intended to support workflows in digital format. It is based on the XPDL/BPMN standards for describing the taxonomy of digital workflows and the Wf-XML specification for interoperability at workflow level. This specification defines how business processes are defined by modelling tools to be executed by an application workflow management component. If a business process is defined in XPDL by a modelling tool, a workflow management application component can execute that business process. Likewise, the use of standards allows traceability of processes running in multiple WfMS systems. The process launched in one system will continue in another without being noticed by the user.

According to the objective of creating the Electronic Contravention Case File, the data architecture of the future conceptually automated solution is guided by the following decisions:

1. All information objects are managed exclusively in electronic mode.
2. Information objects are maintained using open standards of digital data representation.
3. The e-Contravention Case Management System will operate with the following two categories of information:
   a) Structured information - represents documents with structured content in the form of attributes of related objects relevant to the contravention process, for which the proposed data model is presented later in this section;
   b) Unstructured information - represents information of any type (e.g. images, files with video, audio content, etc.). This will be recorded by means of electronic documents describing the information, resulting from obtaining a scanned copy of an original printed document (scanned documents may be marked "true to original" certified by digital signature).

According to these decisions the following key artifacts of the data architecture are characteristic and are to be supported by all functional components of the e-Contravention Case Management System:

1. Electronic document

The electronic document is the main entity that is worked with in the digitized contravention process. Any information identified in structured (document) or unstructured form (message, audio/video file, etc.) can be considered a document. An electronic document is characterized by the following properties:

1. The electronic document is the basis for the e-Contravention Case Management System and the processes for working with it. Each document added to the e-Contravention Case is accepted in qualified electronic form. Documents received in the traditional paper or non-qualified electronic form shall be transferred into qualified electronic form by the reporting officer or other authorized person.

2. All documents generated by the e-Contravention Case Management System related to the handling of contravention cases shall be produced in (qualified) electronic form. Parties who cooperate with the reporting officer and need documents represented in a different way shall use document viewing services or may request a simple or holographical authenticated copy. The parties may access the electronic document whenever necessary to obtain qualified copies of the document or to re-generate non-qualified representations/copies of the document.
3. Documents bearing a holographic signature will also be used in digital format. The scanned copy of these documents shall be confirmed by the digital signature of the reporting officer or authorized person.
4. Any electronic document can be uniquely identified in the e-Contravention Case Management System. Unique identifiers are assigned to each electronic document - no matter how insignificant. The unique identifier is used for document retrieval by parties, cross-linking between documents and for inclusion in thematic files.
5. QR codes are incorporated in all representations/views of electronic documents generated by the e-Contravention Case Management System.

The electronic document stored in the e-Contravention Case Management System is structured using standards and a common format, such as XML (Extensible Markup Language), or JSON (JavaScript Object Notation) that allow users to store and transmit information in a structured, easy to interpret and use.

All documents stored in the e-Contravention Case Management System have header information that includes at a minimum:

1. the registration number of the document;
2. the date and time of concluding the document;
3. the date of document registration;
4. the place where the document was concluded;
5. the author of the document;
6. the type of document (from the register of documents);
7. the status of the document (original/copy/certified copy).

2. Electronic file

The electronic file is the mechanism for the thematic grouping of all electronic records and documents accumulated for the resolution of a case. In addition, the File is also used to ensure a common handling of all documents/messages contained in it. The File in its essence is also a document with records about its contents. This is indicated by the relationship of the File to the Document.

3. Tags

Tags are metadata that characterize the information object and can be freely associated with it. Some restricted access tags may signal automated processing by the information system of the tagged information object. Tagging practice provides a flexible and powerful mechanism for semantic classification of documents.

4. Systematized tags

Systematized tags represent a category of tags that the System can recognize and process automatically. For example, a systematized tag may be "@website" and when this tag is associated with a document, the system

automatically initiates the process of disseminating it on the MIA website. Another systematized tag could for example be "#solved" and the automated system hides these information objects from the user interface to avoid cluttering it.

5. Notification

Notifications alert participants about changes in the information objects intended for them and about impending certain events in the system. Notifications are usually sent to participants via external channels that the participant in question monitors e.g. email, SMS or computer alert.

The data model directly associated with the process of managing contravention cases and related activities is shown in Annex No. A4.

6.3.2. Data model associated with the keeping of departmental state registers

The central object of the data model associated with the registers is *a record*. A record refers to a document or information that is kept in a static and unchangeable format to serve as a form of evidence in case of dispute or uncertainty of rights and obligations. The record must be managed in a secure manner and be available only to persons authorized to access and manage it.

1. The data model associated with the records management component is characteristic of a records management application component. It is recommended to consider the European Commission's recommendations to the Electronic Records Management Systems - "MoReq2010" for the data model associated with the records management component.

   Similarly, the data model shall also comply with the requirements of SM SR ISO 15489:2016 "Information and documentation - Documentation management", ISO 16175: Information and documentation - Principles and functional requirements for records in electronic office environments and SM RM ISO 14641 Electronic records management - Design and operation of electronic records storage information system - Specifications.

   Alignment with international standards and European practices ensures the ability to be interoperable with other national and international IT systems, the possibility to easily implement best practices in the field, reduce costs by reusing ICT solutions, reduce the time and effort to develop ICT services, etc.
2. The registers do not contain the documents that are in the e-Contravention Case Management System. The unique number of the document in the e-Contravention Case shall be entered in the register.

List of registers

The following registers shall be digitized in the e-Contravention Case Management System according to these ToR:

1. State Register of Contraventions;
2. Register of Road Accidents;
3. Register of emergency restriction orders;
4. Register of restriction orders
5. Register of persons and means of transport announced as wanted;
6. Register of blank forms of strict record;
7. Register of issued Contravention Records;
8. Register of offence referrals (R1);
9. Register of other information on offences and incidents (R2);

The implementation of other registers in the e-Contravention Case Management System shall be subject of other procurement exercises.

6.3.3. Data model associated with interoperability flows

The data model associated with the interoperability component of the MIA - is a canonical data model designed to ensure communication between different data formats. To ensure interoperability with external information systems the use of the MConnect Semantic Catalogue is recommended[3].

L Similarly, all semantic assets created within the e-Contravention Case Management System are to be registered in the MConnect Semantic Catalogue.

The information objects describing the statistical model for recording road accidents shall be defined according to the DDI standard and shall include the statistical variables and their values according to the CADaS (Common Road Accident Data Set) model[4]. The CADaS model, approved by the European Commission, consists of a minimum set of standardized data elements, comparable across the European Union, on road accidents.

6.3.4. Data architecture security model

All data architecture artefacts must be identified and described. Each artefact shall be assigned a security category. MIA is to provide the nomenclature of security levels applied to the data, the list of user categories and the CRUD (Create, Read, Update, Delete) data access matrix.

The security model to be implemented in the IT solution must comply with the principle of restricting access to information according to the need-to-know and officially assigned competences. To this end, access to the information managed in the IT system must be controlled in two distinct scenarios:

- Access to information in a specific contravention case;
- Display of the result of a search on the whole dataset ("search" type searches).

For the first scenario, access to data in a specific contravention case, access will be restricted by the intersection of four rights logics:

- Whether the user belongs to a user group or profile that has access to the type of information or functionality that allows viewing/editing of that information (for example, two users with different profiles may have the right to access the same contravention case in the system, but one profile allows access to a limited set of data and metadata, while the other profile allows access to the entire set of data and metadata in the contravention case).
- Permissions (rights) on how to access information in the information system will be set for each defined role. These permissions are as follows: create, read, modify and delete information, at database object level and at object attribute level.
- The affiliation of the officer/agent holding the user account to a subdivision of the MIA that has the right of access to the respective contravention case. For example, a user who has the profile of an MIA sub-unit leader will only have access to cases handled by that sub-unit, not to all contravention cases;
- Current status of the contravention case. For example, access to certain data and functionality is only granted when the contravention case reaches a certain stage in the flow. Or, conversely, after the

[3] https://semantic.gov.md/ro/categories
[4] CADaS glossary is available at https://ec.europa.eu/transport/road_safety/specialist/statistics_en

contravention case passes a certain stage (e.g.: the decision is completed) the restrictions on accessing the information in the contravention case are removed;

- The role of the officer/agent in the contravention case;
- The required IT system must have the capability to model and configure all of these types of data access restriction logic and functionality;
- With respect to limiting access to information accessible in the system based on search queries, the system must have the capability to assess the following access limitations on each contravention case recorded in the system:
    - Maximum level of access restriction: as a result of a search in the dataset, regardless of the criteria used, the system does not return any record of a contravention case that has this property activated, even if it matches the search criteria, unless the search is carried out by the holder of the information itself;
    - Medium level of access restriction: as a result of a search in the dataset, the system will only return the contact person who has information about the entities searched according to the search criteria used by the user;
    - Low level of access restriction: as a result of a search in the dataset, the system will only return certain non-personal data (e.g. fact, location, period) in addition to displaying the information holder
    - Full access: all elements contained in the information package will be accessible for viewing.
    - The required IT system must have the capability to dynamically calculate the properties of the offence cases from a search display perspective, based on their metadata and attributes, and to return search results according to these properties.

6.4. . Application architecture

6.4.1. Reference model for MIA IT applications

The reference model for MIA IT applications is defined in MIA's Future ICT Architecture document in accordance with the conceptual model for MIS's IIS. The reference model indicating the place of the e-Contravention Case Management System in the MIA Future Application Architecture is shown in the image below.

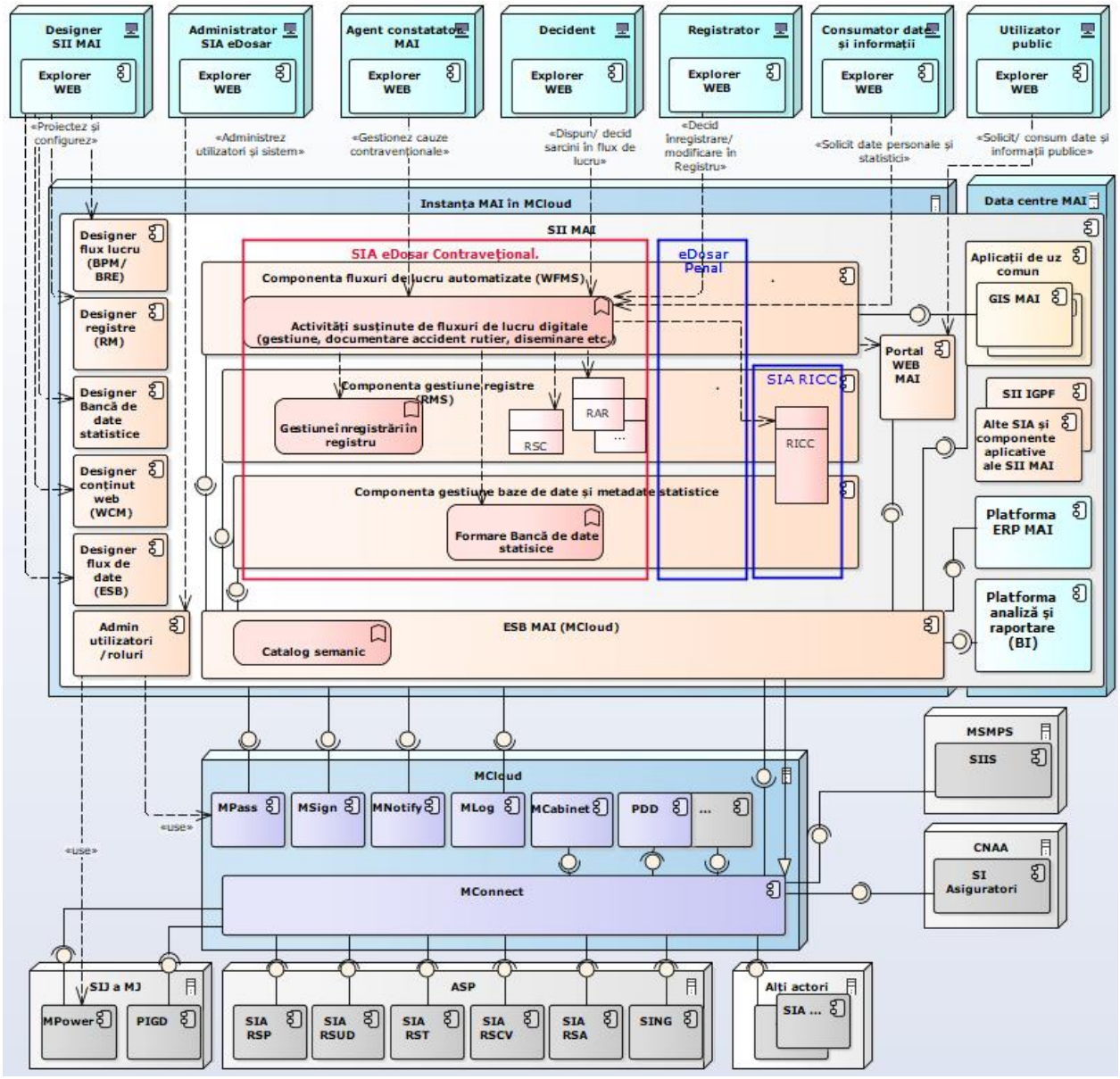


Fig. 5 the place of the e-Contravention Case Management System in the MIA and government ICT architecture

The e-Contravention Case Management System is part of the MIA IIS. The MIA IIS architecture, is SOA, and designed as a set of embedded services and microservices designed to explore diverse types of digital content, regardless of where and how it was created and stored, across numerous use cases, by different MIA and external user groups, realized through a set of integrated platform programs, separate applications sharing common APIs and data repositories, and co-opted and reused content service components.

6.4.2. Relevant application capabilities for the e-Contravention Case Management System

The capabilities provided by the MIA IIS components (applications, platforms and services) are used to create the services for human users and IT systems provided by the e-Contravention Case Management System. The

services of government platform SaaS, PaaS that provide capabilities for the creation of services of the e-Contravention Case Management System are also co-opted.

Depending on the purpose of use, the services provided by the e-Contravention Case Management System are of the following types:

1. “front end” - intended for non-face-to-face use/interaction with the user,
2. “back end” - intended for processes and content management (data and metadata).

Front end services are WEB services accessed by users through the WEB Explorer. The "front end" services of the e-Contravention Case Management System are created by using the following capabilities of the MIA IIS components:

1. Workflow Management Component (WfMS) – the application component provides the necessary capabilities to make it possible to configure workflows according to MIA's needs. Virtually any paper-based information flow can be transitioned to an equivalent electronic flow. These applications serve as "front end" applications providing user interfaces and interaction mechanisms with other AIS within the workflows. By using the capabilities of this component, the following business processes and functions are digitized within the e-Contravention Case Management System:
    - Digitization of the workflow related to the registration of the reports in the R1 and R2 registers
    - Digitization of the process for the management of contravention cases and related activities;
    - Digitization of the workflows related to the maintenance of departmental state registers (registration, updating, provision and deletion of records);
    - Digitization of the workflow related to the request for access to files and documents stored in the electronic archive
2. Mobile Application Components - is a set of application capabilities designed to support informational support of activities in the field. The application provides a unified interface for access to all functionalities offered by MIA applications and access to any information held in MIA and external AIS relevant to the field activity.
3. Online Referrals Service - set of capabilities intended for online registration of referrals by citizens.
4. E-Contravention Record Service - service realized by reusing the capabilities of the governmental platform solution services.go.md intended for consultation of the e-Contravention Record.

Back end services are provided through APIs. They are intended to be used by "front end" components or external systems with which the e-Contravention Case Management System exchanges data. The e-Contravention Case Management System's "back end" services are created using the following capabilities of the MIA IIS components:

1. The Records Management component of the MAI (Record Management): is designed to design and manage registers and the processes for working with them. It includes API interfaces for connecting MIA front end systems and external beneficiaries' systems. The solution is used for the design and maintenance of the Registers within the e-Contravention Case Management System.
2. Indexing and Data Search Component – Set of capabilities that provide content indexing to provide a subsequent indexed search solution of documents, records and other data and present query results to users based on relevance.

    The e-Contravention Case Management System will provide indexing of at least the following categories of data:
    a. The content of documents created within the workflow
    b. Workflow metadata
    c. Content of records in the Registers;
    d. Metadata of records in the electronic archive.

The e-Contravention Case Management System will provide a full text indexing solution for documents providing facilities to reduce synonyms, prefixes and suffixes as well as normalizing the relevance of document terms to the size of the document (the calculation of the weight of terms should not depend on the file size) in order to eliminate cases of priority of large documents over small documents.

3. MIA ESB – the ESB MAI interoperability platform provides a unique mechanism for interconnecting internal applications and communicating with the outside world. ESB MAI includes the Semantic Catalogue as a single, authentic source of semantic assets. Semantic assets are collections of metadata (XML schemas, generic data models, ontologies) and reference data (code lists, taxonomies, dictionaries, vocabularies, etc.) As the technology solution for the MIA ESB the PaaS MConnect service is used.
4. Reporting management platform service

   The e-Contravention Case Management System will have capabilities to generate reports based on predefined templates and ad hoc reports. It is desirable that the IT system integrates a solution dedicated to the configuration and generation of reports (report generator) that can also be reused for the configuration and extraction of specific business process templates of the e-Contravention Case Management System.

5. Government platform services (MCloud) are used to develop the services of the MIA IIS. At least the following capabilities will be used:
   - MPass - identification, authentication and role management capabilities for authorized users.
   - MPower - capabilities used to validate the powers of the reporting officer.
   - MSign - electronic signature capabilities used for signing and verifying documents and datasets.
   - services.gov.md - capabilities used for the creation of the IT Service e-Contravention Record
   - MLog - event logging capabilities used for storing events occurring in the system;
   - MNotify - capabilities used to notify system users and others of events generated by the system or at the direction of system users
   - MCabinet - capabilities designed to digitize communication flows with individuals involved in the process
   - MDoc - capabilities for storing and sharing documents for parties involved in the contravention process and related activities other than users of the system
   - MConnect - capabilities used to exchange data with the IT systems of the MIA and other public and private authorities.
   - MPay - capabilities used for the payment of fine-related payment bills
6. Specialized IT services, such as:
   - IT service for generating payment bills for fines / Billing – Set of capabilities designed to issue payment bills for fines issued by the MIA and for public services provided by the MIA to citizens. Allows the definition of payment invoice templates for different usage scenarios. Ensures the transmission of payment bills to MPay. Ensures the tracking of a payment invoice throughout its life cycle. Provides information for reconciliation of paid invoices.

In addition to the platform components that are used for the direct formation of the services constituting the e-Contravention Case Management System, the following IT systems interact with it:

1. Web portal web– includes public web applications, through which the MIA designates information of public interest, including electronic public services. This block includes the web pages of the MFA and MFA subdivisions, other websites through which electronic services are provided (whether in the MIA environment or on the MCloud platform), such as data.gov.md and services.gov.md;

2. MIA GIS platform service The service is intended for the management of GIS maps required in MIA activity, generation of specialized map layers based on data provided by other MIA applications, according to the specific needs of MIA subdivisions. In the context of the e-Contravention Case Management System, the capabilities of the GIS platform service are used for geolocation of mobile devices, crime scene and evidence collection location.
3. Other AIS and applicative components of the MIA IIS may interact for the purpose of data exchange with the e-Contravention Case Management System, such as:
   - AIS Traffic Control - interacts for the purpose of providing data on contravention facts recorded by technical means (photo-video monitoring system and "trap car" system);
   - AIS e-Criminal Case - interacts with the e-Contravention Case Management System for the purpose of exchanging data and documents for cases of reclassification of the contravention into/from a criminal case;
   - AIS RICC – interacts with the e-Contravention Case Management System for the purpose of exchanging data and documents for the maintenance of the Register of Forensic and Criminological Information.
   - AIS AFIS - interacts with e-Contravention Case Management System for the exchange of fingerprint identification of the person
   - Etc.
4. Third-party information systems – the e-Contravention Case Management System interacts with other external systems for the purpose of exchanging data related to supported business processes, maintaining semantic assets (e.g. classifiers, geospatial data, etc.) and automatic dissemination of data and information or upon request. These may include:
   1. The Public Services Agency as the holder of the state registers provides data from:
      - AIS State Register of Population - data on individuals, home address and documents, which have been issued to them;
      - AIS State Register of Legal Entities - data on all categories of legal entities, constituted on legal basis, legal address, rights to exercise various licensed activities;
      - AIS "State Register of Transport" - data on means of transport (including units with identification numbers), their owners and other authorized persons, documents and registration numbers;
      - AIS "State Register of Vehicle Drivers" - data on the right of the natural person to drive the corresponding means of transport;
   2. Ministry of Justice as possessor of:
      - AIS "Management of judicial expertise files" (SIGDEJ) - expert reports drawn up by or with the participation of judicial experts;
      - Integrated Case Management System - court decisions and judgments on contravention cases;
   3. MIA IT Service as holder of the MIA AIS provides data from:
      - AFIS (Fingerprinting Register);
      - AIS RICC (Register of Forensic and Criminological Information);
      - AIS e-Criminal Case (once implemented);
   4. Land Relations and Cadaster Agency
      - AIS State Register of administrative-territorial units and addresses - data on administrative-territorial units, streets, buildings and apartments when registering residence
   5. State Tax Inspectorate

- AIS „Register of contravention fines", part of the Information System of the State Tax Service - in order to provide information on administrative fines to the State Tax Service, according to the set provisions

6. Interpol/Europol
   - As an IT service provider for the automated exchange of DNA data, fingerprinting data and vehicle registration data;

The full list of relevant reusable application capabilities of the e-Contravention Case Management System is provided in Annex A5.

6.4.3. User interface of the e-Contravention Case Management System

The e-Contravention Case Management System must provide an ergonomic, intuitive user interface that is accessible to all types of users. The user interface of the IT system will be accessed via an Internet browser. The e-Contravention Case Management System must have an intuitive, user-friendly, balanced and distinct graphical design optimized for the minimum resolution of 1360x468 working on PCs. The user interface must also be adaptable for smartphone and tablet device resolutions and optimized for touch screens.

For user-friendliness, the IT solution shall have an online context-sensitive help system at the level of each user interface.

Depending on the categories of users (their rights and roles) the IT system will provide a customized interface for each user category.

Users of the IT system will have a minimum of 8 basic levels of access to the user interface and data (in perspective the sets of rights and roles assigned to them, as well as the optimal number groups of users.

The e-Contravention Case Management System will provide an interface in Romanian and Russian. The system will allow for additional language versions to be added if needed. Information and records retrieval procedures will be carried out by means of simple searches (specification of search strings) or more complex searches, through which more accurate filtering of information can be achieved (QBE forms). Regardless of the nature of the information sought, the user will use the same method of querying and retrieving information for any compartment of the IT product.

In addition to the search module based on the QBE principle, which will make it possible to define sophisticated queries visually, the interface must offer the possibility of refining the search results by providing the possibility of filtering the data in the list of search results.

The user interface of the information system must ensure that records matching the search criteria presented to users are filtered according to their access rights.

Indexed measures (values from classifiers, nomenclatures) must be filterable by choosing the value from predefined lists. For numeric or calendar date fields, it must be possible to filter by the exact value of the searched characteristic or by the search mask.

The content of any results table or electronic form, depending on the nature of the information contained, must be exportable in either CSV, RTF or PDF format.

All user interfaces shall contain background text (water marks) with the user's Name, Surname and Individual Code. This measure is intended to make users accountable and limit information leakage.

7. Use cases of the e-Contravention Case Management System

Taking into account the architecture of the e-Contravention Case Management System, the functionalities offered to users are divided into 3 groups:

1. Basic Authorized User functionalities providing all available cases common to all categories of authorized users.
2. Administration functionalities which implement all the use cases necessary for the administration and configuration of the e-Contravention Case Management System;
3. System functionalities that implement all use cases provide the system functionalities of the e-Contravention Case Management System.

The totality of functionalities delivered by the e-Contravention Case Management System and the actors benefiting from them are described in the following chapters:

7.1. Basic functionalities of the e-Contravention Case Management System

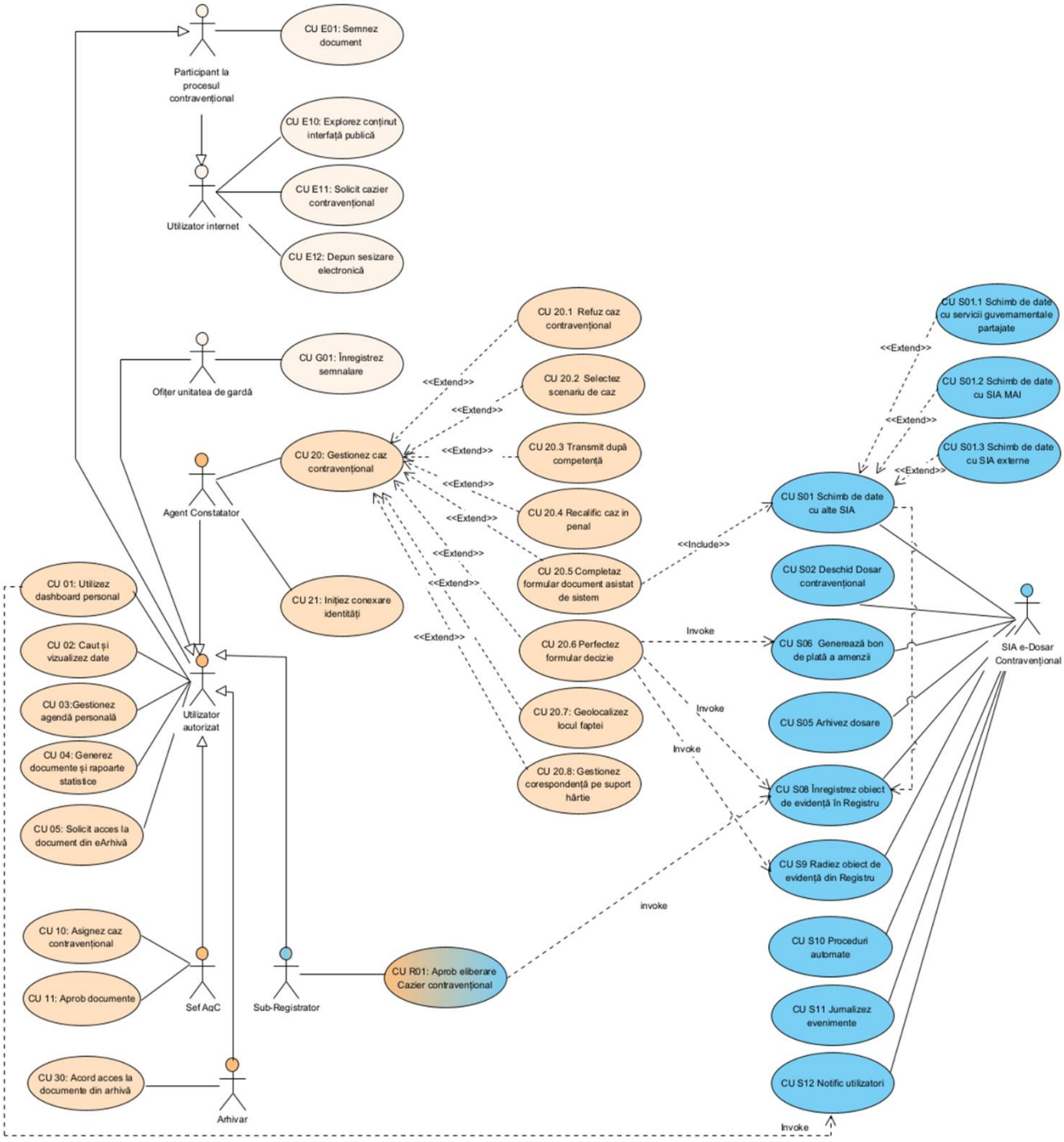


Figure 6. Use cases of the e-Contravention Case Management System

7.1.1.1. Common use cases

CU 01: Personal dashboard use. Represents a functionality through which the authorized user of the e-Contravention Case Management System accesses the personalized working environment. The dashboard will serve as the main page of the authorized user interface of the e-Contravention Case Management System.

The e-Contravention Case Management System user dashboard will display business events relevant to the functionalities and data available according to the rights and roles of each individual authorized user. At least the following categories of business events will be available according to the roles and rights of the authorized user of the e-Contravention Case Management System:

1. Top 5 pre-established scenarios for documenting the contravention case relevant to the role of the Reporting Officer
2. Top 5 contravention cases associated with the Reporting Officer, pending, in order of expiry of the statute of limitations of the cases
3. notifications of deadlines for the completion of tasks assigned to the user that are at risk of being exceeded;
4. notifications of acts or processes awaiting approval from the deciding roles.
5. notifications on approval of dates of proposed agenda events;
6. notifications of approaching events planned in the user's agenda.

The areas/windows with data displayed in the dashboard will have a reference to windows with details of the subjects displayed in the dashboard (e.g. list of e-Contravention Cases, e-Contravention Case, agenda, electronic form, etc.).

The e-Contravention Case Management System will provide each user with individual content configuration functionality (configuration of notification preferences, configuration of areas with important content currently worked on by the authorized user, location of content categories) and display mode (visual filters, location of elements, colors, language, style, etc.).

The system will provide pre-configured versions of the dashboard for groups of users. The user group defines the key elements to be displayed in the dashboard.

When displaying data in the dashboard, the e-Contravention Case Management System will take into account the user's right of access to qualified documents according to the MIA information security management system.

The dashboard will allow access to any functionality of the e-Contravention Case Management System whether it is basic functionality or functionality provided by separate functional modules in no more than 2 clicks.

CU 02: Search and view data and documents This use case contains all the functionalities to explore the data and documents stock created or managed through the *e-Contravention Case Management System*.

The e-Contravention Case Management System will provide mechanisms to explore the available data and document repository taking into account the rights of authorized users based on data and document classification mechanisms and document indexing technologies.

The e-Contravention Case Management System will provide a search component for data and documents taking into account information sources:

1. documents and metadata associated with the documents contained in the e-Contravention Case;
2. data associated with workflows;
3. data contained in the records of the Registers kept in the e-Contravention Case Management System;
4. data from the State Registers interoperable with the e-Contravention Case Management System kept by the MIA and other authorities.
5. Documents shared in MDoc
    - Access to the data and documents stored in the e-Contravention Case Management System is differentiated according to the role of the user:

Access to the data and documents associated with the *e-Contravention Case:*

- the owner of the file who has full rights to all documents associated with the file
- other users who have been granted access rights by the owner or by virtue of their role.

Access to data in the Registers kept in the e-Contravention Case Management System:

- The Registrar/Sub-Registrar has access to all records of the register they manage;
- The data provider has access to the data provided;

Access to archived documents is limited.

- Access to the data in the archived files is restricted to the user with the role of Archivist.
- Other authorized users may access meta-data associated with the archived file(s)/documents.
- Access to archived file data may be granted on request to other users for a specified period of time.

Access to other data and documents stored in the e-Contravention Case Management System (workflow data, reports, etc.) shall be granted according to the user's rights and roles.

Access to data stored in the MDoc is explicitly set by the document owner. Implicitly the document has access rights of the document stored in the e-Contravention Case Management System

Access to public data and documents is granted to all authorized users.

- The e-Contravention Case Management System will allow the content of the dataset to be explored both using the document and file classification system and based on the search result.

The e-Contravention Case Management System will provide at least the following functionalities related to the search of documents and data:

1. Search documents by keywords. Searching by keywords will be performed both in the metadata describing the document and in its content. In order to facilitate the search all documents shall be indexed according to the requirements of CU S10 Automated procedures
2. The search for archived documents shall allow queries to be formulated on the basis of the metadata values attached to the documents.
3. Document and file search shall provide morphological and indexed search solutions for documents and files (search based on document search images).
4. The e-Contravention Case Management System will be able to search the document based on the associated barcode/QR containing the unique document identification number.
5. The e-Contravention Case Management System will present the search results according to the relevance of the document content to the query made by the user (in order of decreasing relevance of the documents found).
6. The e-Contravention Case Management System will provide functionalities for refining the search (searching within the results found) filtering and sorting the results found.
7. The e-Contravention Case Management System will provide direct access reference to the found document/file. The ways of further manipulation of the document/file will depend on the rights and roles of the user and the status of the document/file.

A specific aspect to be provided by the e-Contravention Case Management System is the search of information about the person for identification purposes. The need to identify the person is conditioned by several factors such as: lack of information about the IDNP, the existence of several identities associated with the same person in the SRP, persons holding foreign nationality can be authenticated with different identity documents, the registration of foreigners is done on the basis of the presented document which can be different over time, etc.

The system will provide at least the following mechanisms for identifying the person:

1. Identification of the person based on IDNP;
2. Identification of the person on the basis of the identity card;
3. Identification of the person based on other data (e.g. Name, Surname, Patronymic, etc.);
4. Morphological search in Name, Surname, Patronymic;
5. Identification of the person based on fingerprint;
6. Person identification based on facial image.

The system must search all available resources: internal and external registers, documents produced in workflows, workflow metadata, etc.

CU 03: Manage personal agenda Use case that provides the functionality to manage the individual agenda of the authorized user.

Users should be able to view and manage their personal agenda via an interactive calendar. This includes scheduling appointments, assigning tasks and setting deadlines.

The personal agenda should be able to be synchronized and integrated with other calendars or applications used by the user installed on the computer, tablet or mobile phone. This allows events to be imported or exported, synchronizes events with other users and ensures that all activities are up-to-date and visible in one place.

Users should be able to prioritize activities, filter them by different criteria (such as date, time, categories, etc.) and organize them according to their needs. This makes it easier to manage tasks and identify the most urgent or important ones.

CU 04: Generate documents and statistical reports. It is a use case accessible to users of the e-Contravention Case Management System that contains all the functionalities required to generate structured documents in a printable format and predefined and ad-hoc reports on the information content of the information system and the activity of authorized users.

The reporting system of the e-Contravention Case Management System shall delimit at least the following categories of documents and reports:

1. Documents generated based on the predefined template - for each type a template will be created which will be populated with information relevant to the document (*e.g. report on a contravention, summons, decision, etc.*);
2. Enforcement discipline reports - for each type a template will be created and populated with information relevant to the report;
3. Public statistical reports - this type of report includes reports intended for the general public that contain public data and do not contain personalized data. This category of outputs will provide, in particular, public statistics and KPI values to be published via the official MIA website or the Open Data Portal.
4. Individual performance and workload level reports (KPI) - represents a set of KPI indicators on the basis of which the activity performance of the users of the e-Contravention Case Management System can be assessed regardless of their role;
5. Register extract - intended to provide information about the records contained in the departmental state registers kept in the e-Contravention Case Management System.
6. System Monitoring Reports - is a category of reports for system administrators used to assess how authorized users interact with the e-Contravention Case Management System. This category of reports will allow to anticipate performance problems in the activity of subdivisions and employees or security and vulnerability problems of the system.

The e-Contravention Case Management System will use, at least, the following as data sources for generating documents and reports:

- the content of the structured documents in the e-Contravention Case;
- the metadata associated with the e-Contravention Case and its documents.
- data associated with workflows;
- data contained in the records in the Registers kept in the e-Contravention Case Management System;

- data from external State Registers.
- nomenclatures and classifiers
- authorized user activity;
- access and security permissions

It is desirable that the IT system integrates a solution dedicated to the configuration and generation of reports (report generator) that can also be reused for the configuration and extraction of the template documents specific to the business processes of the e-Contravention Case Management System.

The e-Contravention Case Management System must provide users with a standard number of pre-configured reports (at least 20 reports) and allow ad-hoc reports to be produced on demand.

The e-Contravention Case Management System shall log any document and report generation event.

The e-Contravention Case Management System will take into account the intended use of the generated document/report (printing or storage as a file) and will provide different functionalities depending on it, such as:

> E.g.1: documents that are generated for printing cannot be regenerated or stored as a file. Similarly, the system will ensure that no virtual printer is used.
>
> E.g.2: when generating documents to be printed on strictly recordable blankets, it will be required to indicate the series and number of the blank. Information on the series and numbers of the blankets used will be saved in the Register of Blanks of Strict Record. Similarly, the system will ensure that the series and number of the blank belongs to the user initiating the generation of the document.

A user viewing a report or document within the system should be able to export it to an external file that can be edited, unless there are restrictions on this.

When generating the printable version of a structured document processed within the e-Contravention Case Management System workflows, a barcode containing the unique identifier of the document and a QR code containing the basic metadata of the document will be generated and placed on its title page.

Complex documents consisting of several compartments (e.g. minutes of contravention) will be printed and displayed/viewed as a single document. Including blank parts will be printed according to the print template, containing blank areas.

The e-Contravention Case Management System must have statistical data dissemination capabilities on public resources (e.g. MIA website, data.gov.md, etc.).

CU 05: Request access to documents from eArchive. This use case refers to a workflow in which the system user requests access to a e-Contravention Case or document in the digital archive.

- Access to data in the archived file must be motivated and can be granted for a specific period of time.
- Access to archived documents is granted in accordance with the MIA's archival data management regulations.

7.1.1.2. Use cases specific to the role of Chief of the Reporting Officer

CU 10: Assign the contravention case. This use case contains all of the functionality required by the Chief of the Reporting Officer to distribute an unassigned referral, reassign a case, and monitor the reporting officer's case assignment.

CU 11: Approve documents. This use case provides the functionality required to coordinate incoming documents on the workflow.

The coordination process must provide at least the following activities:

- Returning the document to the author for completion;
- Approving the document by applying the digital signature;
- Entering comments/notes in the document;
- Track Changes editing of the document;
- Setting tasks and deadlines;

In the case of documents referring to other documents (e.g. list of documents in the file) the system will allow consultation of their metadata according to the viewing rights of the latter.

An example of a process supported digitally by this use case is the coordination and signing of accompanying letters by the Chief of the Reporting Officer.

7.1.1.3. Use cases associated with the role of the Reporting Officer

CU 20: Manage contravention case Represents a generic use case through which the full functionality required to digitize the contravention process and related activities will be provided.

According to art. 374, point (2^1) the contravention process starts automatically from the moment of the referral or self-reporting of the contravention by the reporting officer.

In practice, in the e-Contravention Case Management System, the workflow for the management of the contravention case is initiated by the process of " Alert registration process" which delivers the "referral" or "self-report" to the address of the reporting officer.

A total of 4 sub-processes were identified for the contravention procedure:

1. Sub-process "Case allocation";
2. Sub-process "Case acceptance";
3. Sub-process "Establishment";
4. Sub-process "Examination";
5. Sub-process "Decision making";

In addition to the basic process " Contravention procedure ", the management of the contravention case is assisted by 3 auxiliary processes:

1. The process of monitoring the case, carried out by the chief of the reporting officer;
2. The process of signing the accompanying letters;
3. The process of managing payment bills and monitoring payments carried out by the billing system of the MIA e-Services system.

The detailed description of the contravention case management workflow is presented in Chapter 6.2.1.3 and Annex No. 2.

CU 20.1: Refuse as contravention. This use case supports the sub-process of accepting or refraining the reporting officer from considering the contravention case.

After receiving the referral, the ROC reviews the case and, if there are no compelling reasons to decline that case, the RO accepts it, with the status of the referral recorded in the system. If there are reasonable grounds for refusal, the RO refuses the referral and draws up a report.

In addition to the digital support of the workflow of refraining from handling the case initiated by the RO according to art. 385 CC, the system will digitally support the activities of recusing the RO by the participants in the contravention process in question, vested with such right.

CU 20.2: Select case scenario. This use case contains all the functionalities used by the reporting officer to select a scenario for the management of the contravention case. A scenario includes the totality of the actions to be taken by the RO to manage a contravention case of a certain type. The user can select more than one scenario. In this case the system will merge the necessary activities to be performed.

The easiest working scenario is to select a separate procedural document for completion.

There will be a scenario in the System that includes all articles of the normative acts. When selecting this scenario, the RO will be warned that the System will not check the correctness of the completion of the document.

The selection of scenarios by the RO is logged.

CU 20.3 Send according to competence. Use case that provides the full functionality required to forward the file to another authority / reporting officer according to competence. In the case of sending the file on paper, the system shall provide correspondence management capabilities for the purpose of completing accompanying letters and printing electronic documents in accordance with the requirements of CU 20.8: Manage correspondence on hard copy.

CU 20.4 Requalify in criminal case. Use case that provides the full functionality required to forward the file to the prosecuting authority/prosecutor in the case of reclassifying the contravention case to criminal. In the case of sending the case file on paper, support is provided for the completion of accompanying letters and the printing of electronic documents in accordance with the requirements of CU 20.8: Manage correspondence on hard copy.

CU 20.5 Fill in the assisted document form in the system. This is the second most important use case. This use case contains all the functionalities required to assist the reporting officer to produce the necessary process and procedural documents. The use case uses the logic configured in the system (CU D01: Configure the e-Contravention Case Management System) for suggestions for auto-completion and validation of the data entered.

The documents in the e-Contravention Case will be stored in structured XML format. The provider of the e-Contravention Case Management System will propose the taxonomy for structured documents.

The system will ensure that versions of the documents are kept. A new version can be initiated both by the user and by the system as a result of an event occurring in relation to the document (e.g. use of the document to make an entry in the register). When the document is used as the basis for the entry in the register, if it is not signed, the current version will be stored and kept by the system. The system shall ensure that the version of the document used to enter data in the registry remains unchanged.

In the event of a signed document being overwritten (e.g. if errors have been identified) both versions will be retained. For some documents the correction procedure is foreseen, which consists of producing a new document in which the relevant entry is made (e.g. Minutes of the contravention - Art. 443 para. (7) of the CC) or an additional document "report" is made specifying the error/reason for correction.

Procedural documents can be challenged in court and annulled. In this case, the original document will be kept in the system and will have a reference to the document that cancelled it and will be perceived as part of the contravention file.

For the fields referring to articles, points or text in the normative acts, the system will restrict the filling in only to the values in the nomenclature. Predefined scenarios will be used to determine the set.

In the case of fields requiring the entry of free-form text, the System will check whether the articles, points indicated are from the set defined by the scenario and will warn the RO about discrepancies.

There will be a scenario in the System that includes all articles of the normative acts. When selecting this scenario, the RO will be warned that the System will not check the correctness of the completion of the document.

The nomenclature of articles/items of the normative acts, which are taken over in procedural documents, must support versions. For each version the period of validity can be established. The time of entry into force shall be deemed to be 00.00 on the day indicated.

The documentation of the contravention on paper will remain optional, the reporting officer having the possibility to decide the course of documentation. A final decision on the exclusion of paper blanks will be taken at the end of the successful implementation of the e-Contravention Case by all public authorities where reporting officers work. The e-Contravention Case Management System will support both the production of electronic documents in the workflow and the input of data from completed paper documents.

CU 20.6 Conclude the decision form. This is the 3rd most important use case. This use case contains all the functionality needed to assist the reporting officer to make an informed and legally valid decision. The use case uses the logic configured in the system (CU D01: Configure the e-Contravention Case Management System) for auto-completion suggestions and validation of the data entered.

CU 20.7: Geolocate contravention scene. This use case contains all the functionality required to geolocate an object/place on the map. Geolocation is used by the RO to indicate the location of the event, evidence or other object on the map.

The system will propose at least the following ways of georeferencing objects:

a. By indicating the object/location on the map
b. By indicating the GIS coordinates of the location on the map.
c. By taking coordinates from the tablet (if used to fill in the document).
d. By taking the geo-location from the data provided by the approved mobile equipment listed in the documents attached to the "self-report form".

CU 20.8 Manage the correspondence. This use case contains all the functionalities required to manage correspondence on paper and/or other formats through official data exchange channels. In this respect the e-Contravention Case Management System must provide:

1. Concluding and sending the outgoing correspondence
2. Registering the incoming correspondence in the system.

For concluding and sending the outgoing correspondence the e-Contravention Case Management System will ensure:

1. Generate the document/report in a printable format as required by CU 04: Generate statistical documents and reports.
2. Where appropriate, concluding the accompanying letter using predefined templates. Accompanying letter will include the list of documents to be sent. The outgoing letter shall indicate the system identity code of each attached document.
3. Coordinate the outgoing letter with the Chief of Reporting Officer (as per CU 11: Approve documents

4. Record the document registration number in the organization/subdivision's outgoing document register.

Recording of incoming correspondence in the e-Contravention Case Management System provides for:

1. Uploading the incoming external document into the system. In the case of paper documents, a scanned copy is uploaded into the system.
2. Filling in information about the document in the document's electronic file. The document's electronic file must contain at least:
   a. The document registration number
   b. The document registration date
   c. Author of the document (In the case of RO, also indicate the RO code)
   d. Type of document (from document register)
   e. Status of the document (original/copy/corroborated copy)
   f. Brief description of contents (to be completed optionally)
3. Granting access to the document. The uploaded document inherits the rights of the e-Case in which it was included. Only the owner of the e-Contravention Case can withdraw the rights of access to the uploaded document.

The e-Contravention Case Management System shall have capabilities to integrate with Document Management Systems (DMS) through which it can send and receive documents, or at least record in the outgoing register / receive data from the incoming register.

Documents received by email are considered external documents.

CU 21: Initiate identity linking. Use case containing the functionalities needed to link different identities belonging to a person. Multiple identities may occur when one and the same person has been assigned more than one IDNP. This can be historical errors, resulting from the assignment of IDNP codes to foreigners or citizens of Moldova with multiple citizenships based on identification with different identity documents.

The e-Contravention Case Management System will ensure the possibility of linking information objects referring to individuals from the e-Contravention Case and registers in case of identification of multiple identities held by one person.

The e-Contravention Case Management System will ensure the initiation of the error reporting procedure to the holder of the SRP in case of identification of more than one IDNP attributed to the same person.

7.1.1.4. Use cases associated with the Archivist role

CU 30: Grant access to documents from archive. Use case that performs workflow with respect to granting access to the contravention record and/or other archived electronic documents and data (e.g. records from state registers entered into the archive).

The user in the role of Archivist is responsible for granting access to archived documents and data.

Access to data in the archive may be granted on request to other users for a specified period of time.

7.1.1.5. Use cases associated with the Sub-Registrar role

CU R01 Approve Contravention Record issuance. Use case where the authorized user approves the issuance of the Contravention Record.

The approval of the issuance of the "contravention record" is done by the user in the role of Sub-Registrar and serves as a trigger for registration in the Register of issued e-Records.

The Sub-Registrar signs with an electronic signature (CU E01 Sign document) each approved "contravention record" form.

In case of rejection of the request, the system will provide the Sub-Registrar with the necessary functionalities to complete the Reasoned Refusal Report. The report is available in electronic format only. The report is signed by the Sub-Registrar with an electronic signature (CU E01 Sign document) and serves as a trigger for the registration in the Register of issued e-Records.

Where appropriate, if the printout of the Contravention Record is requested, the use case CU 04: Generate documents and statistical reports will be invoked.

7.1.1.6. Use cases associated with the role of Participant in the contravention process

CU E01 Sign the document. This is a generalizing use case containing all the functionalities required to electronically sign a document. For the purpose of e-signing documents by default the MSign service is used, but alternative solutions such as MoldSign Desktop Suite and electronic holographic signature are to be supported.

7.1.1.7. Use cases associated with the Internet user role

CU E10: Explore public interface content. The use case refers to the possibility of accessing public information disseminated to an Internet portal (e.g. MIA website, date.gov.md, etc.).

CU E11: Request contravention record. The use case reflects the functionalities offered by the Contravention Record Service

The e-Contravention Record service is implemented by reusing the reusable services.gov.md platform capabilities and the capabilities of e-Contravention Case Management System. In this case the services.gov.md solution provides front-end capabilities and the e-Contravention Case Management System provides back-end capabilities.

The use case offers the following functionalities from the e-Contravention Case Management System:

- Receipt of the Contravention Record request and identification of the applicant
- Generation of the electronic contravention record form
- Initiation of the validation flow of the contravention record according to CU R01 Approve the issuance of contravention record
- Issue the " contravention record " in electronic format to the applicant.

CU E12: Submit electronic referral. Represents the use case where the "e-referral" submission service is offered.

The IT service "electronic referral" is offered to Internet users via the official website of the MIA. The e-referral can only be submitted by an authenticated person. The person authenticates him/herself with an electronic signature. The system will provide integration with the MPass service for the purpose of authenticating the person.

CU G01: Register alert. Use case whereby the user in the role of Duty Unit Officer ensures the reception, recording and qualification of alerts.

The user in the role of Duty Unit Officer also has the role of Registrar for the Register of offence referrals (R1) and the Register of other information on offences and incidents (R2).

The officer in the duty unit at the time of registration of the referral makes the preventive qualification of the act: it refers to criminal or contravention. Referrals qualified as contravention and self-referrals on

contravention facts are sent to the contravention case management workflow. In the case of alerts on other offences (R2) that are not qualified, they remain in the alerts module until they are qualified.

7.2. System functionalities of the Contravention Case Management System.

CU S01: Open contravention case. Automated process that provides for the creation of the information object e-Contravention Case in the System as a result of the registration of the Referral or Self-report. At the moment of the initiation, the e-Contravention Case object receives the identifier assigned to the Referral or Self-Report.

E-Contravention Case includes all documents and other data related to the contravention case (e.g. the logbook of the activities carried out by the RO related to the case). The "de facto" e-Case represents the contravention case.

The e-Case is the mechanism for the thematic grouping of all electronic records and documents accumulated for the resolution of a case. In addition, the e-Case is also used to ensure a common handling of all documents/messages contained therein. The case file in its essence is also a document with records about its contents. This is indicated by the relationship of the Case to the Document.

The opening of the e-Contravention Case is done automatically according to the trigger described in the "Workflow associated with the contravention case management process and related activities" described in chapter 6.2.1.3. The process of managing contravention cases and related activities.

CU S03: Data exchange with other AIS. This is a complex use case that ensures interoperability with internal MIA and external IT systems. This use case provides the following capabilities:

1. Search and consultation of information from State Registers and Departmental Registers held by public authorities, including the MIA, including those held in the e-Contravention Case Management System and from commercial registers held by third parties.
2. Exchange of data with the AIS of the process partners regarding the management of the contravention case
3. Receiving information from the AIS of the Providers of the data of the registers kept in the e-Contravention Case Management System.
4. Interoperability with external partners' information systems (e.g. Europol, Interpol, etc.)
5. Reporting of referrals regarding offences recorded in the Register of offence referrals (R1) to the e-Contravention Case Management System
6. Recording of self-reporting from the AIS Traffic Control, e-Data v2 and other AIS of the MIA capable of recording violations.
7. Integration with shared government services (MSign, MPay, MNotify, MCabinet, MDoc, MPower, etc.).
8. Dissemination of data to public interfaces (e.g. MIA website, data.gv.md portal, etc.)

In practice, the interoperability of the e-Contravention Case Management System will be ensured with at least the following AIS:

1. AIS held by MIA used for data exchange purposes:

- AIS Traffic Control - interacts for the purpose of providing data on contravention facts recorded by technical means (photo-video monitoring system and "trap car" system);
- AIS e-Criminal case - interacts with the e-Contravention Case Management System for the purpose of exchanging data and documents for the cases of re-qualification of the contravention into/from a criminal case;
- AIS RICC - interacts with the e-Contravention Case Management System for the purpose of exchanging data and documents for the maintenance of the Register of Forensic and Criminological Information.

- AIS AFIS - interacts with the e-Contravention Case Management System for the purpose of exchanging the identification of the person on the basis of the fingerprint
- AIS State Register of Weapons - interacts with the e-Contravention Case Management System for the purpose of identifying natural and legal persons in possession of weapons and ammunition for civilian use
- Etc.

2. Third-party information systems - the e-Contravention Case Management System interacts with other external systems for the purpose of exchanging data related to supported business processes, maintaining semantic assets (e.g. classifiers, geospatial data, etc.) and automatic dissemination of data and information or upon request. These may include:
    1. The Public Services Agency as the holder of the state registers provides data from:
    - AIS State Register of Population - data on individuals, home address and documents, which have been issued to them;
    - AIS State Register of Legal Entities - data on all categories of legal entities, constituted on a legal basis, legal address, rights to exercise various licensed activities;
    - AIS "State Register of Transport" - data on means of transport (including units with identification numbers), their owners and other authorized persons, documents and registration numbers;
    - AIS "State Register of Vehicle Drivers" - data on the right of the natural person to drive the corresponding means of transport;
    2. Ministry of Justice as the possessor of:
        - AIS "Management of judicial expertise files" (SIGDEJ) - expert reports drawn up by or with the participation of judicial experts;
        - Integrated Case Management System - court decisions and judgments on contravention cases
        - IT solution e-Judiciary Case (e-JC IS) – for information within the limits of the request and the powers of the administrators
    3. Land Relations and Cadaster Agency
        - AIS State Register of administrative-territorial units and addresses - data on administrative-territorial units, streets, buildings and apartments when registering residence
    4. State Tax Inspectorate
        - AIS "Register of Contravention Fines", part of the Information System of the State Tax Service - to provide information on contravention fines to the State Tax Service.
    5. National Commission of Financial Markets
        - The information system RCA Data – provides information on compulsory third party liability insurance for damage caused by motor vehicles
    6. National Agency of Road Transport
        - Register of Road Transport Operators - provides information on natural persons and legal entities providing road transport against payment;
    7. National Union of Bailiffs of the Republic of Moldova (UNEJ)
        - Enforcement Records and Management Information System (SIEGDE) - for the purpose of exchanging data on persons owing fines.
    8. Interpol/Europol

- As an IT service provider for the automated exchange of DNA data, fingerprinting data and vehicle registration data;

3. Government platform services (MCloud) are used for the development of MIA IIS services. At least the following capabilities will be used:
    - MPass - identification, authentication and role management capabilities for authorized users.
    - MPower - capabilities used to validate the powers of the reporting officer.
    - MSign - electronic signature capabilities used for signing and verifying documents and datasets.
    - services.gov.md - capabilities used for the creation of the IT Service e-Contravention Record
    - MLog - event logging capabilities used for storing events occurring in the system;
    - MNotify - capabilities used to notify system users and others of events generated by the system or at the direction of system users
    - MCabinet - capabilities designed to digitize communication flows with individuals involved in the process
    - MDoc - capabilities for storing and sharing documents for parties involved in the contravention process and related activities other than users of the system;
    - MConnect - capabilities used to exchange data with the IT systems of the MIA and other public and private authorities.
    - MPay - capabilities used for the payment of fine-related payment bills

CU S04: Record self-report. This use case performs the necessary functionalities for recording self-reporting of contravention cases from:

1. AIS Traffic Control,
2. Mobile component e-Data v2
3. Other AIS of the MIA capable to record violations

The reporting officer does not have to fill in additional documents other than the ones establishing the contravention (the Minutes on the contravention, Decision of the reporting officer). The e-Contravention Case Management System can use a system document "self-reporting form" to record data on the self-reporting event. The self-report is recorded in the Register of offence referrals (R1). The self-report serves as a trigger to initiate the contravention case management workflow. The "self-report form" is accompanied by documents including evidence, all of which are entered in the e-Contravention Case.

CU S05 Transfer documents and files to the archives. This is a use case that represents an automated functionality of the information system to pass electronic files and/or records from departmental state registers into the MIA digital archive.

The transfer of the contravention case file (e-Contravention Case) to the archive is performed as a result of the following actions performed by the RO:

1. Receipt of the decision of the court on the cases dispatched according to Art. 400 (5), (6), for the decision on the sanction.
2. Closure of the case file without the completion of the minutes on the contravention;
3. Annulment of the sanction.

Closure of the file signals the fact to the activity of "Monitoring the progress of the contravention process" carried out by the Chief of the RO.

CU S06: Generate a receipt for the fine. Use case that provides the necessary information to generate the fine payment bill (e.g. identification data of the authority, treasury accounts, payment destination text, etc.).

CU S07: Index documents and records. Complex use case providing the full functionality required to analyze and index content in order to provide a subsequent indexed search solution for documents, records and other data and present query results to users based on relevance.

The e-Contravention Case Management System will ensure the indexation of at least the following categories of data:

1. The content of documents created within the workflow
2. Workflow metadata
3. Content of records in the Registers;
4. Metadata of documents in the electronic archive.

The e-Contravention Case Management System will provide full-text document indexing solution providing facilities to reduce synonyms, prefixes and suffixes as well as normalizing the relevance of document terms to the size of the document (the calculation of the term weight should not depend on the file size) to eliminate cases of priority of large documents over small documents.

The system must allow morphological searching of data. There are persons whose name transcription was changed during Soviet times, there are persons who have more than one citizenship, etc. Transcriptions and their pronunciation in different languages should be taken into account (e.g. "chi" in Romanian reads "chi", Ukrainian "ki", German "ch" can be "h", "k" or "ș").

The system will have editable morphological dictionaries.

CU S08: Register the record object in the register. A use case that ensures the recording of record objects in the registry based on the event of the RO, who also acts as Registrar, signing the confirmatory documents as part of the workflow. The triggering events for the entry/modification/deletion of data in the registers is described in Chapter 6.2.1.4. *Departmental state record keeping activities related to the contravention process.*

Process/procedural documents that serve as the documentary basis for registry entries shall not be duplicated in the registry. The unique identifier of the document in the e-Contravention Case Management System and its version will be kept in the register.

The value of the information attribute at the time of the record shall be recorded in the register. As some records may be based on different documents or draft documents (e.g. the primary record of the traffic accident is based on the referral) it is important to record the version of the document on which the record was made.

CU S9 Delete the record object from the Register. This use case performs the functionality required to delete records from the register.

CU S10: Automated procedures. The use case includes all automatic procedures performed by the System according to a pre-defined schedule or upon triggering of an event. Examples of automated procedures may serve:

- Generation of predefined reports
- Dissemination of public data and reports via the data.gov.md platform service and the MIA website
- Data backup
- Follow-up of fines payment
- Initiation of procedures for synchronization of data in registers
- Indexing documents and data

- Entering tasks, deadlines for execution of process activities, group events to which the user belongs in the personal agenda
- Etc.

CU S11 Log events. Represents a use case whereby events will be logged in the e-Contravention Case Management System. Any event generated within the business processes digitized in the e-Contravention Case Management System is liable to be logged and saved in the Local Event Logs and MLog.

The logging mechanism will be developed based on standards and best practices implemented in the industry. The IT system will deliver functionalities to configure the logging strategy for business events, including: categories of business events subject to logging, calendar period for logging (fixed or indefinite), etc.

For critical or sensitive business events, logging will be additionally performed via the MLog platform service.

At least the following 3 categories of events will be logged:

1. System events - logging of which is mandatory.
2. Key business events logged on a mandatory basis (e.g. creation of a e-Contravention Case, registration/access/removal of registration from the Register, etc.) - the beneficiary will provide the list of system events.
3. Logging events that can be enabled/disabled by the system administrator.

Logged events will save at least the following categories of data (depending on the nature of the logged event):

- the identifier of the logged event;
- the identifier of the user who generated the event;
- the identifier of the organization to which the user belongs;
- the category of the logged event;
- the time the event was logged;
- the application component that generated the business event;
- the logical component of the e-Contravention Case Management System (contravention case management, registers, etc.) that generated the business event;
- the record affected by the business event;
- details of the action taken by the user;
- reference to the affected information object
- etc.

Logging will maintain a sufficient set of data so that the nature of the modified or deleted data is clear and records affected by the creation or modification events of the e-Contravention Case Management System entities can be easily retrieved.

The logged event shall contain a direct access reference to the information object (document, electronic form, etc.) related to the business event. The only exception shall be events of deletion of information objects.

The user with the role of Administrator of the e-Contravention Case Management System will be able to configure logging strategies for each category of business event produced by e-Contravention Case Management System.

The e-Contravention Case Management System will provide the mechanism for generating reports related to logging events.

The logging mechanism will be able to integrate with the MLog platform service for logging critical business events.

The Administrator of the e-Contravention Case Management System will be able to configure the categories of business events to be additionally logged via MLog.

CU S12: Notify users. Use case that provides the full functionality to notify authorized users of the e-Contravention Case Management System and external actors participating in the contravention case.

The System will automatically generate and dispatch notifications related to any workflow business event.

Depending on the user (user profile configuration data), the e-Contravention Case Management System will provide the following notification strategies:

- notification in the user's dashboard;
- - Email notification;
- - notification via MNotify
- - all the above categories.

Authorized users of the e-Contravention Case Management System (regardless of their roles) will be able to configure their preferences for notification means.

For authorized users, notifications will be stored in their dashboard providing direct access to the source document or file of the notification.

The e-Contravention Case Management System will integrate with the MNotify platform service for the purpose of sending notifications to internal and external users and implementing other means of notification offered by MNotify (SMS, Instant Message, Push, etc.).

A number of events can be mentioned that require notifications to be sent:

1. Notifications to system users:
   - assignment of tasks to the user;
   - traceability events of documents under control;
   - exceeding the deadlines for completion of tasks;
   - agenda event proposed for acceptance/announced/to be carried out in the near future;
   - need for user involvement in workflow activities;
   - need to perform approval actions;
   - outcome of action requested by the user (e.g. signing of electronic document);
   - document traceability events in the workflow (in case of monitoring the progress of the document review process);
   - notifications on automated procedures related to the managed e-cases (e.g. registering/modifying data in the register, moving the file to the archive, etc.)
   - etc.
2. Notifications to participants in the contravention process:
   - notification of individuals participating in the process, in MCabinet, regarding the storing in MDoc of the summons and other documents.
   - notification of individuals participating in the process of the agenda events set out in the summons;
   - notification of the offender about the sanction of the fine imposed and the methods of payment of the fine;
   - etc.
3. Notifications to system administrators

- problems affecting the performance of the operation of the e-Contravention Case Management System;
- etc.

4. Other relevant categories.

7.3. Basic functionalities of the mobile application components e-Data v2

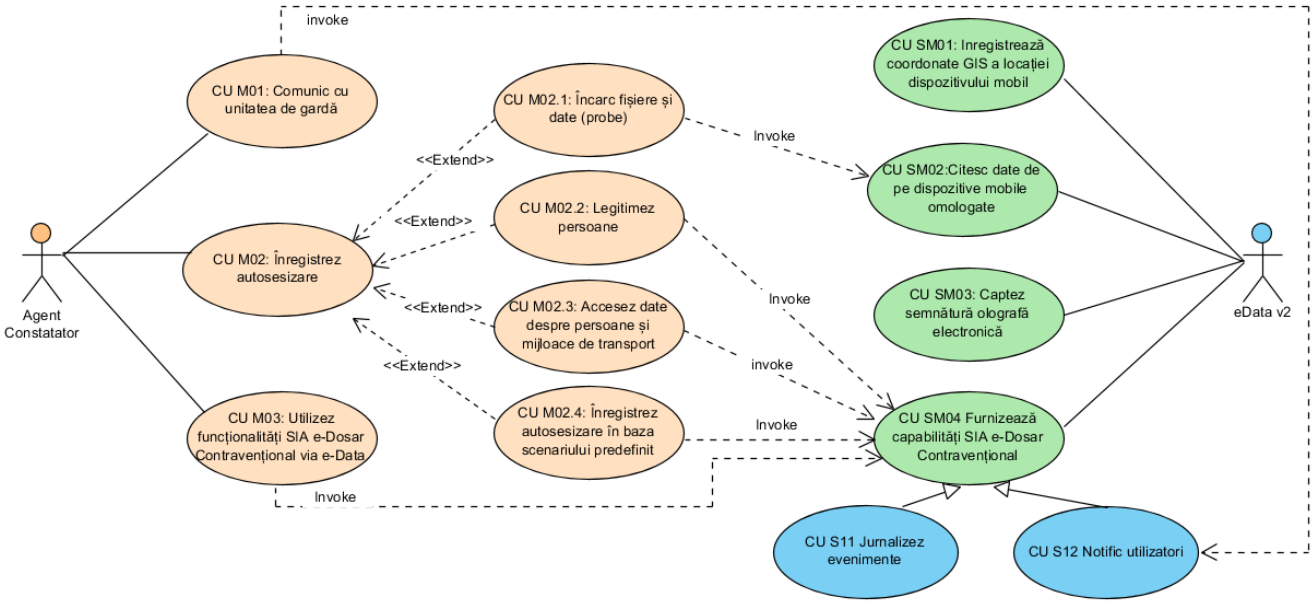


Figure 6. Use cases for the mobile application

7.1.2.1. Use cases – human user

CU M02: Communicate with the duty unit. Use case providing the full functionality required for the communication of the user in the role of RO with the duty unit, such as:

- receiving guidance information in the context of hot track restraint operations;
- receiving directions, orders and instructions to the mobile team;
- communicating to the operational direction center relevant information on events on the ground, actions taken and relevant requests (authorization of actions, help, etc.);

In order to ensure communication, the capability of the e-Contravention Case Management System to notify users of the system is reused.

CU M02: Record self-reporting. Complex use case providing the full range of functionalities required to digitally support the activity of recording contraventions in flagrante delicto.

By using the functionalities provided by the use case the following activities are supported:

1. Collecting evidence of flagrant contravention:

1. Using approved and non-approved mobile devices (CU M02.1)
2. Verifying the identity of the person (CU M02.2)
3. Verifying information on violations based on the consultation of data on persons and means of transport in the e-Contravention Case Management System and other AIS (CU M02.3);

2. Recording the RO self-report by generating the 'self-report form'. The "self-report form" is created:

a) By the system, automatically:

1. On receipt of the structured message with pre-filled 'self-report form' fields from an offence detection AIS (e.g. Traffic Control AIS);
2. On receipt of the structured message, with pre-filled "self-report form" fields, from an approved mobile device that is undeniably capable of identifying the infringement (e.g. Radar);
3. Based on a predefined scenario selected by the reporting officer (e.g. road accident, speeding, etc.). Scenario includes pre-completed templates of the "self-report form".

b) At the deliberate indication of the RO:

1. The system generates a "self-report form" in which the system metadata (system number, document name, data of the reporting agent, date and time of creation, etc.) are filled in. The system assists the RO in filling it in by suggesting different information according to what has been filled in (e.g. when filling in the IDNP, the person data will be extracted from the SRP, when filling in the CC article number, the text will be suggested, etc.)

3. Recording the self-report in the Register of offence referrals (R1) and sending the "self-report form" and evidence to the offence case management workflow.

4. Keeping records of user activities involving access to and processing of personal data in connection with the carrying out of citizens' legitimization and checks by employees of the Ministry of the Internal Affairs and its subordinate institutions.

Similarly, by using e-Data functionalities all photo, video samples will include the geo-location reference. If specialized devices (e.g. radars) are used that transmit geo-location information, this will be retrieved. When the user creates the 'self-report form', it will include the geo-location reference of the location of the mobile device from which it was generated, if the data was not taken from approved mobile devices.

CU M02.1: Upload files and data (evidence). Use case providing the functionality required by the user in the role of the RO for the collection of evidence related to the violation found in flagrante delicto. The use case automates the following RO activities:

1. Accessing data from approved mobile devices for the purpose of detection of violations.
2. Capture photo, video and audio images from non-approved mobile devices for the purpose of being used as evidence. Non-approved mobile devices are considered to be Smartphones and Tablets running e-Data application.
3. Audio recording of the fact of the communication of the person's rights by the RO (or photo/video recording of the fact that they were communicated to him/her.
4. Automatic reading of information from QR code on ID documents (ID card, driving license, etc.).
5. Capturing vehicle identification data, including registration number and vehicle type in real time using the mobile device's camera;
6. Recording the location where the contravention took place.

CU M02.2: Legitimize persons. Use case that provides the functionality required by the user in the role of RO for undeniable person identification. Identification of the person by the RO is done by the following methods:

1. Identification of the person based on the IDNP code written in an official document (ID card, passport, driving license) in:
    a. State Register of Population;
    b. State Register of Drivers;
2. Fingerprint identification of the person, including:
    a. Capturing the fingerprint;
    b. Searching the person by fingerprint in AFIS AIS

3. Identification of the person based on facial image, including:
    a. Capturing the facial image;
    b. Searching for the person in the SRP based on the facial image using the PSA facial recognition solution;

CU M02.3: Access data on persons and means of transport. Use case that provides functionalities with which the user in the role of RO searches and accesses information on persons and means of transport in AIS and eRegisters for the purpose of identifying lack of violations.
The e-Data solution will provide for the search of data on persons and means of transport in both the information resources held by the e-Contravention Case Management System and in:

- e-Contravention cases - information on persons and means of transport in pending cases
- State Register of Contraventions – information on offenders, repeat offenders, penalty points and other currently valid restrictions
- Register of persons and means of transport announced as wanted - data on persons announced in orientation (as wanted) and the reason for their search, data on means of transport announced in orientation (as wanted) and the reason for their search
- The RCA Data Information System - provides information on compulsory civil liability insurance for damage caused by motor vehicles
- "State Register of Population"– provides access to and interaction with data on individuals, serves to retrieve and validate registrations, amendments or deletions (containing data on individuals) for the purpose of checking their correctness in terms of IDNP combinations (if information on the person's IDNP is available), name, surname, ID and others, as appropriate;
- "State Register of Legal Entities" – provides access to data on all categories of legal entities, established on a legal basis. The interaction takes place for the purpose of retrieving and validating data on legal entities regarding the correctness of IDNO, name, code combinations;
- State Register of Transport – provides access to technical, economic and legal information on motor vehicles and motorcycles, tractors, machines and specialized road construction machinery, as well as their owners, for the purpose of verifying the vehicle identification number, title of ownership, holder of the registration certificate and others, as appropriate
- State Register of Drivers - data on the right of the natural person to drive the corresponding means of transport
- State register of administrative-territorial units and addresses - data on administrative-territorial units, streets, buildings and flats when registering residence
- AIS "Register of contravention fines", part of the Information System of the State Tax Service - in order to provide information on fines to the State Tax Service, in accordance with the provisions of Government Decision No 746/2020 on the procedure for providing information on fines to the State Tax Service
- RCA Data Information system – provides information on compulsory civil liability insurance for damage caused by motor vehicles
- Integrated Case Management Programme (ICMP) – for information within the limits of request and administrators' powers
- e-Judicial Case Information Solution (e-JC IS) – for information within the limits of the request and the administrators' powers
- Disability and Workability Determination Information System - for information within the limits of the request and the administrators' powers

CU M02.4: Record self-reporting based on the predefined scenario. This is a functionality whereby the RO is given the possibility to select a predefined scenario for documenting a flagrant violation.

Based on the scenario, the system auto-fills the 'self-report form' and guides the RO to collect evidence. In case of scenarios involving the collection of evidence using approved mobile devices the system automatically interrogates the device, retrieves the data/file and attaches it to the 'self-report form'.

The scenarios are then used to document the case in the contravention case management workflow. Based on the scenario, within the workflow, the RO is proposed to fill in the set of documents that are relevant to the case.

CU M03: Use the functionality of the e-Contravention Case Management System via e-Data. The use case specifies the capability that allows the authorized user to access the full functionality of the e-Contravention Case Management System according to their individual role and rights in the e-Data mobile application interface. The user will be able to access the functionalities provided by the mobile application and other functional components of the e-Contravention Case Management System within a unified interface.

7.1.2.2. Use cases – e-Data system

CU SM01: Record GIS coordinates of the mobile device location. This is a system functionality that provides the recording of GIS coordinates of the location of the mobile device running the mobile application (e-Data v2).

The capability is then used to record in the metadata of unstructured files (images, videos, etc.) and documents (e.g. "self-report form") the GIS coordinates of the mobile device with which they were created.

CU SM02: Read data from approved mobile devices. Represents a capability of the System to integrate with applications provided by the manufacturer of approved mobile devices to retrieve data, images, video, etc.

At least the following approved mobile devices are to be integrated:

1. LTI 20/20 ,,TruCAM" (laser) speed measuring device for vehicles;
2. Drager Alcotest 7510 breath ethanol concentration analyzer;
3. Drager Alcotest 6820 breath ethanol concentration analyzer.

For the purpose of accessing data from approved mobile devices the e-Data application will have capabilities to integrate with device/driver management applications provided by the device manufacturer. The e-Data application shall have integration capabilities with the mobile device management applications/drivers listed above for the purpose of retrieving structured and unstructured data (images, video, etc.).

CU SM03: Capture electronic holographic signature. Represents a functionality whereby a person can electronically sign a document or file using a touch screen device. The electronic holographic signature is attached to the specific document or file being signed. This can be in the form of an image of the digital signature or a specific format that stores the signature information. The electronic holographic signature must be protected by security mechanisms to prevent forgery or subsequent alteration of the signature.

CU SM04 Provide capabilities of e-Contravention Case Management System. Generic use case defining the capability of the e-Data v2 solution to access the functionalities of other modules/applications that form the e-Contravention Case Management System. The capability is used to provide unified interface service for accessing all front end application functionalities intended to support operational activities performed by the police officer;

CU S11: Log events. This use case indicates the mobile app's capability to reuse the e-Contravention Case Management System capability for the purpose of logging business and technology events produced directly when using it. The functionalities provided by the use case relate to:

- logging of business events generated by the functional components of the e-Data mobile application;
- fixing the legal actions taken by the police (e.g. checking the person, means of transport, search, arrest, etc.);
- tracking the location of the mobile device assigned to the user.

7.4. Administration functionalities of the e-Contravention Case Management System

The administration and configuration functionalities of the e-Contravention Case Management System are shown in the diagram in the following figure and consist of the following specific use cases.

Figure 7. Use cases for the administration of the e-Contravention Case Management System

CU A01: Manage users, roles and rights groups. Use case describing the functionalities through which profiles, roles and groups of authorized actors of the information system are managed.

This use case will also provide the full functionality required to define user access rights to user interface components, data or documents and specify the specifics of the behavior of user interface components in interaction with authorized users.

The information system shall provide the necessary functionalities for the management of groups/roles and their associated rights to be subsequently assigned to authorized users. Access rights to the user interface and database records shall be defined by the user's group/role or explicitly for each individual user.

For specific roles, user access rights to the data and functionalities of the e-Contravention Case Management System will be explicitly assigned by the users with administrator role.

The system will provide the administrator with a mechanism to export and synchronize the roles and access rights defined in the e-Contravention Case Management System in MPass. MPass will be used to authenticate users and grant access rights.

The system will have capabilities to set user groups. The group can be used to set different user group specific parameters: e.g. action scenarios, components displayed in the dashboard, etc.

UC A02. Manage classifiers, nomenclatures and metadata. It is a functionality intended for the e-Contravention Case Management System through which it manages all the nomenclatures and metadata related to the System (including the user interface of the information system). A particular feature of this use case is the provision of the functionalities for the drafting of the correlation tables necessary for the normalization of the data received from external sources in accordance with the identifiers of the nomenclatures and classifiers used in the e-Case and the electronic registers.

The nomenclature of articles/items of normative acts, which are taken over in process/procedural documents, must support versions. For each version the validity period can be set. The time of entry into force shall be deemed to be 00.00 on the day indicated.

UC A03. Other administration activities. Set of functionalities outside the implementation objectives of this TOR intended for the e-Contravention Case Management System that includes all operations for the administration and assurance of the functionality of the System that have not been described in other use cases and will be performed through the mechanisms of the operating system or other IT solutions operated within MIA.

UC A04. Configure data exchange interface. Represents a functionality with which the system administrator can set the logging of additional events than those defined by default by the system.

Use cases specific to the Local Administrator role.

CU A05: Configure the system Represents a use case that provides the functionality to configure the operating parameters of the e-Contravention Case Management System. The e-Contravention Case Management System must be a configurable system and its adaptation to the current needs of users and the legal framework in force must be carried out via the user interface without the need for intervention in the program code, its compilation and repeated deployment activities of the information system.

The System Administrator will be able to define at least the following configurations:

- jobs for automatic procedures;
- access paths, values of the variables necessary for the operation of the e-Contravention Case Management System;

- workflows;
- document and report templates;
- validation rules for content, type and size of documents;
- document retention periods (according to document categories and sources);
- rules for indexing document content;
- integration parameters with external information systems;
- information security management system configurations;
- other relevant configurations.

CU A10: Manage users. This is a use case whereby the local administrator via the e-Contravention Case Management System manages user accounts.

It includes associating user roles to functions defined by the flowchart.

> CU A10.1: Manage user account in MPass. This is a use case where the local administrator via the e-Contravention Case Management System manages user accounts in MPass.
>
> The system will provide the administrator with a mechanism to assign the roles and access rights defined in the e-Contravention Case Management System to users registered in MPass. MPass will be used to authenticate users and assign access rights.
>
> CU A10.2: Manage authorized person account in MPower. This is a use case whereby the local administrator via the e-Contravention Case Management System manages accounts of authorized persons in MPower.
>
> The system will provide the administrator with a mechanism to associate users of the system with authorized persons registered in MPower. MPower will be used to validate the empowerment of the RO.

CU A11: Manage stock of blanks of strict record. This use case contains all the functionality required to generate, distribute and track the use of strict record form blanks.

The following strict record blanks are used:

1. Contravention registration report
2. Request for the submission of the declaration of the identity of the driver of the vehicle at the time of committing the contravention.
3. The minutes of collecting objects and documents
4. The order of removal
5. Decision on the examination of the contravention on the basis of the personal finding of the reporting officer
6. Decision on the contravention case
7. Cooperation agreement
8. Minutes of the contravention
9. Contravention record

CU A12: Authorize mobile device. This use case provides functionality for associating mobile devices with a RO. The association is performed for the purpose of monitoring the location of the device and the RO.

Use cases specific for the Designer role

CU D01: Configure entity. Use case providing functionality to create and customize entities. Basically, through the entity builder, users can create and modify entities, defining specific properties, workflows, validation rules,

data entry forms and associated reports. This allows the application to be tailored to the specific needs of the organization and its business processes, improving their efficiency and effectiveness.

CU D01.1: Define organization. This use case provides functionalities for the configuration of the organization type entity in the System, the solution of e-Contravention Case Management System is intended to digitize the workflows for the management of the contravention cases carried out by the competent authorities to resolve contravention cases that do not have their own IT system. In this respect at least the following business functions are to be supported:

- Configure the "organization profile" which includes:
  - Registering the organization in the system which includes creating the information object describing the organization;
  - Defining the organizational structure, roles and specific rights of the users of the organization;
  - Defining the scope of competence according to the Contravention Code;
  - Associating IT Services, workflows, information objects, nomenclatures, reports, screen forms and navigation flows within the application, data flows (interoperability interfaces), notifications and alerts, etc. specific to the organization,
- Manage organization-specific configuration settings for additional modules of the application (e.g. functional module for managing payment bills and tracking fines - "Billing", etc.)
- Perform testing and validation of the organization's configuration to ensure that it meets the organization's requirements and standards.

CU D02: Configure workflow. Represents a use case that provides the functionality required to configure and manage workflows.

Workflows should be definable by specifying processing steps (workflow evolution steps) performed by both well-defined (appointed) users and generic workstations. In this sense a workflow must be able to be designed as a collection of activities that are carried out either sequentially or in parallel according to certain predefined or dynamic scenarios. The number of steps that can be included in a workflow should not be limited.

Similarly, it offers the possibility to automate certain business processes by setting rules and automatic actions. This may include, for example, assigning automatic tasks based on certain events, automatically generating reports or notifications, automatically updating the status of a process, etc.

Provides the ability to link different entities (e.g. screen forms, document templates, etc.) to the workflow which will allow users to create and configure different types of forms needed for business processes. These forms can include data entry fields, selection options, file uploads, custom validations and rules, etc.

Provides the ability to configure workflow integration with other applications and systems so that data and information can be automatically transferred between different applications.

Includes setting of workflow monitoring mechanisms. This allows users to monitor and track the progress of business processes so that any problems can be identified and remedial action taken in a timely manner. This functionality can include generating reports and statistics on the performance of business processes.

CU D03: Configure workspace Represents a use case describing the functionalities intended to delimit the information boundaries of workspaces and the users or groups of users with access to workspaces.

The workspace will increase the convenience of the user interface operation, the users' quick access to the information related to their working environment and the stimulation of collaboration between users of the same group. A workspace can be a grouping of several documents and folders related to a specific issue, access to which is based on access rights.

CU D03.1 Configure forms Use case that provides all the functionality needed for the user to create and manage forms: screen forms, document templates, report templates. The functionalities provided include:

- Form creation and customization: users can create and customize forms according to the specific needs and requirements of their organization.
- Define form structure: Users can define the structure and design of the form, including graphics, fields and supported data types.
- Configure data validation: Users can configure the validation of data entered into forms to ensure that data is accurate and complete.
- Adding rules and actions: Users can add rules and actions to forms to automate processes and ensure data consistency.
- Forms administration: Users can administer forms, including modifying, deleting and updating them in real time.

CU D04 Configure data exchange interface. With this use case the Designer configures new interoperability flows both via MConnect and customized APIs.

CU D05: Register approved mobile device. This use case provides functionality required to integrate the e-Contravention Case Management System with various approved mobile devices for the purpose of retrieving data from them.

CU H01.1: Access archived documents. Use case providing the full functionality required for the authorized user to search and access documents in the digital archive.

The authorized user has access to the metadata describing the archived e-Contravention Case.

The e-Contravention Case Management System will provide authorized users with pre-configured workflows through which they can request access to documents in the archive.

Access to documents in the archive is granted for a specific period of time.

8. Non-functional requirements for the e-Contravention Case Management System

This section sets out the requirements for the non-functional features that must be provided by the IT solution being procured.

Conventions when formulating non-functional requirements

The requirements for the implementation of the e-Contravention Case Management System set out in this document are marked using the following convention:

- all requirements have a unique identifier consisting of two values X.Y, where X is the category of the requirement described in Table 8.1 and Y is the unique identifier of the requirement in the category to which it belongs.
- for each requirement, the mandatory nature is mentioned: M - mandatory requirement to be implemented, D - desirable requirement to be implemented, optional, and *I* - informative requirement.

Table 8.1. Categories of requirements of the ToR

Value	Meaning	Interpretation
LCR	Licensing and intellectual property requirements	The requirements relate to the intellectual property rights related to the e-Contravention Case Management System and the software components required to operate the system.
ARH	Architectural requirement	The requirement relates to the architectural aspects of the design of the e-Contravention Case Management System.
DEL	Deliverable requirement	The requirement refers to the deliverables to be submitted by the developer of the e-Contravention Case Management System.
FLEX	Extensibility requirement	The requirement refers to the extensibility of the e-Contravention Case Management System to adapt to new needs.
GMS	Warranty, maintenance and post-implementation support requirement	The requirement refers to the characteristics of the operational maintenance and post-implementation development services o the e-Contravention Case Management System, requested in the procurement.
INT	Interoperability requirement	The requirement refers to the interoperability framework of the e-Contravention Case Management System.
SLA	Service level requirement	The requirement refers to the quality parameters at which warranty, maintenance and post-implementation support services must be provided.
MG	Project management requirement	The requirement relates to project management aspects during the design, development, implementation, deployment and operation of the e-Contravention Case Management System.
PERF	Performance requirement	The requirement relates to the operational performance of the e-Contravention Case Management System.
RC	Resilience and Continuity requirement	The requirement refers to the properties of the e-Contravention Case Management System to respond to critical events and quickly restore its functionality.
SEC	Security requirement	The requirement refers to the information security aspects that the e-Contravention Case Management System must meet.
SC	Scalability requirement	The requirement refers to the scalability properties of the e-Contravention Case Management System when increasing the number of users, transactions and information base.
SM	Maintenance requirement	The requirement relates to the post-delivery maintenance aspects of the e-Contravention Case Management System.
TP	Platform requirement	The requirement relates to the required technology platform for th e-Contravention Case Management System
UI	User Interface requirement	The requirement refers to the user interface that the e-Contravention Case Management System will provide to authorized users.

The tender submitted by the tenderer must comply with all the requirements indicated as mandatory.

The tender submitted by the tenderer will obtain a competitive advantage for each optional requirement to which it corresponds.

Informative requirements are intended to provide more information for a better understanding of the context of other requirements.

8.1. General requirements

Table 8.2. contains the specification of general requirements.

Table 8.2. Licensing and intellectual property requirements

ID	Compulsoriness	Requirement
MG 001	I	The Service Provider shall ensure and if necessary be able to demonstrate that any component of the e-Contravention Case Management System has been designed and complies with the principles established for the e-Contravention Case Management System specified in Chapter 1.5 of this document.

8.2. Licensing and intellectual property requirements

MIA will hold all the necessary rights for the unlimited use of the IT system and all the software components required for the proper functioning of the Information System.

Table 8.3. contains the specification of the licensing and intellectual property rights requirements for the information system and soft components necessary for system operation.

Table 8.3. Licensing and intellectual property requirements

ID	Compulsoriness	Requirement
LCR 001	I	MIA ensures the following operation environments for the IS: - Production environment; - Test environment; - Development environment. The Beneficiary will deliver the operating environments for the e-Contravention Case Management System in the MCloud platform frame.
LCR 002	M	The tenderer shall include in its bid the licenses for all COTS software products required for the implementation and use of the IS in the three environments provided by MIA. This includes, but is not limited to, the following: operating systems, database management systems, software libraries, utilities and other system software. The quantity of licenses offered must allow access and use of the IS (in any environment in which it operates) by an unlimited number of nominal users, as well as an unlimited number of external systems. There will be no restrictions on the number of documents, transactions or mode of access to the IS (e.g. limitations on concurrent access). The quantity of licenses offered must allow access to the IS application interfaces by any application and external system.

ID	Compulsoriness	Requirement
LCR 003	M	The licensing offer for all software components offered under the above terms will be on a "perpetual" basis.
LCR 004	M	The tenderer shall transfer to MIA all rights to the developments, adjustments, configurations and customizations made for the implementation of the IS as required. These may be related to licensed third-party software products, or may be separate components.
LCR 005	M	The tenderer shall provide the source code for all application components of the e-Contravention Case Management System developed specifically for MIA.
LCR 006	M	For COTS products there will be at least 3 local vendors using the solution. Otherwise, the tenderer will provide source code for COTS products.
LCR 007	M	Any data stored within the SI related databases are the property of MIA. Access to this data throughout the vendor's contract period and beyond is subject to information confidentiality requirements and clauses.
LCR 008	M	The tenderer shall submit its proposed licensing model for the solution, which must meet the above requirements. The tenderer shall describe the proposed licensing model, justifying why it is optimal for MIA. Will provide a comparative analysis with other licensing models typically offered for the offered solution.

8.3. System architecture requirements

The architecture of the e-Contravention Case Management System must be aligned with the needs of the MIA at least in aspects related to extensibility, flexibility and maintenance of the IT system. The MIA opts for an open, modular architecture based on interoperable components. These principles must be visible at all levels of the architecture.

8.3.1. General architecture requirements

Table 8.4. contains the specification of the general non-functional requirements submitted for the architecture of the information system.

Table 8.4. Architecture general requirements

ID	Compulsoriness	Requirement
ARH 001	M	The overall IT solution shall correspond to the "Reference Model for the Architecture of the Information Systems of the MIA" defined in Chapter 5.1. and each level of architecture to the reference models described in Chapter 6.
ARH 002	M	The architecture must be based on open standards.
ARH 003		The architecture must be Service Oriented Architecture (SOA).

ID	Compulsoriness	Requirement
ARH 004	M	The architecture shall be designed in an integrated way, developed with the application of best practices in the field (e.g. architecture principles and reference architectures aligned to TOGAF 9.2).
ARH 005	M	The architecture will be a client-server architecture, organized in at least 3 vertical levels, clearly divided so that each higher level depends only on its lower level.
ARH 006	M	The architecture shall be suitable for deployment and use in virtualized environments.
ARH 007	M	Characteristics of a computer system with deployment-oriented architecture in virtualized environments are: latency aware, component failure aware, parallelizable, resource utilization aware.
ARH 008	M	Communication between all system components shall be secure, using the internal interfaces of the system components for this purpose.
ARH 009	M	The architecture must be designed in such a way as to ensure that the application is scalable - to be able to adapt to an increase in the number of users or/and the volume of data without reducing performance.
ARH 010	M	Error tolerance: the software solution must be able to handle errors and recover quickly from system or network failures.
ARH 011	M	The Contravention Case Management System architecture must support its running in a computing resource orchestration environment / Kubernetes (K8s).

8.3.2. Requirements for the architecture presentation level

The architecture presentation layer is responsible for ensuring user interaction with the business functions of the architecture. This architecture layer manages how users access and use the functions of the information system for both service and administrative purposes.

The e-Contravention Case Management System is to be accessed by officials from the GPI and MIA, other authorities competent to deal with contravention cases and authorized external users. In addition, it will communicate with other MIA or third party systems through external application interfaces (see Interoperability specifications).

Table 8.5. contains the specification of the non-functional requirements submitted to the presentation level of the IT system architecture.

Table 8.5. Architecture presentation level requirements

ID	Compulsoriness	Requirement
ARH 012	M	The e-Contravention Case Management System will integrate user interfaces to allow the user to use a single access point for all business functions for which they have been authorized. Exceptions are allowed for privileged roles (e.g. application component designer, system administrator, etc.).
ARH 013	M	The client application will be able to run in standard operating environments or with minimal configuration from the Beneficiary (e.g. standard system software only).
ARH 014	M	The default client application will be the web browser.

ID	Compulsoriness	Requirement
ARH 015	M	The e-Contravention Case Management System will be compatible with at least 3 o the most used web browsers (*Microsoft Edge, Google Chrome, Safari*).
ARH 016	M	The user interface must be configurable with the possibility to add widgets. A structured interface similar to "MS Outlook" will be provided
ARH 017	M	The presentation layer will not implement business rules except for input validation

8.3.3. Requirements for the architecture business logic layer

The business logic layer of the architecture implements the core functionalities of the information system. The business logic is responsible for accessing, processing and transforming application data, managing business rules and ensuring consistency and correctness of data.

The business logic layer is accessed by the presentation layer to make the business functions of the information system available to users. It can also provide these functions to external software applications via specialized application interfaces which are also part of the business logic layer.

An SOA architecture implies a high level of granularity at the level of the Business Logic component blocks. Each logic block provides its functions through internally and/or externally owned interfaces. These can be accessed by other business logic components, presentation layer components, or external systems.

Table 8.6. contains the specifications of the non-functional requirements submitted to the business logic layer of the information system architecture.

Table 8.6. Architecture business logic level requirements

ID	Compulsoriness	Requirement
ARH 018	M	The level of business logic must be completely independent of the presentation level and the database level.
ARH 019	D	The business logic layer must have a fully modular architecture based on reusable components and abstract interfaces. There should be no identical functionality implemented by different components at this level (e.g. data access).
ARH 020	D	The business logic layer must contain and have delimited business workflow components and business entity components.
ARH 021	D	Access to the business entity components shall be via the business workflow components.
ARH 022	M	Business entities shall be clearly identified at the business logic level and encapsulated in business entity components.
ARH 023	M	The business entity components must be integral and contain all the data and business logic related to the business entity they support, necessary to perform the business operations, apply the relevant business rules and maintain the integrity and correctness of the data contained.
ARH 024	M	The business logic layer components must communicate with each other through dedicated internal interfaces/functions (*tight coupling*).

ID	Compulsoriness	Requirement
ARH 025	M	The business logic layer components must be accessible to external applications only through the external application interfaces defined for this purpose.
ARH 026	M	The business logic layer architecture will allow concurrent access to objects and functions.

8.3.4. Requirements for the architecture data layer

This architecture level is where data is stored and accessed. The data is accessible via database management systems (DBMS). At the DBMS level, integrity rules for the data are established. The data layer must ensure that the data can only be accessed by authorized entities and its integrity and veracity is ensured.

The data layer must ensure the data necessary to provide the business functionalities and services required by the MIA. The requirements of the architecture data layer are set out in Table 8.7.

Table 8.7. Architecture data level requirements

ID	Compulsoriness	Requirement
ARH 027	M	The implemented and supported data model must correspond to the "Conceptual Data Model" defined in Chapter 6.3.1.
ARH 028	M	The data layer architecture should ensure the achievement of the ACID (atomicity, consistency, isolation, durability) rules designed to guarantee the validity of the data despite errors, outages and other accidents.
ARH 029	M	The e-Contravention Case Management System must support an integrated data model for the reference information.
ARH 030	M	The conceptualized data model must ensure the possibility to migrate data from the IT systems currently operated by the MIA.
ARH 031	M	The data must be accessible only through components contained in the business logic layer.
ARH 032	M	The stored data must be neutral and independent of the Business Logic layer.
ARH 033	M	The data architecture must be optimized from the point of view of fast data access for performing transactions and generating statistics and analysis reports. The generation of analysis reports shall not affect the performance of the transactional operations of the system.
ARH 034	M	The data model implemented must be documented in detail. The documentation must contain both the technical description of the data layer (e.g. XSD) and the semantic description (association of data structures to the business entity and their properties). The semantic description of the data must be available to users within the system, where useful (e.g*: report configuration*).
ARH 035	M	Each information object record will have a unique system-wide identification number. The algorithm for assigning the identification number will be configurable within the system and will allow identification of record corruption.

ID	Compulsoriness	Requirement
ARH 036	M	The architecture of the system shall ensure the integrity and correctness of the data when accessed and modified simultaneously by multiple entities (users internal processes, external applications).
ARH 037	M	Data will be protected proportionally to their sensitivity level. Security requirements must be defined at the data level (not at the application level). This means that data security requirements must be established at the level of the data itself, after which they serve as the basis for defining the security model applied at application and infrastructure level. The security model applied at the data architecture level must ensure sufficient granularity to establish access rights in accordance with applicable legal regulations on data protection, including personal data. The CRUD (Create, Read, Update, Delete) matrix will be used to present and validate the data access model
ARH 038	M	The definition of the data security model will be carried out in accordance with ISO27001.

8.3.5. Requirements of the architecture technology level

The ICT infrastructure components (software and hardware) required to run the components that are part of the above layers (data layer, business logic layer and presentation layer) are placed at this architecture layer.

The technology layer of the architecture must ensure the availability and accessibility of the system components. The requirements of the technology layer of the architecture are set out in Table 8.8.

Table 8.8. Architecture technology layer requirements

ID	Compulsoriness	Requirement
ARH 039	M	The technological architecture of the system must have a high level of resistance to crashes, not containing single points of failure (SPOF).
ARH 040	M	The technological architecture shall ensure the rational and balanced use of processing resources.
ARH 041	M	The technological architecture of the system must be defined taking into account the requirements of consolidating data centers in the public sector and rationalizing the administration of state information systems (Government Decision No 414 of 08.05.2018).

8.4. Requirements for the technology platform

The technology platform consists of all the software and hardware components required to provide the operational environment in which it will run. The technology platform includes: development platforms and programming languages in which the code of the information system is developed, database management systems, operating systems on which the system components can run, specific software assurance required to be installed for the correct running of the information system, hardware platform on which the system components run, etc.

In order to have a scalable, flexible and easily maintainable system, there must be a minimum level of dependency of the system on the technology platform on which its components run.

8.4.1. General requirements for the technology platform

Table 8.9. contains the specification of the general non-functional requirements set for the IT system technology platform.

Table 8.9. General requirements for technology platform

ID	Compulsoriness	Requirement
TP 001	M	The platform technologies present in the architecture must be open technologies (no vendor proprietary technologies).
TP 002	M	Components must be independent of the technology platform on which they run (unless such requirements explicitly result from the current Terms of Reference).
TP 003	M	The system architecture must be optimized for running in cloud computing environments. Characteristics of a system architecture oriented towards the implementation of Cloud solutions are: latency aware, component failure aware, parallelizable, resource aware.
TP 004	M	The technologies present in the technology platform must be homogeneous (minimum number of different technologies, e.g. same operating systems for middleware and database).
TP 005	M	The e-Contravention Case Management System must support the creation, modification, processing, storage and access of text in Unicode format.
TP 006	M	The tenderer shall indicate in its offer complete and exhaustive information on the technology platforms supported by its application and the relevant constraints.
TP 007	M	In order to align with the technology stack used for government solutions, if applicable, the following technologies/solutions will be used: - Container Orchestrator - Kubernetes. - Automated configuration and installation of Kubernetes clusters will be based on Helm packages. - As caching or session server, if applicable, Redis will be used. - As a binary file or object storage system, if applicable, MinIO will be used. - As a queued message management or event distribution system, if applicable, Kafka shall be used.

8.4.2. Requirements for the presentation level of the technology platform

The given compartment contains the requirements related to the technologies present at the presentation level of the IT system. Table 8.10 contains all the requirements specific to the presentation level of the e-Contravention Case Management System technology platform.

Table 8.10. Requirements for the presentation level of the e-Contravention Case Management System technology platform

ID	Compulsoriness	Requirement
TP 007	M	The system must be accessible to any user connected to the MIA's corporate network, using the standard computing technology available in the workplace (desktop stations, laptops, tablets, printers, etc.).

TP 008	M	All generated views and reports must be printable on the specified page format. It must automatically size the output documents to fit the format specified by the user (e.g. A2/A3/A4/A5/A6, portrait/landscape, *etc.*). There must be one or more options for the type of output documents (*e.g.: PDF, XML, XLS, DOC etc.*).
TP 009	M	The client side of the system must be able to run on Windows 10, Android 12, IOs 11 and newer operating environments.
TP 010	M	The mobile app (e-Data v2) must be able to run on Windows 10 , Android 12, IOs 11 and newer operating environments.
TP 011	M	The client part of the system must be independent of the operating environment i is running on (accessed via state-of-the-art web browsers).

8.4.3. Requirements for the business logic level of the technology platform

The given compartment contains the requirements related to the technologies present at the business logic level. Table 8.11 contains all the requirements specific to the business logic level of the technology platform of the e-Contravention Case Management System.

Table 8.11. Requirements for business logic level of the e-Contravention Case Management System technology platform.

ID	Compulsoriness	Requirement
TP 012	M	The components forming the business logic layer must be developed in modern programming languages, widely accepted in the industry and especially in the ICT sector of the Republic of Moldova (*e.g.: Java, C# etc.*).
TP 013	M	The technologies present at this level must allow the integration of components that are or will be developed by the MIA through the application interfaces made available.
TP 014	M	The Helm solution will be used to define packages for application installation and configuration in the Kubernetes orchestration environment

8.4.4. Requirements for the data level of the technology platform

The given compartment contains the requirements related to the technologies present at the data level. Table 8.12 contains all the requirements specific for the date level of the e-Contravention Case Management System technology platform.

Table 8.12. Requirements for the data level of the e-Contravention Case Management System technology platform.

ID	Compulsoriness	Requirement
TP 013	M	The provider will ensure the data storage mechanism.
TP 014	M	If necessary the provider will identify additional needs to ensure the legality and performance of the system (additional licenses, data storage equipment, etc.)
TP 015	M	The e-Contravention Case Management System must be compatible with the database management systems currently used by the MIA.

8.4.5. Requirements for the technological level of the technology platform

The given compartment contains the requirements related to the technologies used by the platform. Table 8.13 contains all the technology specific requirements of the e-Contravention Case Management System technology platform.

Table 8.13. Requirements for the technologies of the e-Contravention Case Management System technology platform

ID	Compulsoriness	Requirement
TP016	M	All system components (e.g. operating systems, middleware, databases) must be able to run in virtualized environments.
TP019	M	The tenderer shall include in its offer detailed information on the recommended technology platform (within the limit of available alternatives), taking into accoun the needs of MIA set out in this ToR. In the case of a winning bid, this will be taken as the basis for determining the technology platform for the system.

8.5. Interoperability framework requirements

Interoperability is the ability of a computer system to communicate with other computer applications. The system architecture establishes the interfaces that must exist between other systems of the Ministry of Internal Affairs or public authorities of the Republic of Moldova. Table 8.14 defines the requirements for the interoperability characteristics of the MIA.

Table 8.14. Requirements of the interoperability framework of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
INT 001	M	All exposed interfaces must be based on open standards. All message flows between and among external entities shall be carried out using open standards.
INT 002	M	The e-Contravention Case Management System shall have the application interfaces specified in the forthcoming ICT Architecture Document, annexed to the Terms of Reference.
INT 003	M	All provided interfaces will be able to interact with external applications in both real and off-line mode.
INT 004	M	The system will have capabilities to define new standard interfaces for accessing all key business functions of the system (e.g. document generation, transaction generation, accessing information about the business entities stored within). These interfaces must allow the management of business entities with the application of all relevant business rules and the use of all business entity properties.
INT 005	M	The system shall have capabilities to define new interfaces for accessing external systems using open standards. These interfaces will be accessible for calling within the system functions when implementing the functionalities.
INT 006	M	The system will have standard interfaces for exporting data to Data Warehouse tools.

ID	Compulsoriness	Requirement
INT 007	M	All system interfaces shall be adequately documented (e.g. applying the Web Services Description Language model).
INT 008	D	The e-Contravention Case Management System will have specific capabilities similar to ESB solutions. These capabilities will be able to be used both for integration with external systems as well as for interoperability with external systems without participating in the information exchange flow.

The e-Contravention Case Management System must take into account the related aspects of the information technologies used and the initiatives in this field in force in the Republic of Moldova. The relevant requirements in this respect are specified in Table 8.15.

Table 8.15. Requirements for ICT related issues and initiatives

ID	Compulsoriness	Requirement
INT 009	M	The e-Contravention Case Management System will integrate with the Government's MConnect interoperability framework for the purpose of interacting and exchanging data with external IT systems (e.g. integration with state registries, document exchange with central public authorities, etc.).
INT 010	M	The e-Contravention Case Management System will use the MPass platform service as a mechanism to authenticate users via electronic identity.
INT 011	M	The e-Contravention Case Management System will use the state information resource Register of empowered persons (via MPower or MPass) to validate the RO mandate.
INT 012	M	The e-Contravention Case Management System will use the MSign platform service as the digital signature infrastructure.
INT 013	M	The e-Contravention Case Management System will use the MLog platform service as a logging mechanism for critical business events.
INT 014	M	The e-Contravention Case Management System will use the MNotify platform service as a user notification mechanism.
INT 015	M	The e-Contravention Case Management System will use the MCabinet platform service as an interaction mechanism with parties participating in the contravention process who do not have a user account or do not use a system interoperable with the e-Contravention Case Management System.
INT 016	M	The e-Contravention Case Management System will use the MDoc platform service to store documents for parties involved in the process who do not have a user account or do not use an interoperable system with the e-Contravention Case Management System
INT 017	M	The e-Contravention Case Management System will integrate with the Open Data Portal of the Republic of Moldova (http://date.gov.md) for the purpose of publishing public datasets.

8.6. Performance requirements

The e-Contravention Case Management System must have the capacity to process transactions made by MIA users in a timely manner, according to the volume resulting from MIA activity. Table 8.16 identifies the performance requirements it must meet.

Table 8.16. Performance requirements

ID	Compulsoriness	Requirement
PERF 001	M	The response time to an external user/service transactional query must not exceed one second (not including report generation)
PERF 002	M	The e-Contravention Case Management System must be able to handle up to 1000 concurrent sessions (authorized user connections and external systems).
PERF 003	M	The tenderer shall include in the system administration and operation guidelines information on the processes that may decrease performance and its recommendations on running these processes concurrently (e.g. it is not recommended to run process X to generate daily reports simultaneously with process Y to generate the backup).
PERF 004	M	Generating reports and accessing information for business analysis purposes should not affect the operational performance of the system at the transaction processing level. System documentation shall identify reports with significant performance impact and provide vendor recommendations for generating those reports in a manner that does not impact performance metrics.
PERF 005	M	The tenderer shall indicate in its tender the minimum guaranteed values for the system performance characteristics with reference to the technology platform recommended by the tenderer.
PERF 006	M	The e-Contravention Case Management System must have the capacity to process at least 100 000 transactions per day.

8.7. Flexibility requirements

The e-Contravention Case Management System must have the capacity to be adapted over time to new needs generated by the activity of the MIA. It is preferable that this is possible through adjustments in the system configurations (without changing the program code), thus minimizing adjustment costs on the MIA side. Table 8.17 contains the flexibility requirements to be met.

Table 8.17. Flexibility requirements

ID	Compulsoriness	Requirement
FLEX 001	M	The e-Contravention Case Management System will allow the configuration of views and forms for users. The IT system will allow the creation of new user forms for accessing the business logic of the system.
FLEX 002	M	The e-Contravention Case Management System will allow the configuration of existing reports (e.g.: data set adjustment, reformatting).

ID	Compulsoriness	Requirement
FLEX 003	M	The e-Contravention Case Management System will allow the addition and configuration of new reports and statistics (example: data set definition, report formatting, definition of calculated fields).
FLEX 004	M	The e-Contravention Case Management System will allow the configuration of performance indicators (KPI) and the graphical presentation of indicators in the Dashboard.
FLEX 005	M	The e-Contravention Case Management System will allow the configuration of automatic report generation. Automatic generation will occur at certain events within the system or at certain points in time. Generated reports will be able to be stored within the system or sent to set email addresses / or users.
FLEX 006	M	The e-Contravention Case Management System will allow the definition and configuration of business entities stored within the system (e.g. definition of new properties) by adjusting its data model accordingly.
FLEX 007	D	The e-Contravention Case Management System will allow the configuration of the scheduled running of system procedures (jobs) according to time or execution parameters of certain events in the system. The IT system will allow the installation and configuration of new system procedures.
FLEX 008	M	The e-Contravention Case Management System will allow the definition and configuration of business flows (e.g.: operation consecutiveness, status transformations for business entity properties, documents and records generated, notifications, roles involved and operations allowed, etc.).
FLEX 009	M	The e-Contravention Case Management System will allow the definition and management of the regulatory reference information used within the system. The data source for the reference information can be internal or external (e.g. external database, external web service, external file).
FLEX 010	M	Potentially variable information in (example: different parameters, constants, data storage paths, connection paths to external services, classifiers, etc.) will be configurable and will NOT require recompilation of the solution or direct intervention in the database. It must be possible to make these changes in user interfaces convenient for administrators.
FLEX 011	D	The e-Contravention Case Management System must allow the integration of components developed by the MIA in other software development projects. These components will have access to the public functions and properties of the system components.
FLEX 012	M	The e-Contravention Case Management System shall allow the definition of the status of an information object or electronic form. The access rights must allow the user to define the operations allowed, according to the status allowed for the information object (the information system must have a conflict detection mechanism in case the status for which rights are set changes).

8.8. User interface and ergonomics requirements

The system interface shall be user-friendly, easy and intuitive to use. Training time for use shall be kept to a minimum. Users shall have access at all times to support information to facilitate correct use of the system. Table 8.18 contains requirements for the usability characteristics to be met.

Table 8.3. Requirements for the user interface of the e-Contravention Case Management System.

ID	Compulsoriness	Requirement
UI 001	M	All user-accessible business functions must be accessible through graphical user interfaces.
UI 002	M	The system must have user interfaces that are friendly, intuitive and convenient t use for users in non-administrator and administrator roles. The information required by the user for the purpose of performing service tasks must be visible and accessible. The user interface shall have unique graphic design styles. The graphical elements and texts used shall be used consistently in terms of their associated meaning
UI 003	M	All user interfaces must be developed at least in Romanian and Russian. The user will be able to select the language version of the user interface.
UI 004	M	User interface elements must comply with Level A Web Content Accessibility Guidelines (WCAG) 2.0 requirements.
UI 005	M	The user interface shall be optimized for desktop or notebook computers with 1360x768 resolution.
UI 006	M	The e-Contravention Case Management System will have, for the most important functionalities, the possibility to adapt the user interface (it will deliver responsive interface) depending on the device used by the user (notebook, desktop computer, tablet, smartphone).
UI 007	M	The e-Contravention Case Management System must allow the centralized definition or translation of specific terms used within the system (e.g. Delete = Deletion). These terms will be retrieved in this way in all cases of their use within the system.
UI 008	M	The e-Contravention Case Management System will allow intermediate saving of work and operations initiated by the user (automatically or at the user's request).
UI 009	M	The e-Contravention Case Management System shall have an integrated data search function. The data and records retrieval procedures shall be carried ou by means of simple searches (specification of search strings) or more complex searches, through which a more precise filtering of the information can be carried out (QBE forms). Regardless of the nature of the information searched for, the user shall use the same query and data retrieval method for each compartment of the user interface of the IT product.
UI 010	M	In addition to the QBE-based search module which will allow sophisticated queries to be defined visually, the user interface must offer the possibility of refining the search results by providing the possibility of filtering the information in th list of search results.
UI 011	M	Indexed measures (values from classifiers, nomenclatures) must be filterable by choosing the value from predefined lists. For numeric or calendar date fields,

ID	Compulsoriness	Requirement
		it must be possible to filter by the exact value of the searched characteristic (Example: 01.01.2016 - all records with specified date) or by logical criteria (Example: <31.12.2016 - all records with date older than 31.12.2016, >07.04.2009 - all records with date more recent than 7 April 2009).
UI 012	M	It must be possible to filter the results by mask (e.g. filtering by IDNO) according t the pattern: 1006600058* - all sequences starting with the string "1006600058", *EANU - all sequences ending with the string "EANU" or *IMUNIT* - all sequences containing the string "IMUNIT".
UI 013	M	The content of any table of results must be exportable in either DOC/DOCX, XLS/XLSX and PDF format.
UI 014	M	The system will allow attaching files to information objects, or references to files stored on the file/web server for all information objects by default. This functionality will be used by users depending on the access profile settings. Attachment files will contain a set of attributes: creation date, modification date, responsible person, size.
UI 015	M	System users will have access to context-sensitive help in all system interfaces.
UI 016	M	When using the report definition and configuration functions, users shall be able to access the data dictionary stored within the system.
UI 017	M	All user interfaces shall contain background text (water marks) with the user's Name, Surname and Individual Code. The measure is intended to make users accountable and limit information leakage.

8.9. Maintenance requirements

In order to be available and accessible to business users at the agreed level, it must be continuously monitored and maintained. The IT system must allow proactive identification and prevention of problems through easy operational maintenance activities across all system components. Table 8.19 contains requirements for related maintenance features.

Table 8.4. Maintenance requirements for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SM 001	D	The e-Contravention Case Management System will have mechanisms to monitor the level of loading and operation for all key components (e.g. business logic layer and data layer components).
SM 002	D	The e-Contravention Case Management System will generate notifications if the load level on certain components exceeds critical thresholds (example: for a certain period, the average load level was more than 90%).
SM 003	M	All errors and exceptions in the operation of the system will be recorded.
SM 004	M	The provider will list the means to be used for technical troubleshooting of the system
SM 005	M	The provider shall prepare means facilitating system administration functions: • the start of system components; • restarting system components,

ID	Compulsoriness	Requirement
		• creation of backup of database and content files, • restoring functionality on the basis of the specified backup,
SM 006	M	Source code shall be written according to the recommendations for writing maintainable source code, including: well structured, accompanied by comments, suggestive variables, etc.
SM 007	M	The architecture will allow the implementation of system changes in a simplistic way for the MIA. The perimeter affected by the changes will be minimal and the components to be tested as a result of the changes will be clearly identifiable.
SM 008	M	The e-Contravention Case Management System will allow the definition and running of scheduled tasks for operational maintenance activities (e.g. historical data archiving, data preparation for complex reports).
SM 009	M	The architecture will allow the implementation of new versions delivered by the vendor without affecting existing configurations, components implemented by MIA and interfaces implemented for interaction with external IT systems
SM 010	M	The e-Contravention Case Management System will be easily deployable from the production environment to other operating environments in order to ensure the testing and development processes of the system. The system documentation should describe this process.
SM 011	M	The e-Contravention Case Management System shall have procedures for processing all generated errors. Errors generated in the operation of the system will be recorded and accessible for further analysis and improvemen of the quality of the functioning of the IT solution.

8.10.Scalability requirements

Over the course of use, the number of transactions processed and concurrent users is likely to increase or decrease significantly from period to period. In order to make rational use of processing resources, the IT system must be easily scalable (upwards and downwards). Table 8.20 contains requirements for the related scalability characteristics.

Table 8.50. Scalability requirements for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SC 001	M	The e-Contravention Case Management System will allow for increased processing capacity without disrupting their operation. To this end, the system will support horizontal expansion of processing capacity (e.g. adding new server nodes and performing load balancing).
SC 002	D	The e-Contravention Case Management System will be configurable for automatic scaling at the level of key components (lag sensitive). Scaling of the system will be both up and down.
SC 003	M	The system shall have the ability to serve virtually an unlimited number of transactions, subject to appropriate allocation of processing and data storage resources. Resources will be allocated horizontally (allocation of nev servers without increasing performance on existing servers).

SC 004	M	The e-Contravention Case Management System must support the running in a computing resource orchestration environment Kubernetes (K8s) in order to ensure horizontal scalability.

8.11. Requirements for ensuring security

The e-Contravention Case Management System shall allow adequate control over the information security risks associated with its use. The security measures implemented must be aligned with the security policies approved within the MIA and ensure adequate prevention, detection and response to security incidents.

The Contravention Case Management System must implement a "Multi-layered security" approach at the system level and have the ability to be integrated into the institutional model of the MIA for information security management (based on the ISO 27000 family of standards).

In this section, the requirements for the system-related security features required by the MIA are established.

8.11.1. Security architecture requirements

The given compartment contains the requirements related to the security architecture implemented in the framework. Table 8.21 contains all the requirements of the security architecture.

Table 8.6. Requirements for security architecture

ID	Compulsoriness	Requirement
SEC 001	M	The architecture should be designed using a 'Secure by design' approach.
SEC 002	M	The security architecture of the system shall be documented at all levels. The documentation shall contain a description of the security model implemented the components present and the role of each component in terms of security
SEC 003	M	For the technical level, the documentation shall contain the specifications for the network placement of the system components and the vendor's recommendations for the network access rules to be set by MIA for secure access to all system components (e.g. inter-service communication matrix).
SEC 004	M	All system processes related to system components will run with the minimum privileges necessary to perform the assigned tasks.
SEC 005	M	All access credentials used by the application shall be configurable in the administrative interfaces. No hard-coded access credentials shall be contained.
SEC 006	M	The e-Contravention Case Management System shall not contain access credentials stored at the level of its components (in the database, configuration files) in open form.
SEC 007	M	All external interfaces will be accessed using secure authentication methods (e.g. X.509 certificates).
SEC 008	M	Access to functions offered to unauthenticated users (case of service exposure to the official MIA web page) is controlled by means of protection against service overload by one or several network nodes.
SEC 009	M	All fields in the forms filled in by users must be validated by type on both client and server.

ID	Compulsoriness	Requirement
SEC 010	M	The e-Contravention Case Management System will be secured for OWASP Top 1 vulnerabilities.
SEC 011	M	The e-Contravention Case Management System will ensure the confidentiality of data transmitted-received over the communication channels.
SEC 012	M	User actions are recorded in electronic logs.
SEC 013	D	The system issues a periodic signal indicating its operational status.

8.11.2.Requirements for login mechanism

The given compartment contains the requirements related to the authentication mechanism to be implemented in the framework. Table 8.22 contains all the requirements of the authentication mechanism.

Table 8.7. Requirements for the login mechanism

ID	Compulsoriness	Requirement
SEC 014	M	The e-Contravention Case Management System will allow access to its functions only after successful user/administrator login.
SEC 015	M	The e-Contravention Case Management System will support at least the following authentication methods: • ID and password based, Windows authentication (Active Directory integration) • M-Pass account based. The e-Contravention Case Management System will allow users to change individua passwords.
SEC 016	M	The e-Contravention Case Management System will allow the registration of users and their profile information (e.g. ID, password, name, surname, email, etc.).
SEC 017	M	Users' passwords must be protected. The password protection method must ensur that passwords cannot be intercepted, deducted or recovered.
SEC 018	M	The e-Contravention Case Management System will allow the definition and implementation of sets of password usage policies. The policies must allow setting requirements for at least: • password complexity; • mandatory password change; • password lifetime; • repeated use of passwords; • number of failed authentication attempts; • dictionary of forbidden passwords. The computer system shall provide the user with timely information on the enforcement of password usage policies (e.g. password expiry message in N days).
SEC 019	D	The e-Contravention Case Management System will allow differentiated applicatior of password usage policies for different user groups.

ID	Compulsoriness	Requirement
SEC 020	M	The e-Contravention Case Management System will allow blocking, deactivating or suspending user accounts at application level.
SEC 021	M	The e-Contravention Case Management System will be able to be integrated with the directory service implemented within the MIA (MS Active Directory solution is used within the MIA). When creating a new user account, it will have the option to select from the list of users available within the directory service.
SEC 022	D	The e-Contravention Case Management System will be possible to be integrated with external services such as ISPs (Identity Services Providers), using open standards and protocols (e.g. SAML). The authentication methods to be supported with the involvement of an external ISP are: • ID and password; • X.509 certificates; • OTP (One Time Password).
SEC 023	M	In the case of mobile applications access will be based on a user's login credentials and a unique key set in the client application configuration. Communication with the System server will be encrypted.
SEC 024	D	The e-Contravention Case Management System will allow differentiated application of authentication methods, depending on the resources accessed (e.g. default ID and password, additional OTP for the administrative interface).
SEC 025	M	The e-Contravention Case Management System will allow setting the number of simultaneous connections that can be initiated by a user.
SEC 026	M	The e-Contravention Case Management System will allow setting the timeout of user sessions in case of inactivity.
SEC 027	M	The e-Contravention Case Management System shall have effective mechanisms to prevent unauthorized takeover of active sessions initiated by legitimate users.
SEC 028	M	The session will be blocked upon user request or automatically when the user session expires.

8.11.3.Requirements for the authorization mechanism

The given compartment contains the requirements related to the authorization mechanism to be implemented in the framework. Table 8.23 contains all the requirements of the authorization mechanism.

Table 8.8. Requirements for the authorization mechanism for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SEC 029	M	The e-Contravention Case Management System will allow granular management of access rights to all IT system objects and possible actions on them (e.g. business entities, business entity properties, electronic forms, menus, reports, create/view/update/delete actions).
SEC 030	M	The method of authorization within the system will be based on the principle "anything not explicitly allowed is prohibited".

ID	Compulsoriness	Requirement
SEC 031	M	The e-Contravention Case Management System will allow the definition of user groups and roles within the system and the association of users to these groups and roles.
SEC 032	M	The e-Contravention Case Management System will allow access rights to be granted to explicit users, groups and roles. A user group will be able to contain multiple subgroups/roles. A user may be associated with one or more groups and roles, with their access rights determined cumulatively.
SEC 033	M	The e-Contravention Case Management System will allow access rights to be granted based on business rules (e.g. only modify the document if the user is the author, or if the operation is done within a certain timeframe, status or context).
SEC 034	M	The e-Contravention Case Management System will allow the temporary assignment of rights held by one user to another user. The assignment will be able to be made with the preservation or suspension of the rights held by the user to whom the rights are delegated.
SEC 035	D	The e-Contravention Case Management System will allow the segregation of administrative activities (e.g. Administrator 1 modifies, Administrator 2 confirms).
SEC 036	M	The e-Contravention Case Management System will provide views and reports on the access rights configured. These will be configurable according to at least the following criteria: user group/roll in, user ID, business entity, business entity ownership, actions allowed.

8.11.4.Requirements for the input/output data validation mechanism

The given compartment contains the requirements related to the input/output data validation mechanism in the provided electronic forms. Table 8.24 contains all the input/output data validation mechanism requirements of the electronic forms provided by the system.

Table 8.9. Requirements for the input/output data validation mechanism of the electronic forms provided by the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SEC 037	M	The e-Contravention Case Management System will have adequate mechanisms to prevent manipulation of input data (input data from authorized users, input data from external applications).
SEC 038	M	All critical and sensitive data modification actions will be carried out through specialized forms and documents, according to the workflow established for these categories of documents.
SEC 039	M	The e-Contravention Case Management System will perform full and independent data validation on the presentation level, business logic level, data level, in order to ensure data integrity, completeness and correctness.
SEC 040	M	All data displays within must be accompanied by a security flag, as per a classifier established for this purpose within.

ID	Compulsoriness	Requirement
SEC 041	M	Confidential data will not be stored and accessed insecurely within (e.g. in log files, caching).
SEC 042	M	The e-Contravention Case Management System will have additional mechanisms to protect particularly confidential data (e.g. masked data display, data storage in encrypted form, repeated user authentication, etc.).
SEC 043	M	The e-Contravention Case Management System will have routine procedures for checking and detecting possible corruption of data integrity relationships.
SEC 044	M	The e-Contravention Case Management System will have appropriate mechanisms in place to prevent manipulation of data stored within the application.

8.11.5.Requirements for the logging and audit mechanism

The given compartment contains the requirements related to the event logging mechanism and the security audit within. Table 8.25 contains all the requirements of the provided logging and audit mechanism.

Table 8.10. Requirements for the event logging and audit mechanism of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SEC 045	M	The e-Contravention Case Management System will have audit components that wi centrally collect and manage audit records at the level of each module of the IT system.
SEC 046	M	The audit component will allow granular configuration of audit policies.
SEC 047	M	The e-Contravention Case Management System will allow the establishment of audi policies at the object/business entity level and at the logged event level.
SEC 048	M	The E-Contravention Case Management System will allow setting specific characteristics of events to be logged (e.g. products within a certain time frame a certain value of business entity owners).
SEC 049	M	The e-Contravention Case Management System will allow auditing of any event, at the level of any object or business entity within the IT system.
SEC 050	M	Each audit record will contain at least: • the time of occurrence of the event; • the subject of the event (user ID); • the business object or entity affected; • the event produced; • the IP address of the source initiating the event.
SEC 051	M	Audit records will not contain confidential business information (e.g. passwords entered on failed login attempts).
SEC 052	M	Errors that may occur when logging audit records must not affect the normal functioning of the system.
SEC 053	M	The audit component will use the system clock set at the operating system level where the audit component is running.

ID	Compulsoriness	Requirement
SEC 054	M	The audit component shall have a mechanism for archiving historical audit records. The archiving process will be configurable (frequency, data age, archiving format, destination, etc.).
SEC 055	D	The e-Contravention Case Management System will be able to automatically generate notifications to the responsible persons when certain security events occur, according to the configured settings.
SEC 056	D	The audit component will be able to be integrated on the basis of open standards with solutions such as SIEM (Security Incident and Event Management) in order to take over the audit records produced within the system by those solutions.
SEC 057	M	The e-Contravention Case Management System will allow the fixing of historical versions of data, which will be considered particularly sensitive.
SEC 058	M	Status change activities and responsible for records will be logged.
SEC 059	M	The e-Contravention Case Management System will have convenient tools for accessing and processing logged events, including filtering audit records by any field held and exporting them in the usual format. The system's audit tools will also be usable for importing audit file archives for occasional analysis activities.
SEC 060	M	The e-Contravention Case Management System will have secure mechanisms to protect the integrity of the recorded audit information.
SEC 061	M	Critical business events will be able to be logged in parallel via the government's MLog logging system.
SEC 062	M	The e-Contravention Case Management System will provide a mechanism to configure business events to be logged alternatively and through the MLog service.

8.11.6.Requirements for the exception and error management mechanism

The given compartment contains the requirements related to the exception and error management mechanism. Table 8.26 contains all the requirements of the exception and error management mechanism provided by the system.

Table 8.11. Requirements for the exception and error management mechanism for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
SEC 063	M	The e-Contravention Case Management System will centrally record all exception and errors generated by its components.
SEC 064	M	When an error occurs, it will display a generic error message to the user. It may contain an error code and a unique error identifier to facilitate the involvement of support services.
SEC 065	M	The e-Contravention Case Management System will have the necessary tools to analyze and process exception and error records.
SEC 066	D	The e-Contravention Case Management System will be able to automatically generate notifications to the responsible persons when certain errors occur in the operation of its components.

8.12. Resilience and continuity requirements

This section sets out the requirements for continuity and resilience features related to the system required by the MIA.

Table 8.12. Requirements for the resilience capabilities of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
RC 001	M	The e-Contravention Case Management System will have implemented tools to execute the automatic generation of backups and management of historical backups.
RC 002	M	The e-Contravention Case Management System will have mechanisms in place to ensure data integrity in the event of a failure of any component.
RC 003	M	The e-Contravention Case Management System must have mechanisms in place to operationally restore availability and accessibility in the event of continuity incidents.
RC 004	M	The architecture must be resilient to component failures and have no single point of failure (SPOF).
RC 005	M	The e-Contravention Case Management System must have mechanisms in place to ensure data integrity in the event of accidental failures of any of its components.
RC 006	M	The e-Contravention Case Management System must have mechanisms in place to operationally restore availability and accessibility in the event of continuity incidents.

Annexes

Annex. A1
Management of referrals and self-referrals: GPI Order No 562/2021 on the approval of the Standard Operating Procedure for the receipt, registration, recording, examination and archiving of referrals

Generalities

Referral - is the action of bringing to the attention of the police authorities a case (considered illegal) for investigation and resolution and is the primary source of information on possible acts committed, which may be criminal, contravention, administrative or disciplinary misconduct.

Depending on the form in which they are received, the content of the information and the procedure for examining them, referrals are divided into two categories: referrals concerning offences and other information concerning offences and incidents.

Referrals about offences include complaints, denunciations, self-denunciation made by a natural or legal person, reports on the direct detection by the prosecution body or prosecutor of a reasonable suspicion that an offence has been committed, drawn up in accordance with the provisions of Articles 262-264 of the Criminal Procedure Code (hereinafter referred to as CPC).

Other information on offences and incidents - includes information made public by the media, received by telephone, fax, telefax, teletype, Internet and other unverified sources, anonymous complaints and denunciations, as well as verbal and written signals about facts and incidents, which do not contain the description of a concrete offence, and contain deviations from the provisions of Articles 262-264 of the CPC.

The registration and recording of referrals on offences and other information on offences and incidents is carried out in the automated information system "Register of Forensic and Criminological Information".

Referrals of offences shall be recorded in the Register of Referrals of Offences (hereinafter referred to as Register No 1) and other information on offences and incidents shall be recorded in the Register of Other Information on Offences and Incidents (hereinafter referred to as Register No 2), which shall be regarded as a single primary record.

The registration and recording of referrals of offences and other information on offences and incidents is carried out by the specialized units (Duty Service/Statistical Service).

In the absence of a specialized unit in the structure of the police subdivision, the activities of registration and recording of referrals of offences and other information on offences and incidents are carried out by the person authorized by the administrative act of the head of the subdivision.

Referral to police subdivisions

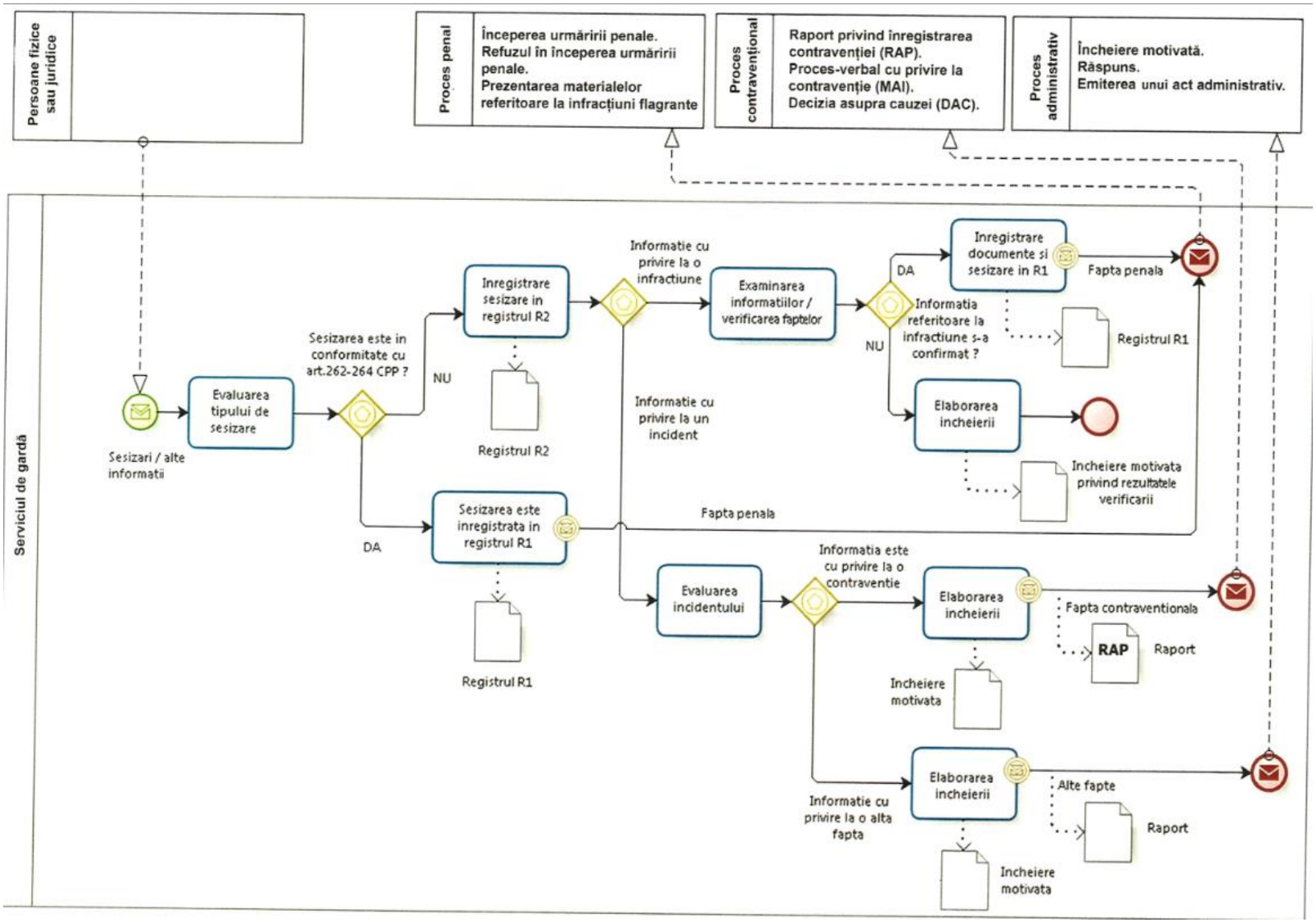
Referrals to police subdivisions can be made as follows:

1. Referrals received at the Duty Service;
2. Referrals received by telephone;
3. Self-reporting;

4. Petitions submitted to the Secretariat/Chancellery or petitions received through the "Posta Moldovei", Special Courier Office of the Intelligence and Security Service;
5. Petitions submitted in electronic form (via web portal and e-mail);
6. Referrals received through the video monitoring system of road traffic.

Referrals received at the Duty Service.

The referrals received directly at the Duty Service are mainly referrals about offences or other information about offences and incidents.

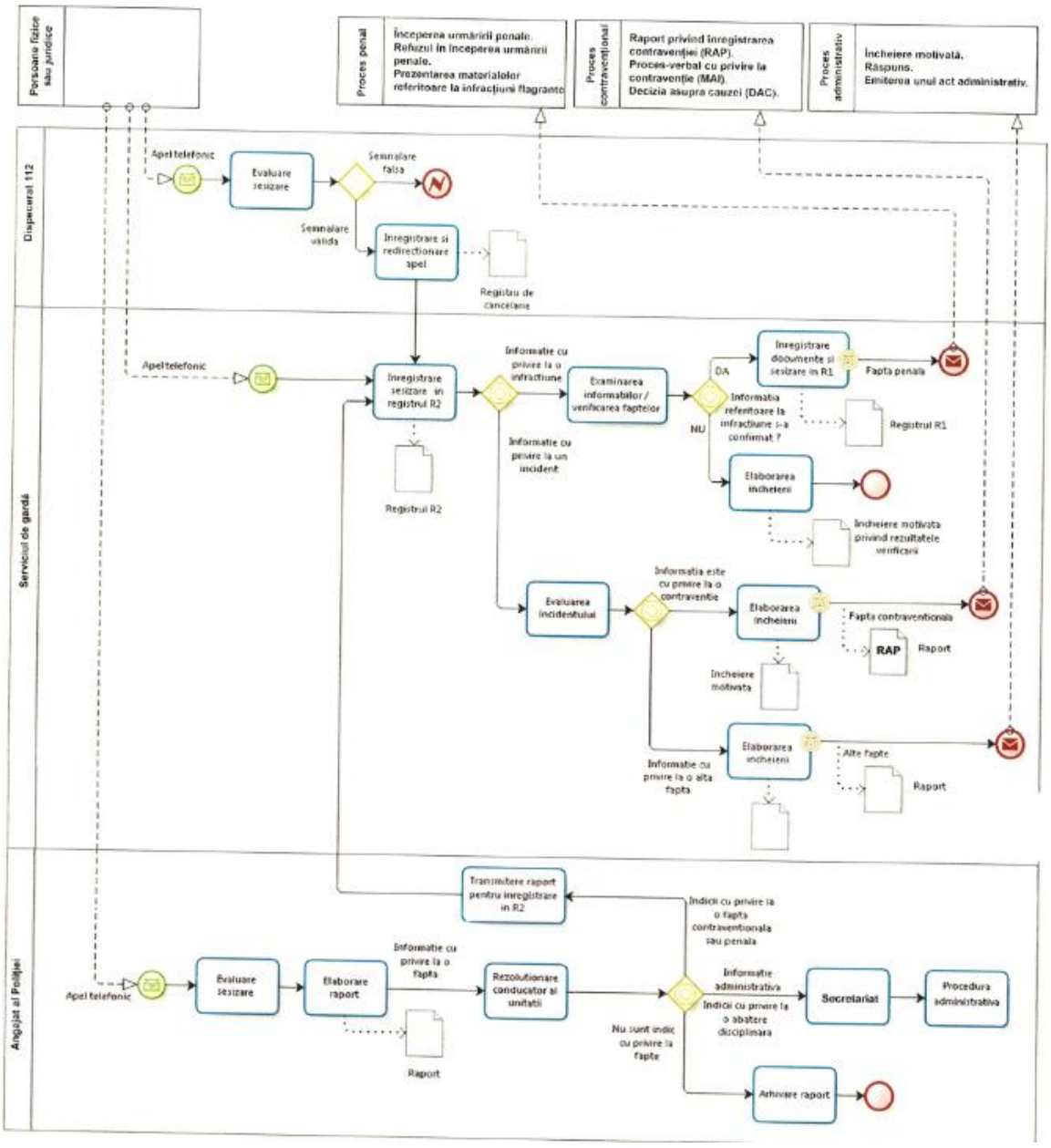


Flowchart of the process of handling referrals received at the Duty Service.

Referrals received via telephone.

From the perspective of the handling of the communicated referral, the information received by telephone may concern the following situations:

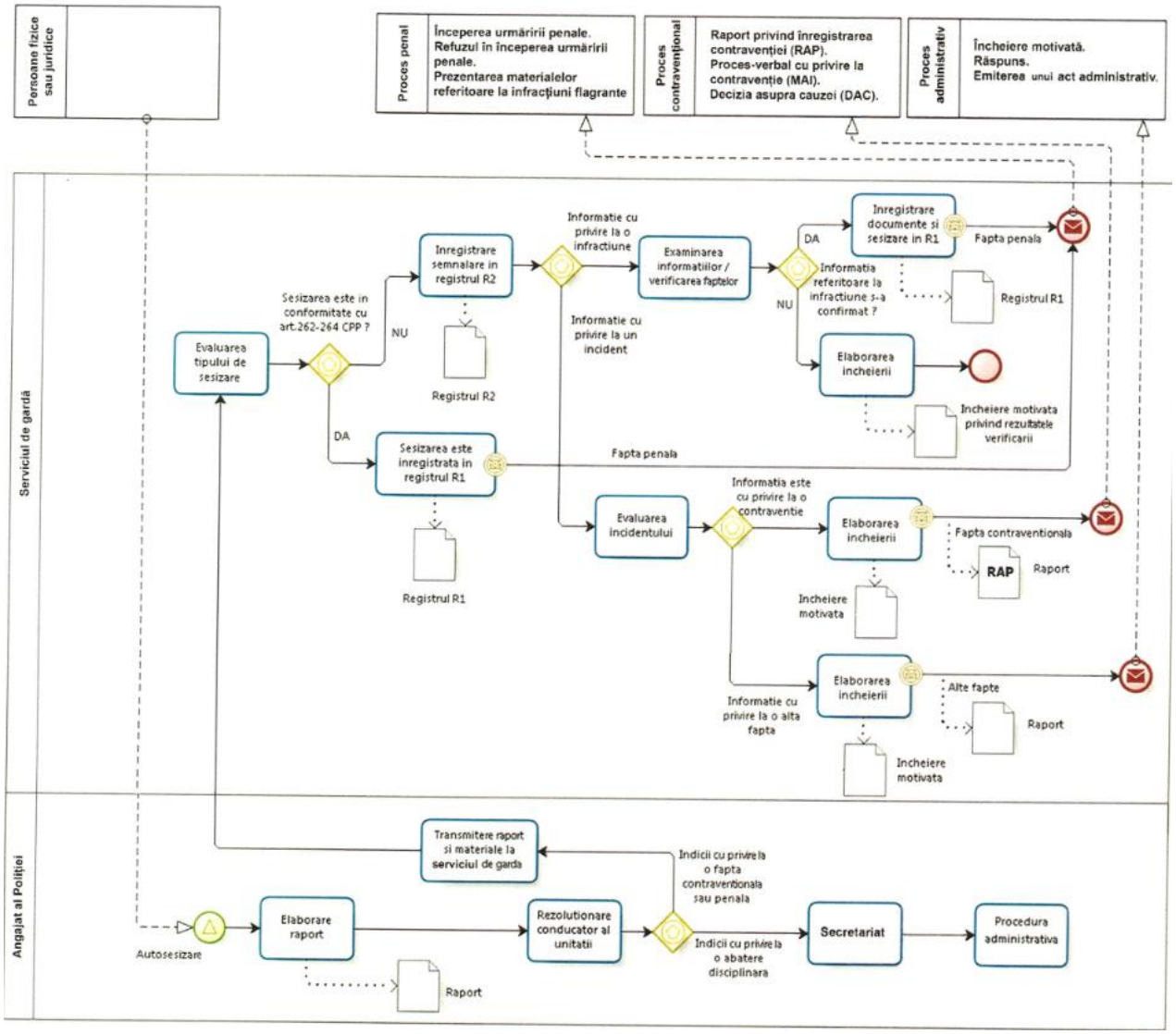
a) information on a possible offence;
b) b) information on an emergency situation.



Flowchart of the process of handling referrals received via telephone.

Self-reporting.

In the case of self-reporting, the police officer who has reported an offence fills in a report (self-report) and sends it to the head of the subdivision to which he/she belongs. The head of the subdivision orders by resolution the investigation and resolution of the case which, in the case of contraventions or criminal offences, is forwarded to the Duty Service for registration and, in the case of disciplinary offences, is registered in the secretariat/chancellery.

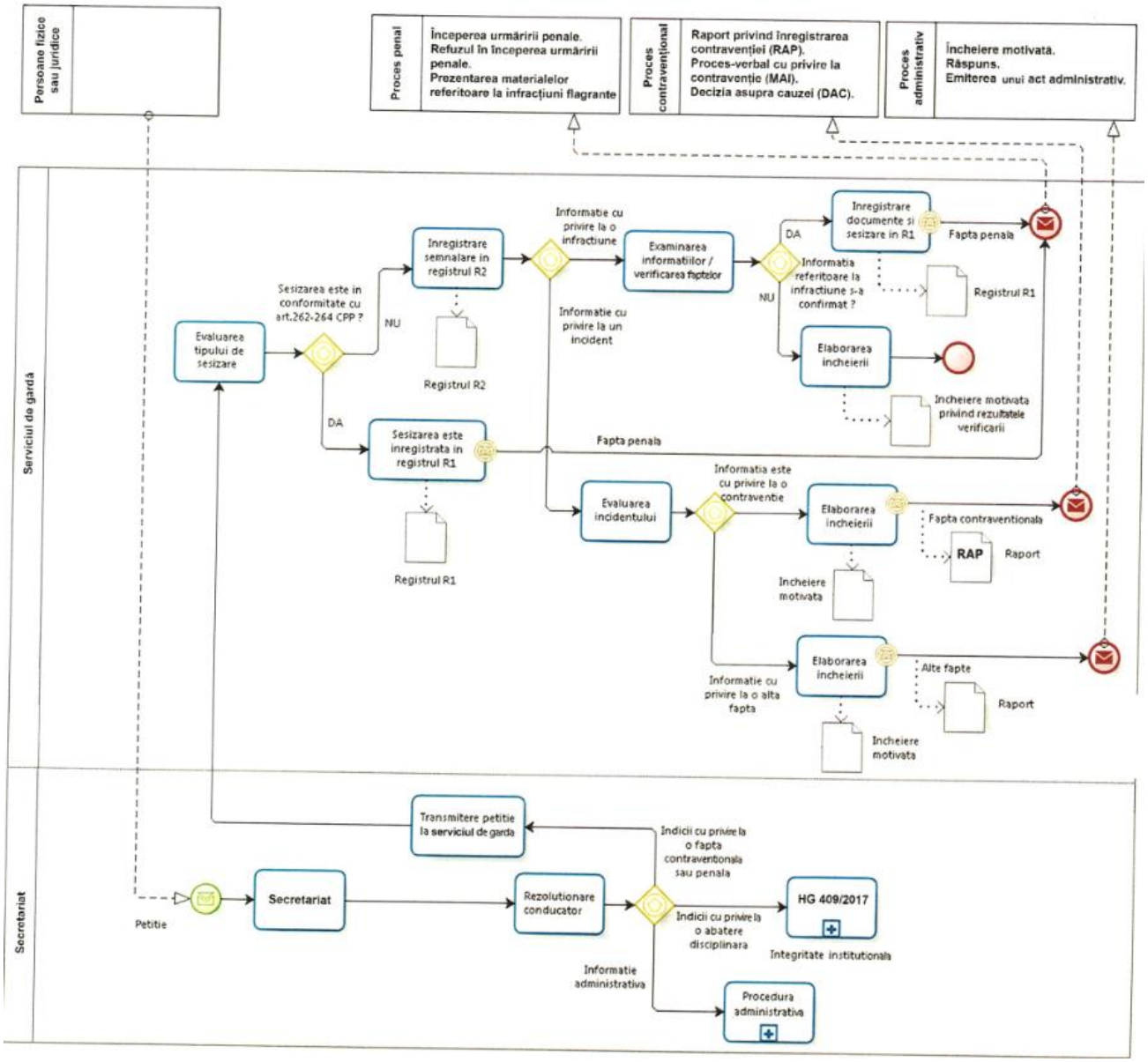


Flowchart of the process of handling self-reports.

Petitions submitted to the Secretariat/Chancellery or petitions received through the Post Office "Poșta Moldovei", Special Courier Office of the Intelligence and Security Service.

Petitions that are submitted to the secretariat/chancellery are registered in the Electronic Document Management Information System and resolved by the head of the institution. In subdivisions where there are no Electronic Document Management Information Systems, they are registered in accordance with Annex No. 2 to the Instruction on keeping the secretariat work related to petitions of natural and legal persons, addressed to state bodies, enterprises, institutions and organizations of the Republic of Moldova, approved by Government Decision No. 208/1995.

If the petition concerns criminal/contravention acts of an administrative nature or signals a disciplinary offence, it will be taken over to the work process corresponding to the type of petition.



Flowchart of the process of handling petitions submitted to the secretariat.

The heads of police subdivisions shall distinguish clearly at the stage of examining the received correspondence, the difference between a petition that is included in the examination process according to the administrative technique, and a referral of a contravention to be registered and examined according to the contravention process.

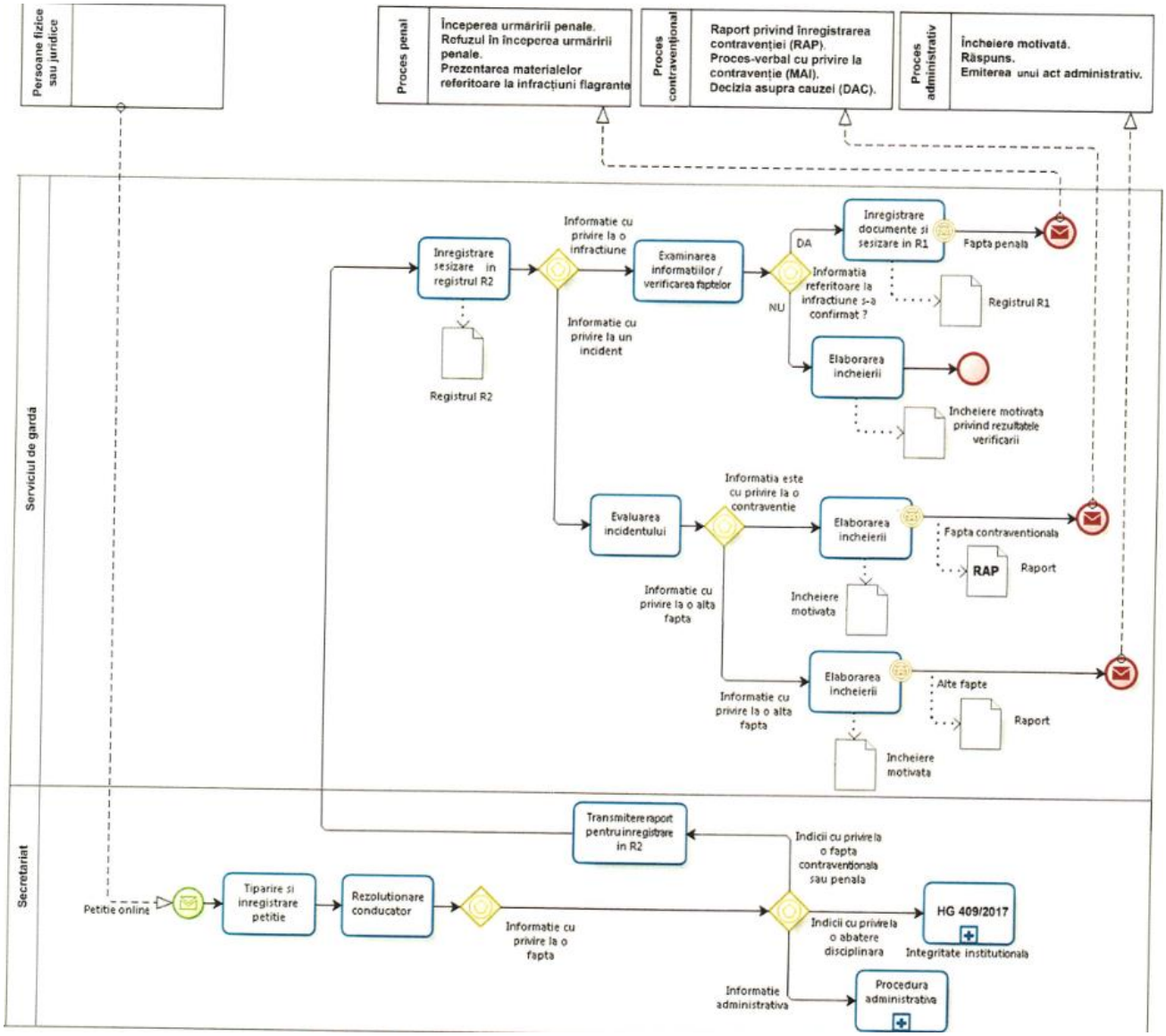
If the petition registered and entrusted for examination under Article 73 of the Administrative Code meets the constituent elements of a contravention, the Police subdivision shall correctly cease its examination initiated under the Administrative Code and transfer it to the order of the Contravention Code, bearing in mind, as a matter of imperative necessity, that the Administrative Code does not apply to the legal relations of the public authority acting under the Contravention Code or the Criminal Code.

Under the conditions described above, the employee authorized to examine the petition shall draw up a reasoned conclusion in accordance with Article 3 1 and Article 118 of the Administrative Code with a proposal to cease examination of the petition in accordance with the Administrative Code and to pass it on

for examination in the order of the Contravention Code (see model conclusion in Annex No. 6 of this procedure).

Petitions submitted in electronic form.

Petitions in electronic form are submitted via specialized web portals or by e-mail and are handled in a similar way to written petitions, the only difference being that petitions in electronic form are printed and then taken to the work process corresponding to the type of referral.



Flowchart of the process of handling petitions submitted online.

Referrals received via the video traffic monitoring system.

In the case of the video traffic monitoring system, the referral is not recorded in Registers No. 1 and No. 2, but is generated "From traffic control - DCT" under which the minutes of the contravention/decision on the contravention case are concluded and recorded in the special register.

Receipt and examination of referrals of offences

Referrals of offences may be submitted to the Duty Service in writing or verbally by any natural or legal person as well as by Police employees. At the request of the Police employees who submitted offence referrals, the Duty Service employee countersigns the copy of the referral and applies the unique registration number.

Referrals on offences received by mail in the subdivision secretariat/chancellery shall be registered in accordance with the rules of registration of incoming mail and immediately reported to the head of the prosecution body, who shall order their registration in Register No. 1.

The official person of the body that received the referral on offences shall study its content, verifying its compliance with the requirements of Article 263 of the CPC.

In the case of a person who has filed a denunciation or complaint, the person shall be informed of the responsibility he/she bears if the denunciation or complaint is intentionally libelous, which shall be recorded in the content of the denunciation or complaint and confirmed by the signature of the person who filed the denunciation or complaint.

Immediately after the procedure of receiving and registering (in Register No. 1) the referral of offences, the employee of the Duty Service informs the head of the criminal prosecution body about the content of the registered referral, requesting its examination according to the criminal procedure law.

Subsequently, the employee of the Duty Service informs the criminal prosecution officer assigned to examine the case of the need to receive the referral of offences for examination, in accordance with the resolution of the head of the criminal prosecution body.

The forwarding for examination of the referral of the offence shall be preceded by notification in Register No 1 of the personal and contact details of the criminal prosecution officer responsible for examining the case with an indication of the time of receipt for examination.

The time limit for the examination of referrals of offences is 30 days. Thus, the head of the criminal prosecution body, by his/her resolution, shall set a minimum time limit for examination but shall not exceed 30 calendar days. Article 274 of the CPC stipulates that the criminal prosecution body, after having received a referral under Articles 262 and 273 of the CPC, shall, within 30 days, issue an order for the initiation of criminal proceedings, or if the referral document contains any of the cases that prevent the initiation of criminal proceedings, it shall submit the materials to the prosecutor with the proposal not to initiate criminal proceedings.

The head of the criminal prosecution body shall ensure compliance with the time limit for examination, which may be extended for a reasoned extension. A report on the extension of the examination period shall be submitted before the expiry of the examination period, giving specific reasons for the impossibility of issuing a decision. The report issued with the resolution of the head of the criminal prosecution body shall be attached to the accumulated materials and a certified copy shall be submitted to the Statistical Service.

The record of offences shall be made by means of the completion by the Criminal Prosecution Body (hereinafter referred to as the CPB) of the record of offences established for each specific type of offence established during the reporting period, irrespective of when the offences were committed and whether the persons who committed them are identified.

The following records are used for the single record of offences, criminal cases, materials relating to offences, persons who have committed offences and for the preparation of statistical reports on the state of crime and the results of the fight against crime (form No 1; No 1.1; No 2.1; No 2.2, No 2.7; No 6.0; form No 1 and No 2).

Primary records, drawn up in the established form, are official statistical records. Responsibility for the correctness and completeness of the completion of the record forms shall be borne by the criminal prosecution officer or, where appropriate, by the head of the CPB. Responsibility for checking the completeness and correctness of the completion of the primary record forms and for entering the information on the record forms into the Information System shall be borne by the Statistical Service.

If the record has not been completed correctly or fully, the Statistical Service employee shall return the record to the employee who filled it in, ensuring that the quality of the record is checked.

The Statistical Service manages the "Register of records of offences, criminal cases, offenders and materials on offences" and issues the number of criminal cases.

The responsibility for issuing copies or presenting for information the materials accumulated from the examination of referrals of offences is assigned to the CPB.

Receipt and examination of other information on offences and incidents

If other information on offences and incidents is received, the employee of the Duty Service who has received it shall immediately record it in Register No 2, indicating the specific facts communicated and subsequently organizing its verification. This information may serve as a basis for: going to the scene, carrying out operative investigative measures, keeping traces and evidence, starting reviews or carrying out other verification actions.

Employees of the Duty Service are obliged to receive and record other information about offences and incidents, even if this information does not fall within the competence of the Police subdivision.

Upon receipt of other information on offences and incidents, the employee of the Duty Service shall make the necessary entries in Register No. 2, as follows: personal and contact details of the complainant, brief description of the case which is the subject of the referral, personal details of the perpetrator, if known, and means of evidence, if applicable.

On the basis of the information that has been reported, the employee of the Duty Service prepares a written information and it is forwarded to the employee or to the Police Department in the territorial area where the action took place.

When information about offences is received by fax, electronic mail or web applications, the employee in charge shall print out the information received, record it in Register No. 2 and forward it for examination in accordance with the established procedure.

Police employees, while performing their duties outside their duty rooms, receiving other information about offences, shall immediately transmit its content to the Duty Service by telephone or other means of connection.

The time limit for examining other information on offences and incidents is 30 days. Thus, the head of the subdivision, by his/her resolution, shall set a minimum time limit for examination but shall not exceed 30 calendar days. At the same time, Article 440(3) of the Contravention Code stipulates that within 15 days from the date of the referral, the investigating officer is obliged to verify the referral and take the necessary measures to establish the existence or non-existence of the contravention.

If further action is required to take a decision on the information recorded in Register No. 2, the employee examining the information before the expiry of the time limit shall submit a written report to the head of the subdivision for an extension of the time limit for examination, and a certified copy shall be submitted to the Statistical Service.

If the representative of the fact-finding body, through special investigative measures and/or through the performed fact-finding acts, or in any other way, immediately detects an offence or finds a reasonable suspicion of a committed offence, he/she shall be guided by the provisions of para. (3) Article 265, para. (2) and (3) art.273 of the CPC, shall draw up the necessary reporting documents and minutes recording the findings, which shall be forwarded to the head of the competent criminal prosecution body within 24 hours at the latest, in order to order the immediate registration of the report in Register No. I and to be dealt with in accordance with art.274 of the CPC.

In case the information registered in Register No. 2 has not been confirmed, the Police employee who examined the information shall submit to the head of the respective subdivision a motivated conclusion on the results of the verification to which the accumulated materials shall be attached.

Concurrently with the submission of the reasoned conclusion on the results of the verification of other information on offences and incidents recorded in Register No. 2, if in the process of their examination sufficient information has been gathered to consider with a high degree of probability that a contravention has been committed, but no sanctioning decision has been issued, the Police employee examining the case shall complete and submit the Contravention Registration Report (CRR) to the head of the subdivision.

The Contravention Registration Report shall also be submitted in the case of receipt through the Police Subdivision's secretariat/chancellery for examination of the contravention case detected or found by other competent authorities.

The responsibility for the release of copies of the file accumulated following the examination of other information on offences and incidents is placed on the enforcement officer, where applicable, the immediate supervisor of the latter.

Recording and registering referrals

Referrals are registered immediately and unconditionally upon receipt.

The employee of the Duty Service shall request the head of the territorial/specialized subdivision of the Police to issue the resolution and apply his/her signature to the information recorded in Registers No. 1 and No. 2.

The head of the criminal prosecution body shall issue the resolution and apply his/her own signature, exclusively, on the referrals concerning offences. The Head of the Police Sub-Division shall issue the resolution and apply his/her own signature only to other information on offences and incidents, as well as information on contraventions.

The right to register referrals in Register No. I and Register No. 2 is vested in the employees of the Duty Service of the territorial/specialized subdivisions. The employees of the Duty Service are responsible for the registration of the referral and for the completeness of the completion of Register No 1 (except for boxes 8, 9, 10) and Register No 2 (except for box 7). The responsibility for the completion of boxes 8, 9, 10 of Register No 1 and box 7 of Register No 2 concerning the entries on the results of the examination of referrals on offences and other information on offences and incidents is placed on the Statistical Service.

The employees of the Duty Services are responsible for entering the primary information (content of the information, actions taken, resources allocated, initial examination deadline, employee assigned to examine the referral) recorded in Register No. I and Register No. 2 into the automated information system "Register of Forensic and Criminological Information" (hereafter Information System).

The Statistical Service employees are responsible for entering into the Information System as well as for making entries in Register No. 2 of the data on examination processes and other information on offences and incidents (extension of examination deadlines, dispatch according to territorial jurisdiction, decisions, etc.).

The data entry into the Information System will be based on authenticated copies of the decisions taken by the Police employees and authenticated copies of the reports on the extension of time limits for the examination of referrals and other information on offences and incidents, which are considered as primary evidence documents.

Item No. 7 of Register No. 2, concerning the results of the information check, shall be filled in, as appropriate, with the series/number of the Contravention Registration Report (CRR), the Minutes of Contravention (MIA) or the Decision on the Contravention Case (DAC).

Police employees examining referrals of offences and other information on offences and incidents are responsible for forwarding to the Statistical Service authenticated copies of reports on extensions of examination deadlines and decisions taken with details of the location of the accumulated material by 4 p.m. on the working day.

Procedure for the archiving referrals of offences

The criminal prosecution officer who issued the proposal for refusal to start prosecution on the day the proposal was issued will send the report with the accumulated materials through the secretariat/chancellery to the territorial prosecutor's office.

A copy of the accompanying file shall be submitted for storage to the Statistical Service, which shall make the necessary entries in box 9 of Register No. 1.

The Territorial Public Prosecutor's Office shall register the arrival of the report and the materials mentioned in the registry and within a reasonable period of time, ensured by the head of the Public Prosecutor's Office by setting fixed deadlines, shall order:

- the refusal to initiate criminal proceedings;
- the initiation of criminal proceedings by the criminal prosecution body;
- the commencement of criminal proceedings.

After issuing the order refusing to initiate criminal proceedings, the prosecutor will send to the criminal prosecution body, via the secretariat/chancellery, the materials and the order issued in two copies.

The Statistical Service shall record the materials refusing to initiate criminal proceedings in the Register of materials refusing to initiate criminal proceedings (item no. 6) and shall assign a serial number.

The Register of materials refusing to initiate criminal proceedings must be numbered, stitched, sealed and kept in the records as a nomenclature file. After the end of the reporting period (annually) it is sent to the secretariat/chancellery for storage.

Simultaneously with the registration of the material of refusal to initiate criminal proceedings, the employee of the Statistical Service shall enter the date of the decision not to initiate criminal proceedings and the serial number assigned in the relevant section of Register No. I.

A copy of the prosecutor's order shall be kept in the records subdivision, and the material of refusal to initiate criminal proceedings, after its registration, within 24 hours shall be forwarded to the head of the criminal prosecution body against signature in the register of materials of refusal to initiate criminal proceedings.

Procedure for archiving other information on offences and incidents

Registers No I and No 2 must be numbered, stitched, sealed and kept in evidence as nomenclature files. After the end of the reporting period (annually) they shall be forwarded to the subdivision's secretariat/chancellery

for storage. The retention period shall be determined in accordance with the departmental regulations in force for the retention of nomenclature files.

The secretariat/chancellery shall be responsible for keeping and archiving accumulated material following the examination of other information on offences and incidents, with the exception of contravention files.

The Statistical Service is responsible for keeping and archiving material accumulated as a result of examining contravention cases.

All material from the examination of other information on offences and incidents with the conclusion approved by the head of the subdivision shall be sent for storage in the special nomenclature file, with the assignment of a record number.

Annex A2
Contravention case management: ToBe workflow

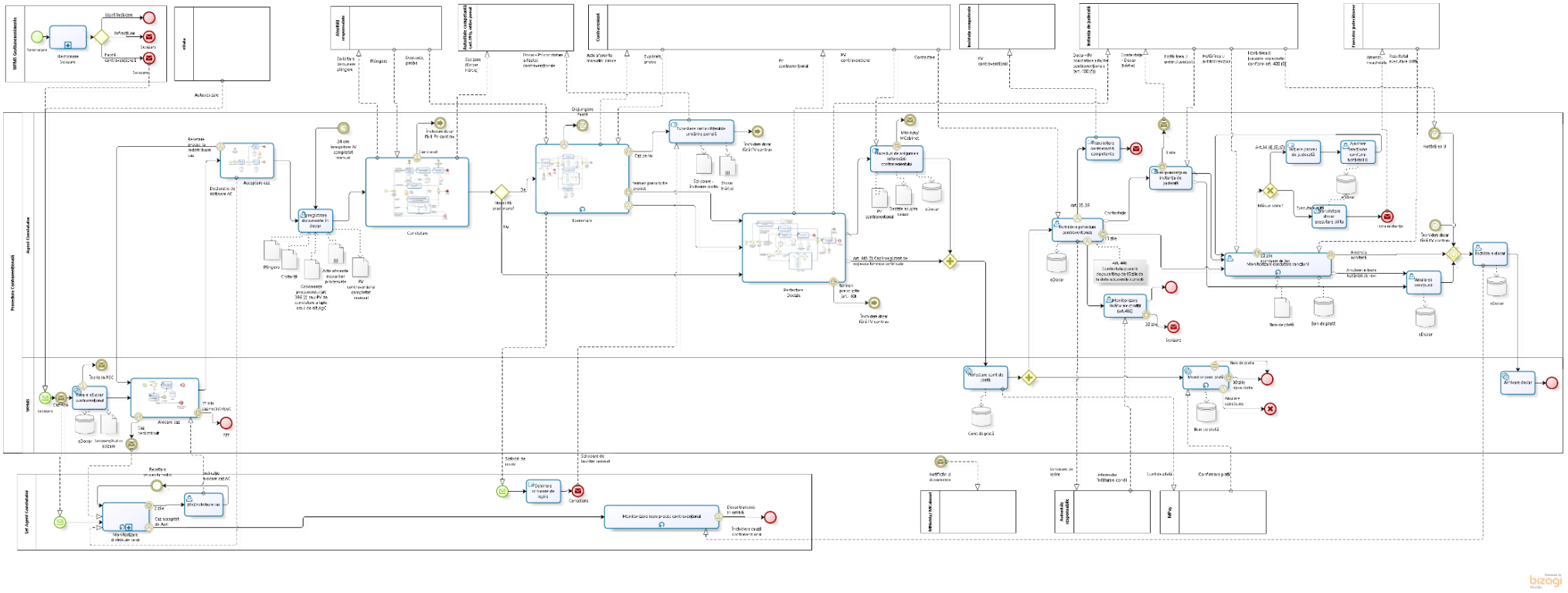
Workflow diagram

The process of contravention case management and related activities is regulated by the Contravention Code of the Republic of Moldova (CC) - Law No. 218 of 24.10.2008 and a number of internal concurrent instructions;

The process of management of contravention cases and related activities aims at:

1. receiving, registering, recording and examining referrals of contraventions;
2. registering and recording contravention cases and the results of their examination;
3. registering and recording persons who have committed contraventions;
4. keeping records of the contravention process, from its initiation through the referral or self-reporting until its completion.

The flowchart of the processes carried out according to the BPMN standard is presented below, at the level of actions and sub-processes:



Flowchart of the contravention process

According to the Future ICT Architecture of the MIA, the "Contravention Procedure" process within the WFMS is initiated when there is a legal qualification or a reasonable suspicion that a violation has been committed.

According to Article 374 (2) The contravention process is the activity carried out by the competent authority, with the participation of the parties and other persons entitled to rights and obligations, with the purpose of establishing the contravention, examining and resolving the contravention case, establishing the causes and conditions that contributed to the commission of the contravention.

In practical terms, the "Contravention procedure" process is initiated by the "Event management" process, which delivers the "referral" to the first. The detailed flowchart of the "Event management" process is represented in another document, dedicated to this process. A number of 5 sub-processes have been identified for the contravention procedure, as follows:

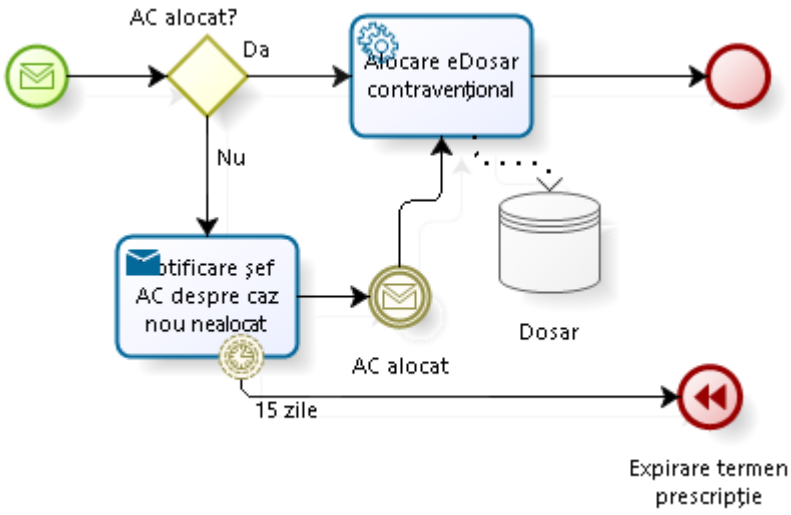
4. The sub-process "Case allocation";
5. The sub-process "Case Acceptance";
6. The sub-process " Finding ";
7. The sub-process "Examination";
8. The sub-process "Decision making";

In addition to the basic process " Contravention procedure ", the management of the contravention case is assisted by 3 auxiliary processes:

9. The process of case monitoring, carried out by the chief of the reporting officer;
10. The process of signing the accompanying letters;
11. The process of management of payment bills and payment monitoring performed by the billing system of the MIA e-Services system.

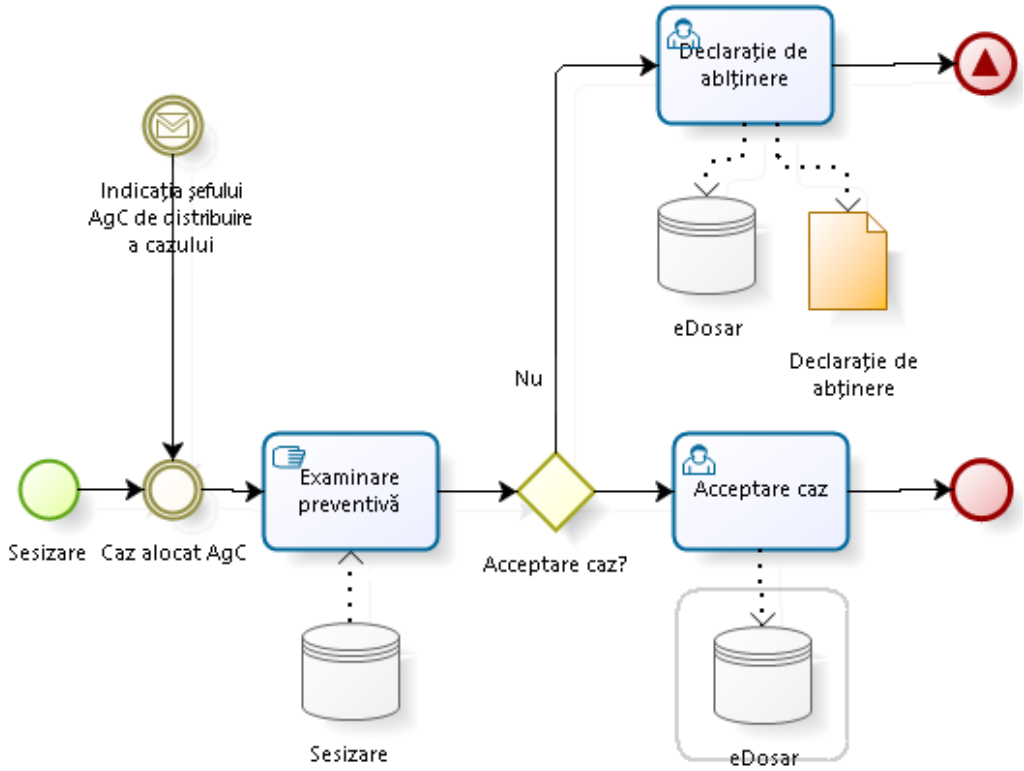
The following are the BPMN diagrams for the 5 sub-processes of the mentioned "Contravention procedure" process:

Sub-process "Case allocation"



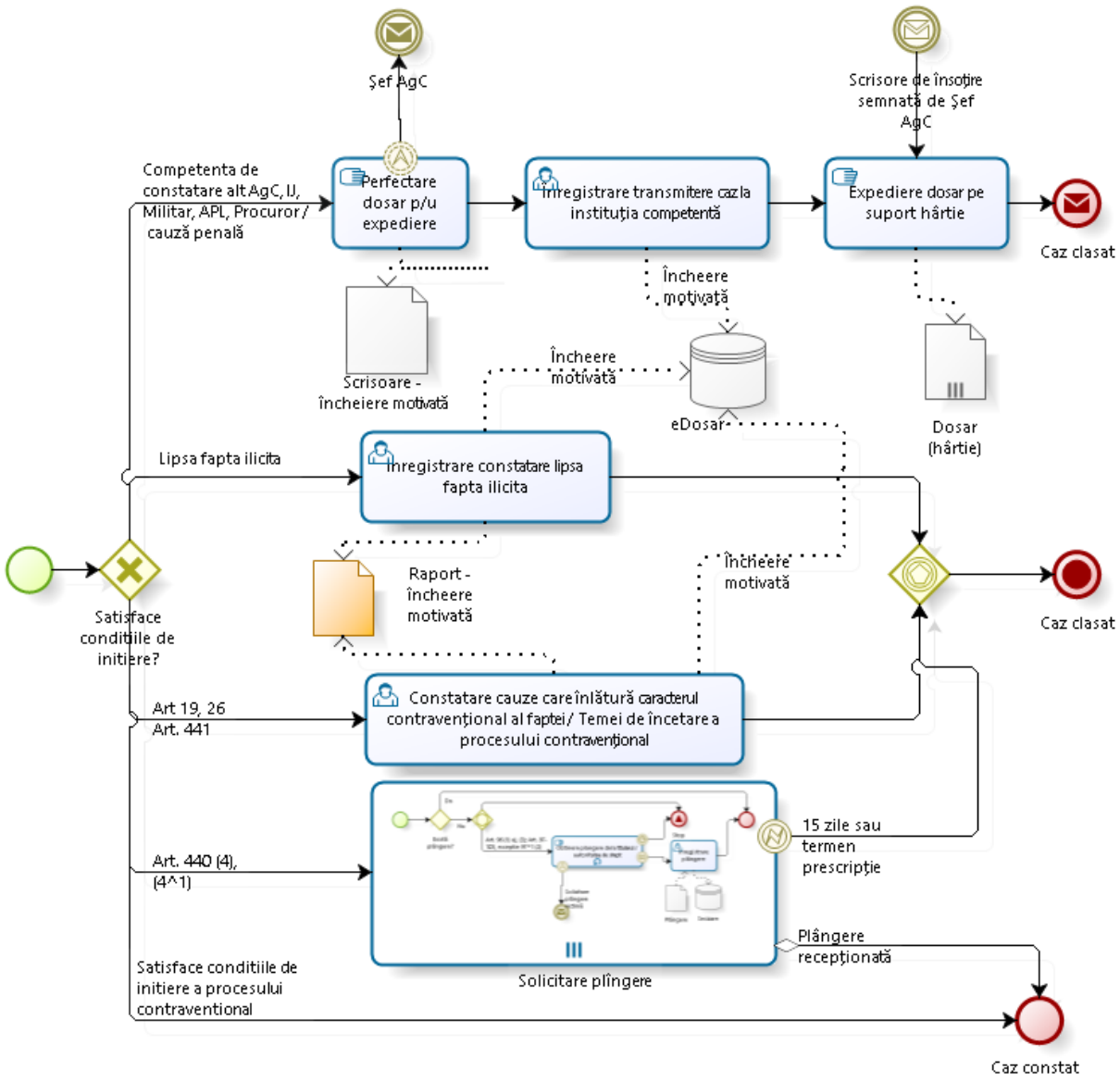
The WFMS computer system will check if the received referral is already assigned to a reporting officer (RO). If the referral has not been assigned, the system will notify the chief of the RO about the fact and will wait for the assignment of the case to a RO.

Sub-process “Case Acceptance”



After receiving the referral, the RO examines the case and, if there are no good reasons to reject the case, he/she accepts it and the status of the referral is recorded in the system. If there are reasonable grounds for refusal, the RO refuses the referral and issues a report.

Sub-process “Finding”

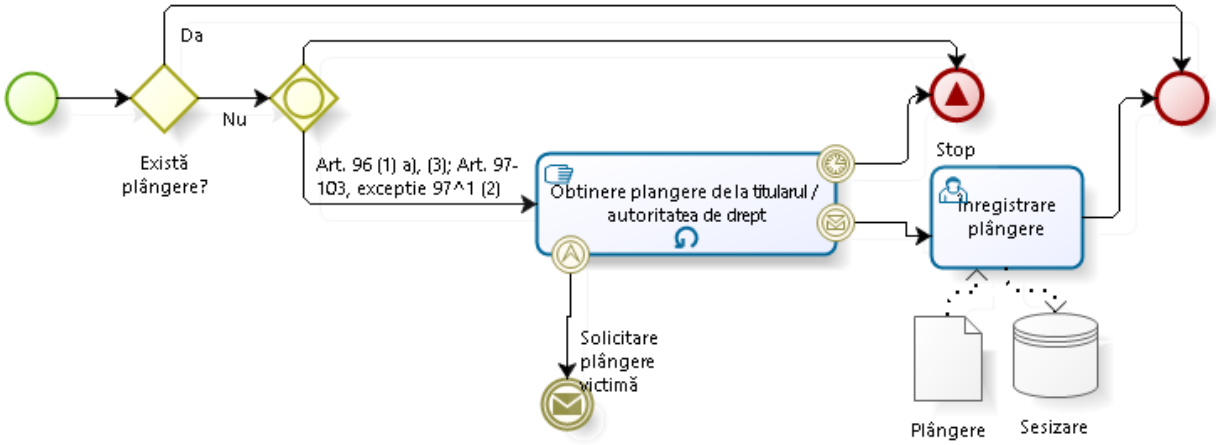


After the acceptance of the referral, the process proceeds with a decision point ("gateway"). At this point, the following situations are checked:

12. Is there an illegal act?
13. Does someone else have the power to establish the fact (another RO, prosecutor, etc.)?
14. Are there any grounds for dismissing the contravention?
15. Is it necessary to request a complaint?
16. Are all the conditions for initiating the contravention proceedings met?

If the RO does not have the competence to establish the fact, he/she completes the file, registers the transmission of the case to the competent authority and sends the file.

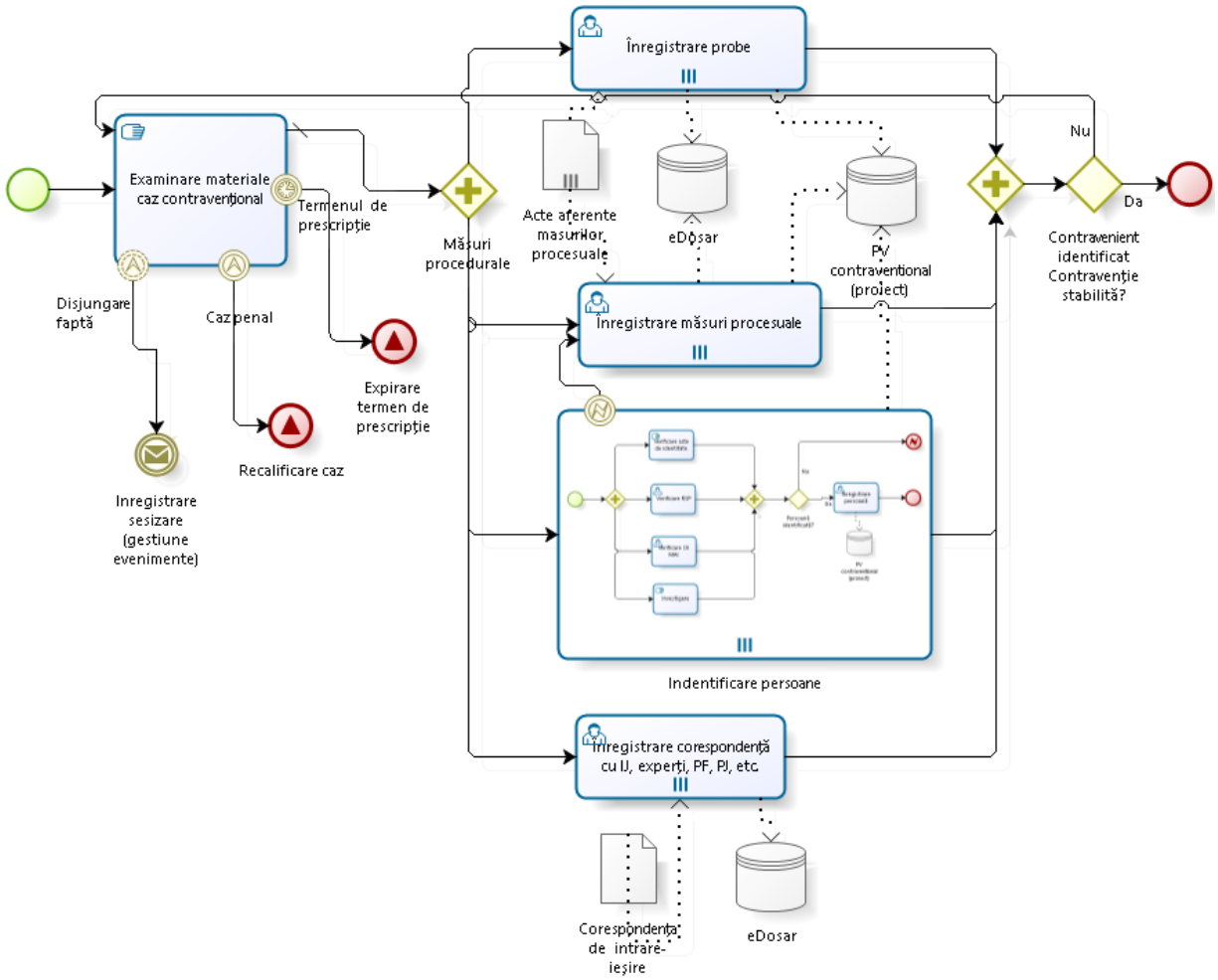
If there is no complaint and it is necessary to request a complaint, another sub-process is modelled within the sub-process " Finding ", i.e. " Complaint request ", which is represented in the following diagram:



This sub-process includes: obtaining the complaint (from the right holder/authority) and registering the complaint in the computer system, after obtaining it in written form. A scanned copy of the complaint is uploaded into the system.

If the conditions for initiating the contravention procedure are met, the RO establishes the fact.

Sub-process "Examination"



In this sub-proceeding, the RO reviews the materials relevant to the contravention case. If necessary, the RO takes procedural steps and records these steps in the computer system together with the evidence obtained.

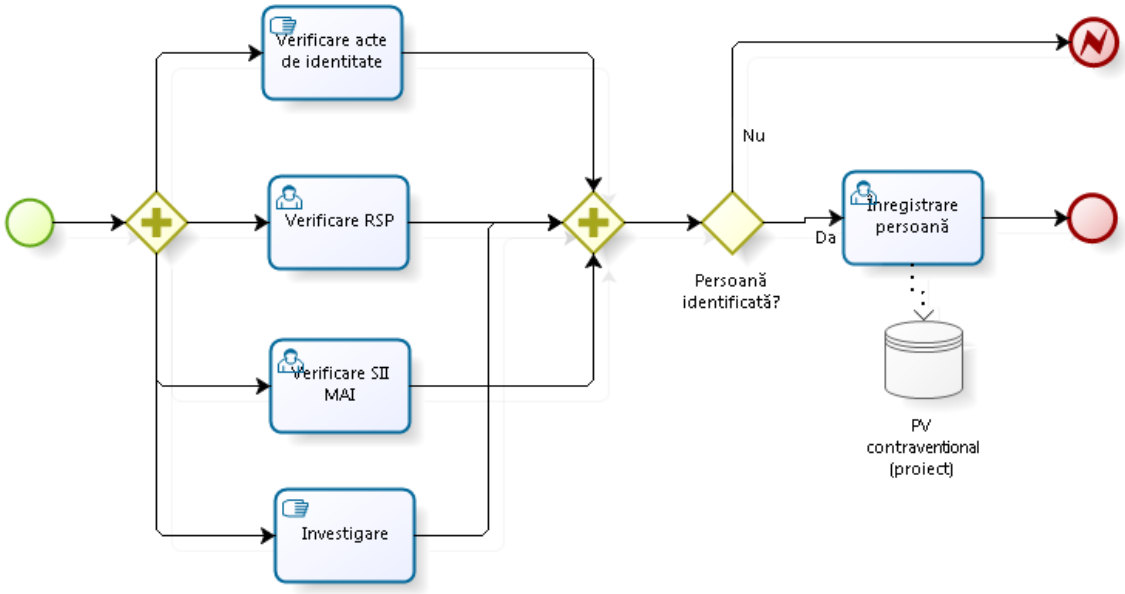
The procedural documents (acts) result from specific procedural actions that are carried out within the sub-process "Examination" and that are not modelled in the sub-process diagram. These actions are shown in the following table:

No.	Procedural action	Procedural document
1	Collection of object and documents	Order to remove objects and documents Decision of the court to remove documents containing information constituting a secret Minutes of removal of objects and documents Order of handing over for preservation Minutes of removal of registration plates Minutes of retention and bringing the vehicle to the special parking are
2	Witness hearing	Minutes of hearing the witness
3	Hearing the offender	Minutes of hearing the offender Explanations of the person in respect of whom the contravention proceedings have been initiated
4	Attachment of corpus delicti to the case	Ordinance on the attachment of corpus delicti
5	On-site investigation	Minutes of on-site investigation Minutes of technical inspection of the vehicle Sketch of the road accident
6	Home search	Authorization of the court of first instance to search the domicile Order to search the domicile (reasoned decision of the reporting officer on the search of the domicile)
7	Body search	Minutes of the body search
8	Retaining	Minutes on the person's retention
9	Expertise and findings	Evidence of technical breakdown of vehicles in road accidents

Procedural documents are entered into the WFMS computer system through the actions shown in the previous BPMN diagram, i.e. "Record procedural measures" and "Record evidence".

Procedural actions may differ from one contravention case to another. Within the WFMS the procedural actions will be selected from a defined list. At the end of the procedural action the computer system will allow the user to attach the procedural documents specific to each procedural action, in electronic format (scanned copy of the document) with the specification of the attribute "document type" which will be selected from the filtered list of document types. The actions and procedural documents presented in the above table are not limitative, the IT system must allow the deletion from the list or the addition to the list of actions and procedural documents, as appropriate.

Within the sub-process "Examination" there is another sub-process defined, namely: "Identification of persons", which is represented in the following diagram:

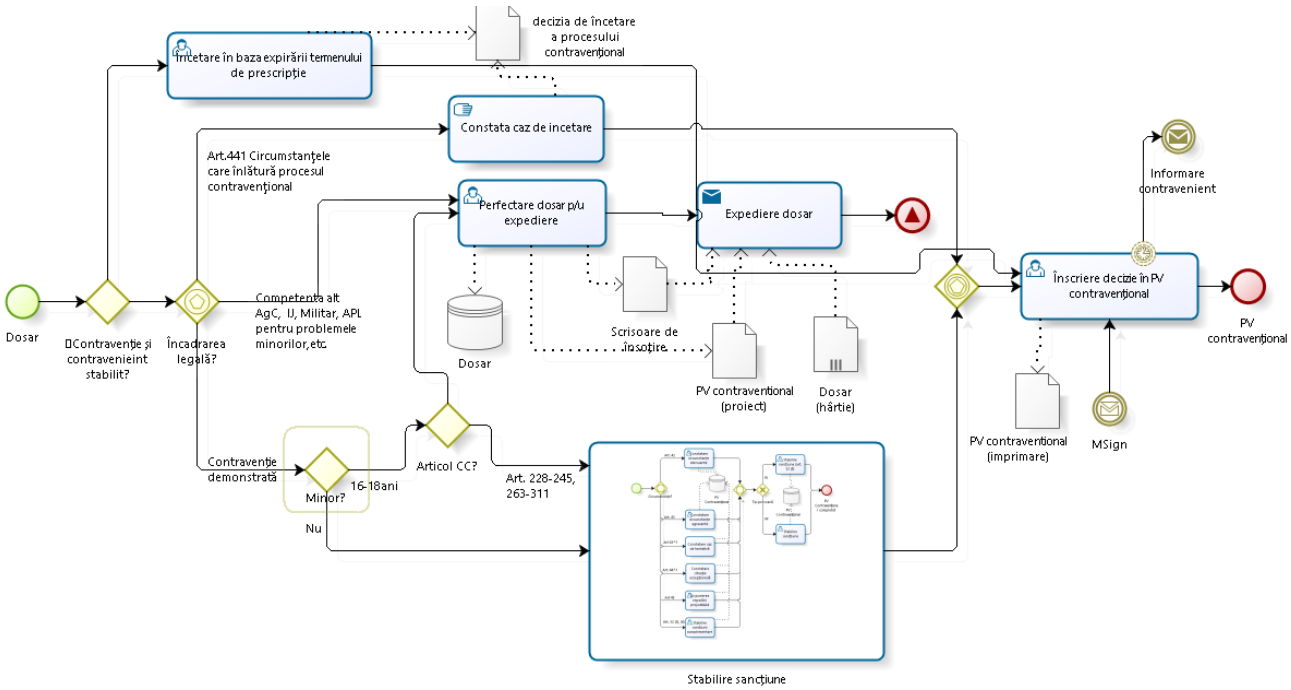


Within this sub-process, the RO carries out in parallel, as appropriate, several specific verification and investigation actions in order to identify the person. If the person is identified, the information about him/her is recorded in the database of the IT system.

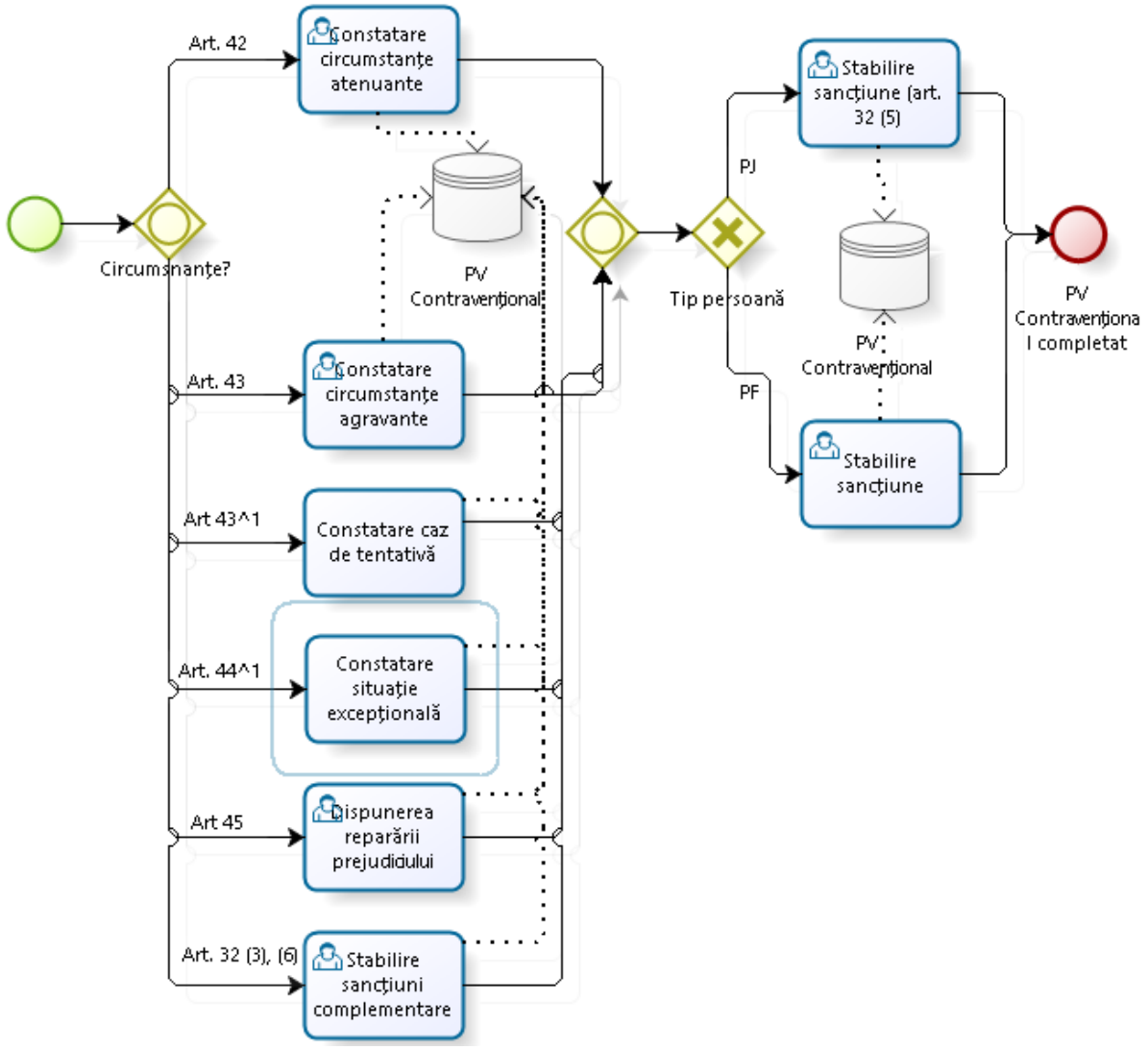
Sub-process "Decision making"

Once the contravention and the offender have been established, the RO makes the legal classification of the offence. If circumstances are identified that remove the contravention process, the RO establishes the termination of the case. If the competence for the decision lies with another RO or another institution, the file is completed and sent to the competent body for decision.

If the RO has competence to take the decision, he/she determines the sanction. Once the sanction has been determined, the RO enters the decision in the contravention minutes.



Within the sub-process "Concluding the contravention minutes (Decision)" there is another sub-process defined, namely: "Establish sanction", which is represented in the following diagram:



In the framework of this sub-process, the RO may conduct, in parallel, as appropriate, actions to establish mitigating or aggravating circumstances, may order reparation of the damage or establish complementary sanctions. Depending on the type of person (natural or legal), the RO determines the sanction and records the information in the WFMS database.

Description of workflow elements

Description of the elements of the business process "Management of contravention cases"

Element	Description
Roles and work areas	
WFMS Event Management	The area of operational work processes related to " Signals to police and event management" The description of these processes will be presented in a separate document.

Contravention procedure	Operational work process area related to the management of contravention cases.
WFMS	Lane of activities carried out by the WFMS
Chief of Reporting Officer	Lane of the activities carried out by the role of Chief of Reporting Officer
Reporting Officer	Lane of the activities carried out by the role of the Reporting Officer
Victim / Responsible authorities	Lane of the activities carried out by the victim role (Art. 387) or the rights holder or the authority empowered under the Law on the Protection of Geographical Indications, Designations of Origin and Guaranteed Traditional Specialties (art. 440 (4^1))
Offender (or Suspect)	Lane of the activities carried out by the role Offender/Perpetrator (Person in respect of whom proceedings have been brought under Article 384 (1))
Responsible authorities	Lane of the activities carried out by the Responsible Authority role under Article 450 (1).
Bailiff	Lane of the activities carried out by the role of Bailiff in accordance with Law No. 113 of 17.06.2010. In the examined processes is responsible for the enforcement of fines.
MPay	Lane of activities carried out by the MPay System role
Court	Lane of the activities carried out by the role of the Court
Competent authority (art.393), criminal officer	Lane of the activities carried out by the role of the Competent Authorities to deal with contravention cases under Article 393. In the examined processes the role is used in case of referral of the case according to the competence (art. 399 (2)).
Process elements	
Referral	The element for initiating the process "Contravention procedure". The procedure starts when a 'referral' message is received from the 'Event Handling' process According to Article 440. The process of establishing the contravention and the powers of the reporting officer, (2) The reporting officer shall be notified by complaint or denunciation or referred ex officio when it is discovered that an unlawful act has been committed or when such an act has been detected as a result of control in accordance with his/her official duties and in cases prescribed by law.
Info new case	Informing the Chief of the Reporting Officer of the arrival of a new referral. The information is intended to start the process of monitoring the distribution of the referral.
	Concatenation of workflows
Case assignment	Sub-process of distribution of the new contravention case. Within the sub-process the WFMS information system will check if the received referral is already assigned to a reporting agent (RO). If the referral has not been assigned, the system will check which is the territorial and institutional competence, based on specific nomenclatures predefined in the

	system. After that, the computer system will check in the human resources database of the MIA which agents are available, so that the referral can be assigned. The referral will be assigned to a RO and this will be recorded in the system as a status attribute for the received referral
 Case acceptance	Sub-process for accepting the new contravention case. After receiving the referral, the RO reviews the case and, if there are no good reasons to reject the case, it accepts it, with the status of the referral being recorded in the system. If there are reasonable grounds for refusal, the RO refuses to assign the referral and draws up a report.
 Recording documents in case file	Activity undertaken by the user to record documents in the electronic file. Associated elements: 1. Entry document “Complaint” 2. Entry document “Receipt” 3. Entry document “Prosecutor’s Order (art. 396 (2)(3) or Minutes of the contravention issued by another RO” 4. Entry documents “Procedural documents”
 Need to complete the minutes (Art. 446)	Decision-making element on the need to complete the contravention minutes under art. 446. Determines the continuity of the process according to the decision: 5. Yes – go to “Closure of the case without contravention minutes” element 6. No – go to “Pre-completion of the contravention minutes” activity
 Closure of the case without the contravention minutes	Skip to the stage of closing the case without contravention minutes.
 Pre-completion of the contravention minutes	Automated activity performed by WFMS on the pre-filling the contravention minutes according to predefined scenarios (Business role). The pre-filling of the minutes is to be performed according to the event/fact data received from the "event handling" process and attached documents. In the case of automated systems (e.g. Road Traffic Video Monitoring System) the information related to the legal framing can be received attached to the event/fact. Associated elements: 7. Electronic case - the pre-completed minutes in digital format are entered into the electronic case file of the administrative offence.
 Saving the contravention minutes	Activity carried out by the Reporting Officer by: 8. completing, saving and printing the contravention minutes or 9. entering the minutes of the offence manually. The completion/entry of the minutes is done on the basis of the document pre-filled by WFMS in the WFMS user interface. The control of the manually filled in report is ensured for 24 hours according to art. 442 (2).

	Associated elements: 10. Output document - draft of the contravention minutes (without decision part).
 Needs examination?	Decision-making block on the need for further work to examine the contravention case. Depending on the decision, move on to the next activity: 11. Yes – move to “Examination” sub-process 12. No – move to ”Concluding the contravention minutes (Decision)” sub-process
 Examination	Contravention examination sub-process In this sub-process, the RO examines the material relevant to the contravention case. If necessary, the RO takes procedural steps and records these steps in the computer system, together with the evidence obtained. The sub-process indicates activities carried out in the cycle. The carrying out of activities within the sub-process of the examination of the contravention can condition the conduct of the business process in the following 3 ways: 13.  Identification of an offence (art. 449 (1)). 14.  Completion of the examination sub-process 15.  Expiry of the limitation period (art. 30) The sub-process may generate a further escalation in the event of another offence being identified during the examination. The new infringement is recorded in the event handling system and a new contravention process is initiated. This escalation does not lead to the termination of the examination sub-process.
 Criminal case	Escalation event generated by the procedure for examining the contravention case. It occurs when it is established that the act considered to be a contravention was committed in circumstances that place it under criminal law (art. 449 (1)). It results in the initiation of the activity of forwarding the file to the public prosecutor or the criminal prosecution officer.
 Sending the case to the criminal prosecution office	Manual activity of sending the file to the prosecutor/criminal prosecution officer according to competence (art. 449 (1)). Sending the case file leads to the closure of the contravention case without the completion of the contravention minutes. The case is closed by skipping to the stage of closing the file without contravention minutes (element  Closure of the case without contravention minutes). Associated elements: 16. Output document – Accompanying letter 17. Output document – File in letter form 18. Motivated conclusion

	The intermediate element placed on the sub-process "Examination" signifies the exit from the sub-process by the completion of the examination activities. The completion of the sub-process ensures the transition to the sub-process "Concluding the contravention minutes (Decision)"
 Expiry of the limitation period	The intermediate element placed on the sub-process "Examination" signifies the completion of activities after the allocated time has expired. The system sets the limitation period in accordance with Art. 30 (2) unless an article providing for another limitation period is specified in the draft minutes on the offence. Completion of the sub-process by the expiry of the limitation period ensures the transition to the sub-process “Concluding the contravention minutes (Decision)”
 Concluding the contravention minutes (Decision)”	Sub-process of formulating and recording the decision in the contravention minutes. After establishing the contravention and the person who committed it, the RO makes the legal classification of the offence. If circumstances are identified that remove the contravention process, the RO establishes the termination of the case. If the competence for the decision lies with another RO or another institution, the file is completed and sent to the competent body for decision. The sub-process is completed in 4 ways: 19. Implicitly, if the contravention is established and the offender is identified, by moving on to the activity "Procedures for ensuring that the offender is informed” (art. 384 (2), art. 443(11)); 20. If the contravention is recorded using technical means certified according to Art. 443 (8), by moving to the activity "Concluding the payment bill”; 21.  Expiry of the limitation period (Art. 30), by moving to Closure of the case without minutes. 22. Sending the case to court (art. 443 (12)).
 Procedures for ensuring that the offender is informed	Manual activity to inform the offender of the sanction decision taken. In the absence of the offender the activity will be carried out according to art. 443 (6) or art. 382 (6). Associated elements: 23. Entry document – signed contravention minutes.
	Parallel flow merging element. The manual activity “Procedures for ensuring that the offender is informed” can also be carried out under the conditions of art. 443 (8).
 Concluding the payment bill	Automatic activity performed by WFMS on concluding the payment bill. The completion of this activity leads to the launch of two parallel flows towards: 24. Activity “Closure of the contravention procedure” 25. Activity “Payment monitoring”

	The activity has associated data object "Payment bill" where it saves the information in digital format.
Closure of the contravention procedure	Activity performed through the user interface to close the contravention process. The activity can be completed in 2 ways: 26. Receiving an appeal (art. 448) 27. Expiry of the 15-day period within which an appeal can be lodged. Additionally, the activity, without interruption, provides for: 28. a dialogue with the authority responsible for favoring the causes leading to the violation (art. 450). 29. a flow to the activity "Monitoring removal of conditions (art.450)" 30. Transmission of the decision to the competent bodies (art. 35-40)
Sending the decision to the competent bodies	Manual activity providing for the transmission of the decision of the RO to the bodies competent to apply the sanction according to art. 35-40. The transmission of the decision leads to the completion of the activity and the given branch of the process.
Monitoring removal of conditions (art.450)	Monitoring the removal of the conditions that fostered the violation is a system-assisted activity that is completed in two ways: 31. Upon receipt of information from the responsible person on the removal of the listed conditions (art.450 (3)) 32. On expiry of the 30-day period, if the information has not been submitted, the RO initiates a contravention case against the responsible person by means of a self-report. In both cases the given branch of the process is closed.
Correspondence with the court	Manual activity that intervenes in the case of an appeal against the decision of the RO (art. 448). The activity provides for dialogue with the court and participation in the trial process. The appeal and the case file are sent within 3 days from the date of lodging the appeal. All appeal procedures, trial in higher courts are carried out within the given activity. The activity can be completed in 2 ways upon receipt of the court's decision: 33. Cancellation of the sanction 34. Maintaining the sanction.
Monitoring sanction enforcement	System-assisted repetitive activity. The activity runs until: 35. Receiving information about the payment of the fine; 36. Cancellation/modification of the sanction as a result of the court's decision on its review. If the fine is not paid within 30 days from the date of informing the offender about the sanction, enforcement measures are applied (art. 34 (4), (5), (7), (8)).

Forced measures	Logical decision by which the RO takes the decision on how to sanction the offender who has not paid the fine for 30 days (art. 34 (4), (5), (7), (8)). The decision can be: 37. Forwarding the request to the court for the sanction to be increased or additional sanctions to be imposed 38. Forwarding the request to the Bailiff for forced execution (Law No 113 of 17.06.2010)
Initiation of court trial	Manual activity undertaken by the RO according to Art. 34 (4), (5), (7), (8) for the purpose of increasing the sanction for failure to pay the fine within the set time limit.
Initiation of court proceedings	The activity includes entering the new sanction in the electronic case file as determined by the court. The adjustment of the sanction leads to the resetting of the deadline for monitoring its payment (return to the activity " Monitoring sanction enforcement").
Forwarding case to forced enforcement	The system-assisted activity provides for sending the information about the outstanding fine payment to the Bailiff for forced execution. Interaction with the Bailiffs is done digitally. The fact of transmission is recorded in the electronic file of the contravention case.
Cancellation of sanctions	The activity of cancelling the sanction may occur as a result of the court's decision following an appeal or review. The cancellation of the sanction is recorded in the electronic file of the contravention case.
Closure of the case	Activity carried out by the Reporting Officer through the system. The activity leads to the initiation of the procedure for archiving the electronic file of the contravention case. The activity occurs as a result of: 39. Receipt of the court's judgment on the cases sent under Art. 400 (5), (6), for taking the decision on the sanction. 40. Closure of the case without concluding the contravention minutes; 41. Cancellation of the sanction. Closure of the case file signals this fact to the "Monitoring the progress of the contravention process" activity carried out by the Chief of the Reporting Officer.
Archiving the case	Automated archiving of data from the electronic file of the contravention case.
	The event to complete the contravention process
Flows	
Referral	Flow between the "Event handling" process and the "Contravention procedure" process. The flow determines the initiation of the contravention process.

Info new case	Flow between the WFMS lane and the "Chief of the Reporting Officer" lane. Starts the process for monitoring the contravention case by the Chief Reporting Officer.
Indication of case allocation to RO	Flow initiated by the action "Case reassignment" (lane "Chief of the Reporting Officer") and the sub-process "Case acceptance" performed by the RO. Aims at reassigning the case if the case has remained unaccepted for 3 days (Art. 440 (3)) by the Reporting Officer.
Complaint lodging request	Complaint request Flow initiated in the sub-process " Case acceptance " to the lane "Victim/Responsible Authority". The flow is initiated according to Article 440 (4) și (4^1).
Complaint	Flow between the "Victim/Responsible Authority" lane and the "Case Acceptance" sub-process carried out by the Reporting Officer. The flow ensures the acceptance of the complaint in cases under art. 440 (4) and (4^1).
Referral (Paper file)	Flow initiated by the sub-process " Case acceptance" ("Reporting Officer" lane) to the lane " Competent authority (art.393), criminal prosecution officer" The flow determines the transmission of the case according to competence to other Reporting Officers, Court, LPA, Prosecutor, Criminal prosecution officer, etc.
Accompanying letter for sending the case	Flow initiated within the sub-process "Case acceptance" (" Reporting Officer" lane) and the "Chief of the Reporting Officer" lane concerning the signature of the accompanying letter in case of sending the contravention case according to competence.
Signed accompanying letter	Flow initiated by the activity "Signing outgoing letters" ("Reporting Officer" lane) addressed to the sub-process "Case acceptance" regarding the return of the signed accompanying letter in the case of dispatch of the contravention case according to competence.
Statements, evidence	Flow from the "Victim/Responsible Authority" lane to the "Examination" sub-process (" Reporting Officer" lane) regarding statements and evidence communicated by the victim or responsible authority.
Proceedings related documents	Flow initiated within the sub-process "Examination" (lane " Reporting officer") to the lane "Offender" on the application of various procedural measures against him/her.
Explanations, evidence	Flow from the lane "Offender" to the sub-process "Examination" (lane " Reporting Officer") concerning statements and evidence communicated by the former.
Outgoing letter (for signature)	Flow initiated within the sub-process "Examination" (lane " Reporting Officer") and lane " Chief of the Reporting Officer" concerning the signature of the outgoing letter in case of sending the contravention case according competence.
Signed accompanying letter	Flow initiated by the activity "Sign outgoing letters" (" Reporting Officer" lane) addressed to the activity " Send case to the criminal prosecution officer" concerning the return of the signed accompanying letter in case of sending the contravention case according to competence.

Case + Contravention Minutes	Minutes Flow initiated within the activity " Send case to criminal prosecution officer" (lane " Reporting Officer") to lane " Competent authority (art.393), criminal prosecution officer”
Contravention minutes	Flow initiated within the sub-process "Concluding contravention minutes (Decision) (lane " Reporting Officer") to lane "Offender" in order to inform the offender of the decision on the contravention.
Case + Contravention minutes (art. 400 (5), (6))	Flow initiated in the sub-process "Concluding the contravention minutes (Decision) (lane " Reporting Officer") to the lane "Court" in order to send the contravention cases found according to art. 400 (5), (6) for decision
Court decision (cases sent according to art. 400 (5), (6))	Flow from the "Court" lane to the activity "Closure of case" (lane " Reporting officer") for the decision taken on the contravention facts, established by the MIA, falling under the jurisdiction of the Court (art. 400 (5), (6). The flow is taken over by the system through the intermediate event "Court decision”.
Contravention minutes (signed)	Flow from the "Offender" lane to the activity "Procedures for ensuring the offender is informed" (" Reporting Officer" lane) which means that the contravention minutes is brought to the attention of the offender according to art. 443 (5).
Payment bill	Flow initiated from the activity "Concluding the payment bill" ("WFMS" lane) to the "MPay" lane. The flow contains the information needed to initiate the payment bill for paying the fine in the MPay system. The flow is automatic.
Payment confirmation	Flow from the "MPay" lane to the "Payment Monitoring" activity (lane "WFMS"). The flow transmits the information on the payment of the fine made by the offender (Payment slip).
Appeal	Flow initiated by the Offender to the activity "Closing of the contravention procedure" (lane " Reporting Officer") concerning the appeal against the contravention minutes according to art. 448.
Appeal + Case	Flow initiated by the activity "Correspondence with the court" (lane " Reporting Officer") to the lane "Court" concerning the transmission of the appeal and the contravention case file. The flow is initiated according to Art. 448(2). The flow includes the dispatch of the materials to all courts in the process of hearing the appeal against the contravention minutes.
Court Decision on the appeal	Flow from the "Court" lane to the activity "Correspondence with the court" (lane " Reporting officer") on the court decision related to the appeal. The flow includes all decisions taken by all courts in the process of contesting the contravention minutes.
Contravention minutes (application of sanction)	Flow initiated by the activity "Transmission of decision to competent institution" to the lane "Competent institution", concerning the transmission of the information on the penalty applied to the offender to the competent institution for its monitoring/execution. The competent institution is established according to art 35-40
Court Decision on sanction review	Flow from the lane "Court" to the activity "Monitoring of sanction enforcement" (lane "Reporting officer") on decisions on review of sanction, art 477.

Outgoing letter Art. 450(1)	Flow initiated by the activity "Closure of contravention procedure" (lane "Reporting officer") to the lane "Responsible authorities", concerning the removal of the causes favoring the contravention, according to art. 450 (1).
Information on removal of conditions favoring the contravention	Flow from the "Responsible authorities" lane to the activity "Monitoring removal of conditions (art 450)" (lane " Reporting officer"), containing information on the removal of causes favoring the contravention.
Unpaid fines (automatically retrieved)	Flow initiated by the activity " Send case for forced enforcement" (lane " Reporting officer"), via the event "List of arrears" to the lane "Bailiff" concerning information on fines not paid on time. The information is retrieved in digital format by bailiffs.
Forced enforcement result	Flow from the "Bailiff" lane to the activity " Monitoring enforcement of sanctions" (lane "Reporting Officer") on the amounts of fines recovered.
Closure of contravention case	Flow initiated by the activity "Closure of case" (lane " Reporting Officer") to the activity "Monitoring of contravention case" (lane "Chief of Reporting Officer") concerning the closure of the contravention case and the transmission of the case to the archive.

RACI Matrix

The RACI matrix for actions in the contravention process is shown in the following table:

No.	Name of action / sub-process	Senior manager	Reporting Officer	Information system
1	Case registration	I, A	-	R
2	Initiation of case reassignment	R, A	-	I
3	Case assignment*	I, A	I	R
4	Monitoring referral assignment	R, A	-	-
5	Case acceptance*	I, A	R	I
6	Signing the outgoing letter	R, A	I	-
7	Recording documents in the case file	I, A	R	I
8	Pre-completion of the contravention minutes	I	A, C	R
9	Saving the contravention minutes	I, A	R	-
10	Examination*	I, A	R	-
11	Monitoring the progress of the contravention process	R, A	-	-
12	Signing the accompanying letter	R, A	-	-
13	Concluding the contravention minutes (Decision)*	I, A	R	-
14	Closure of the contravention procedure	I, A	R	I

15	Concluding the payment bill	I	A, C	R
16	Monitoring the payment	I	A, C	R
17	Monitoring removal of conditions (art.450)	I, A	R	-
18	Correspondence with the court	I, A	R	-
19	Monitoring sanction enforcement	I, A	R	-
20	Forwarding case to forced enforcement	I, A	R	-
21	Cancellation of sanctions	I, A	R	-
22	Closure of case	I, A	R	I
23	Archiving the case	I	A, C	R

***R** – responsible, **A** – accountable, **C** – consulted, **I** – informed*

**Sub-process*

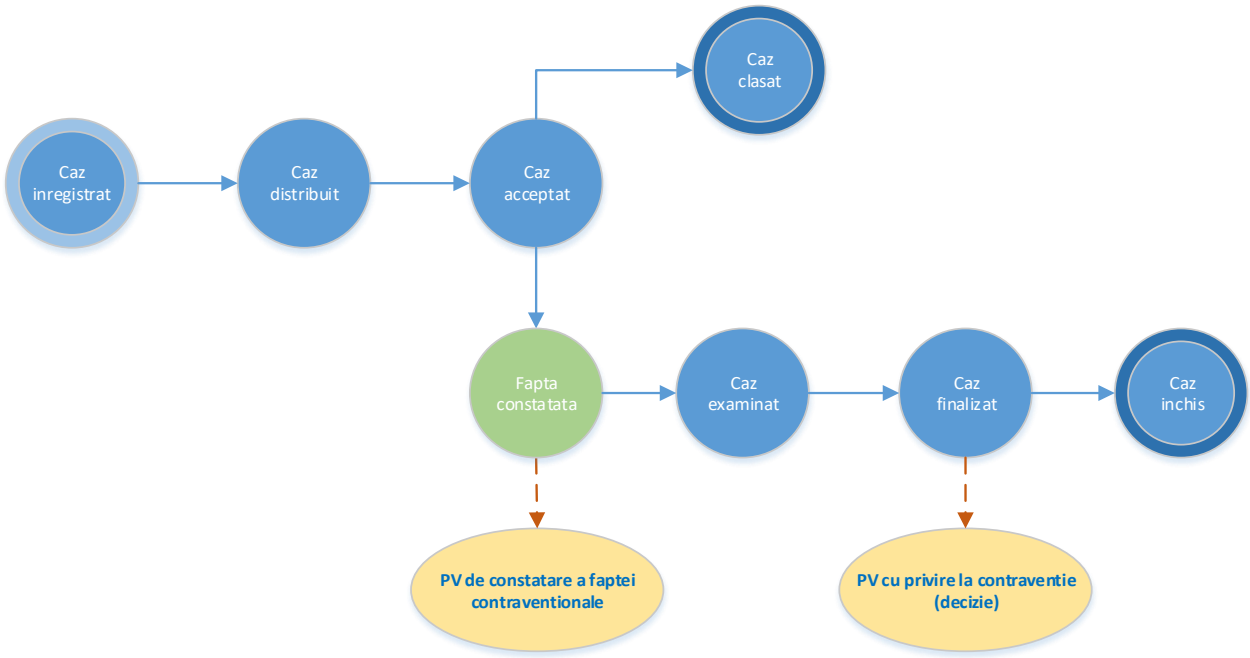
Defining the degree of involvement in the process

CSP.1. *Responsible* – the person who actually carries out the action or sub-process*;
CSP.2. *Accountable* – the person who is responsible for how the action or sub-process is run;
CSP.3. *Consulted* – the person who is consulted on the action or sub-process;
CSP.4. *Informed* – the person who is informed about the action or sub-process;

* In the case of actions automated by the implemented IT system, the system may be responsible for carrying out the action

Status diagram and CRUD matrix

The status of the contravention case, resulting from the processes and their relationships are shown in the following diagram:



The diagram shows the main states for the contravention case and an intermediate state for the offence, which is important in terms of the flow of the contravention process.

The CRUD matrix for the database objects is presented in the following table for each identified state of the contravention case.

No.	Database object	Create	Read	Update	Delete
0.1	*Signaling*				
Status: „Registered case"					
1.1	Event	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
1.2	Fact	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
1.3	Person	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
1.4	ParticipationPerson	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
1.5	Asset	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
1.6	InvolvementAsset	LMAI, AC	SIS, LMAI, AC	LMAI, AC	-
Status: „Assigned case"					
2.1	ContraventionCase	SIS	SIS, LMAI, AC	SIS	-
2.2	ReportingOfficer	SIS	SIS, LMAI, AC	SIS	-
2.3	MIAsubunit	SIS	SIS, LMAI, AC	SIS	-
Status: „Accepted case"					
3.1	ContraventionCase	-	SIS, LMAI, AC	AC	-
3.2	ReportingOfficer	-	SIS, LMAI, AC	AC	-
3.3	MIAsubunit	-	SIS, LMAI, AC	AC	-
Status: „Established fact"					
4.1	Event	AC	SIS, LMAI, AC	AC	-
4.2	Fact	AC	SIS, LMAI, AC	AC	-
4.3	ContraventionCase	AC	SIS, LMAI, AC	AC	-
4.4	Case file	AC	SIS, LMAI, AC	AC	-
4.5	Document/Act	AC	SIS, LMAI, AC	AC	-
4.6	ReportingOfficer	AC	SIS, LMAI, AC	AC	-
4.7	MIAsubunit	AC	SIS, LMAI, AC	AC	-
4.8	Measure	AC	SIS, LMAI, AC	AC	-
4.9	Person	AC	SIS, LMAI, AC	AC	-

4.10	ParticipationPerson	AC	SIS, LMAI, AC	AC	-
4.11	Asset	AC	SIS, LMAI, AC	AC	-
4.12	InvolvementAsset	AC	SIS, LMAI, AC	AC	-
Status: „Dismissed case"					
5.1	Event	-	SIS, LMAI, AC	AC	-
5.2	ContraventionCase	-	SIS, LMAI, AC	AC	-
Status: „Examined case"					
6.1	Event	-	SIS, LMAI, AC	AC	-
6.2	Fact	-	SIS, LMAI, AC	AC	-
6.3	ContraventionCase	-	SIS, LMAI, AC	AC	-
6.4	CaseFile	-	SIS, LMAI, AC	AC	-
6.5	Document/Act	-	SIS, LMAI, AC	AC	-
6.6	Measure	-	SIS, LMAI, AC	AC	-
6.7	Person	-	SIS, LMAI, AC	AC	-
6.8	ParticipationPerson	-	SIS, LMAI, AC	AC	-
6.9	Asset	-	SIS, LMAI, AC	AC	-
6.10	InvolvementAsset	-	SIS, LMAI, AC	AC	-
Status: „Finished case"					
7.1	Event	-	SIS, LMAI, AC	AC	-
7.2	Fact	-	SIS, LMAI, AC	-	-
7.3	ContraventionCase	-	SIS, LMAI, AC	AC	-
7.4	Case file	-	SIS, LMAI, AC	AC	-
7.5	Document/Act	-	SIS, LMAI, AC	AC	-
7.6	Measure	-	SIS, LMAI, AC	AC	-
7.7	Person	-	SIS, LMAI, AC	-	-
7.8	ParticipationPerson	-	SIS, LMAI, AC	-	-
7.9	Asset	-	SIS, LMAI, AC	-	-
7.10	InvolvementAsset	-	SIS, LMAI, AC	-	-
Stare: „Finished case"					
8.1	Event	-	SIS, LMAI, AC	AC	-

8.2	Fact	-	SIS, LMAI, AC	-	-
8.3	ContraventionCase	-	SIS, LMAI, AC	AC	-
8.4	Case file	-	SIS, LMAI, AC	AC	-
8.5	Document/Act	-	SIS, LMAI, AC	AC	-

AC – Reporting Officer, LMAI – MIA employee, SIS – Senior Manager

There will be two types of documents in the WFMS:

1. Documents generated from WFMS;
2. Documents in written form, a scanned copy of which will be attached to the contravention case file;

The WFMS computer system will allow a status to be assigned to each document. The statuses can be selected from a list of statuses available in the computer system.

For documents generated from the WFMS the specific statuses are as follows:

1. 'In work';
2. 'Finished';
3. "Reviewed";
4. "Registered";
5. "Approved";
6. "Transmitted";
7. "Cancelled";
8. "Archived";
9. "Created" (for situations where the document is automatically generated by the computer system, but not yet taken over by the user);
10. "In Control" / "Awaiting response";

The list of values for the status nomenclature shown above is not complete, the application should allow additional statuses to be added to the list and/or existing statuses to be deleted from the list.

Statuses for documents in written form:

1. “Copy document”;
2. “Authenticated copy of document” – marked “true to original” and digitally signed by the person (user) authenticating the document;

The following statuses can be selected from the list of statuses for the Contravention Case:

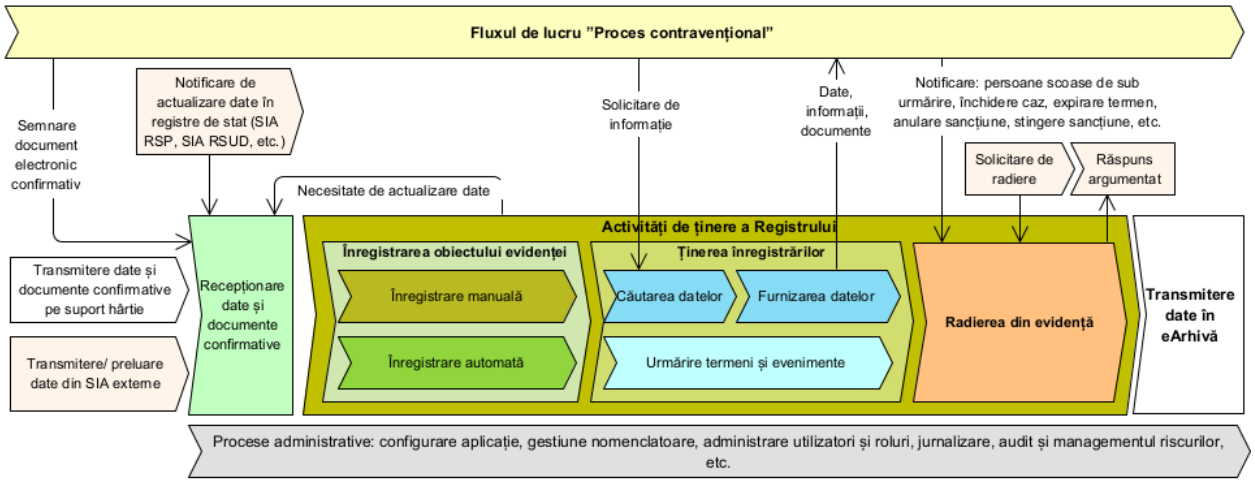
- “open” (“created”) – from that moment on, component elements (documents or metadata) can be added to the case file;
- “in work” (“incomplete”) – stage at which elements have been added to the case file, but the case is not complete;
- “suspended” – temporary phase in which component elements cannot be added to the case file;
- “closed” (“complete”) – phase where all component elements have been added to the case file;
- “archived” – the case file can only be consulted from the archive;

The following statuses can be selected from the nomenclature of statuses for the contravention minutes:

1. “in work” – the reporting officer is working on the preparation of the contravention case minutes;
2. “finished” – the reporting officer has finished the contravention case minutes by completing the decision;
3. “registered” – the contravention case minutes has been registered in the electronic register and has a unique registration number assigned;
4. “sent” – the contravention case minutes has been sent to the offender;
5. “contested” – the contravention case minutes has been contested in court;
6. “final” – the contravention case minutes is final, following a court decision;
7. “cancelled” – the contravention case minutes has been cancelled by a court decision;
8. “paid” – the amount of the contravention sanction has been paid by the offender.

Annex. A3
Workflow associated with the process of keeping departmental state records related to the contravention process

In general, the workflow related to keeping the registers in the e-Contravention Case Management System is shown in the following figure:



The basic workflow includes the following steps:

1. Receipt of information
2. Recording the object of the record, including:
    a. Automated recording
    b. Updating of data
3. Record keeping, including:
    a. Searching and providing data from the register
    b. Tracking terms and events
4. Removal of the record from the register

Receipt of information

The information to be entered in a register maintained in the e-Contravention Case Management System can be generated:

1. Automatically, from within the "Contravention case management" workflow. The signature of the confirmatory document containing the information on the object of record within the workflow by the Reporting Officer who is also the Registrar is considered the trigger for the entry in the register if the regulations for keeping the register do not provide for another procedure.
2. When uploading in the e-Contravention Case Management System, within the workflow of the confirmatory documents on paper (e.g. Court decision).
3. Receipt of confirmatory documents in electronic format from External Data Providers (e.g. Prosecutor's order on prosecution for a contravention, in relation to the non-prosecution or termination of prosecution).

Recording the object of the record

All data relating to the object of the record in the Register shall be entered only on the basis of the Registrar's decision, in the presence of supporting documents or information received from other automated information systems confirming the veracity of the information with reference to the document or information resource on the basis of which the information was entered/updated.
In the case where the Reporting Officer acts as Registrar, the signing of the confirmatory document within the workflow automatically initiates the initial entry or update of the object of the record in the Register.

Initial entry (entry of data in the register) - is carried out after the Registrar's decision to include the entry in the Register. In this case, a unique identifier is assigned to each object subject to registration, with the exception of borrowed information objects, whose identifier is taken from the source registry. The identifier of the object shall remain unchanged throughout the existence of the object in the registry.
Objects shall be recorded in the register in chronological order at the time of submission of the supporting documents or data required for registration, no later than the deadlines laid down by law and the rules for the maintenance of the register;
When the object is entered in the register, the associated metadata, including data on the fact of registration and the documents submitted, on the basis of which the decision on the entry of the object in the register was taken, is assigned to the associated metadata. The set of metadata for each object is determined by the rules for maintaining the register.

Making changes - consists of entering a new version of the object of the record on the basis of the registrar's decision. All changes are kept in chronological order. Together with the amended data, information on the fact of registration of the changes made and the documents on the basis of which the change decision was taken is entered in the register;

Initial recording also involves automatic reporting of the fact to the Statistical Data Bank of the accident information (statistical data recording scenario).

Record keeping

Record keeping involves granting access and providing data from the register. Providing register data is done by:

a. the auto-completion scenarios of the documents produced in the digitized workflows in the e-Contravention Case Management System;
b. granting sanctioned access via the interoperability platform;
c. issuing paper documents, in the established way, only to natural persons-applicants;
d. providing information via electronic mail or other means of communication.

The granting of access to the data in the register shall be carried out in accordance with the legislation in force on data exchange and interoperability.
The provision of data from the register via auto-completion scenarios within the workflow in the e-Contravention Case Management System shall be carried out in accordance with the access rights of the executor. The request for information and the information about acceptance or refusal is recorded in the event log.
Excerpts from the register, certificates and documents are only made available by the registrar. Extracts from the register and certificates shall bear the signature of the Registrar. Electronic documents shall bear the digital signature of the Registrar.
The provision of data and copies of state register documents may be restricted in the manner prescribed by law if it endangers or is likely to endanger:

a. the security or defense capability of the State;
b. the conduct of criminal proceedings;
c. public order;
d. the fundamental economic and financial interests of the State;
e. the rights, freedoms and interests of data subjects or other persons.

The provision of register data to natural and legal persons of foreign states shall be carried out on the basis of the legislation of the Republic of Moldova and international agreements to which the Republic of Moldova is a party.

Keeping records involves *tracking terms and events*. The registers management component of the e-Contravention Case Management System provides notifications on:

17. expiry of the time limit or receipt of a notification providing for deletion of the record from the register
18. deadline providing for a change in the status of the record object (e.g. exceeding the deadline for payment of the fine, limitation period, accumulation of maximum penalty points, etc.).

Removal of the record from the register

Removal of the record from the register can be:
Removal (deletion) from the record - consists of changing the status of the record object (including transferring the record object data to the archive at the end of the life cycle), based on the registrar's decision upon the occurrence of certain events or automatically upon the expiration of the data retention period.
Elimination of the record object - in case of requalification of the fact or discovery of circumstances requiring the elimination of the fact/person from the record, it is done based on the decision of the registrar, based on the primary documents received. The elimination from the register implies the definitive deletion of the record from the register, with the preservation of the associated data (including the identifier of the record object) in which information about the event is entered (basis, confirmatory document, decision maker, etc.).
The deletion from the record also implies the automatic reporting of the deletion of the variant of the statistical variable to the statistical database (statistical data suppression scenario).

In addition to the basic flow, record keeping also includes administrative processes such as: application configuration, nomenclature management, user and role management, logging, audit and risk management, etc.

Annex. A4
Contravention case management: artifacts of data architecture

Data model defining workflow Contravention case management and related activities

The data model reflects the information to be used (entered, processed, stored) to ensure the smooth running of work processes. The data model is reflected in the IT systems that are to store and process the information.

According to the data model, the IT solution that will automate the work processes will allow two categories of information related to the contravention procedure to be stored in the database:

- Structured information - this will be stored in the form of attributes of related objects, relevant to the contravention process, for which the proposed data model is presented later in this section;
- Unstructured information - this will be recorded in the form of documents in electronic format, resulting from obtaining a scanned copy of an original printed document (scanned documents may be marked "true to original" certified by digital signature).

Data sources

The IT solution that will automate the work processes will allow the storage of two categories of information related to the contravention procedure in the database:

- Structured information - this will be stored in the form of attributes of related objects relevant to the contravention process, for which the proposed data model is presented later in this section;
- Unstructured information - this will be recorded in the form of documents in electronic format, resulting from obtaining a scanned copy of an original printed document (scanned documents may be marked "true to original" certified by digital signature).

The data to be managed within the computer system will have the following sources of generation:

- Data contained in the existing nomenclatures within the WFMS computer system;
- Data entered manually into the WFMS computer system via user screens;
- Data provided automatically by other IT systems through specialized data exchange interfaces (e.g. web services);
- Data contained in the own nomenclatures of other computer systems/databases, obtained by query and provided via specialized data exchange interfaces (e.g. web services);
- Data obtained by digitization (OCR-ization) of documents in printed form;

Templates for incoming and outgoing documents:

The documents used in the work process related to the contravention procedure are distinguished in relation to their management mode in the WFMS and their role in the contravention procedure:

All documents stored in the WFMS have header information that includes at least:

1. Document registration number
2. Date and time the document was concluded
3. Date of registration of the document
4. Place where the document was concluded

5. Author of the document
6. Type of document (from the register of documents)
7. Status of the document (original/copy/corroborated copy)

All the documents related to the contravention case are encapsulated in the " Case". The Case is a container for documents and allows the whole package of documents to be managed in the process.

The list of documents used in the contravention process and their characteristics is presented in Annex No. 3. The list can be completed according to the needs of MAI. The list is subject to the Nomenclature of types of procedural documents.

In order to ensure the synchronization of the activities carried out by the Reporting Officer with the process running in WFMS, a number of documents will be perfected in the system. They can then be printed and attached to the file in written form. These documents are considered process documents. The rest of the documents are considered as input documents for the WFMS and only generic information and in some cases scanned copies are entered.

It is important that in the case of the initial completion of the process documents in written form, they are scanned into WFMS.

List of documents to be digitally supported by the e-Contravention Case Management System

#	Name of document	Contravention process stage	Description (brief description of the content, stage of the contravention process to which it applies, etc.)	Regulatory basis	Notes: Specific aspects (e.g. numbering, record keeping, etc.)
1.	Referral	Initiation		art.440 para.(2) Contravention Code	
2.	Complaint	Initiation		art.440 para.(2) Contravention Code	
3.	Contravention Case	Initiation	including: title page and contents page	art.384 para.(2) let.h) and art.440 para.(1) Contravention Code	
4.	Report on registering the contravention	Initiation	Registration of the contravention in the register of contravention cases of the subdivision in which the reporting officer works, initial stage of the contravention process.	Republic of Moldova Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	Blanks of strict record with special numbering (RAP)
5.	Prosecutor's order on contravention prosecution in connection with the non-prosecution or termination of criminal proceedings	Initiation	Prosecutor's order on the initiation of prosecution in respect of the contravention, in connection with the refusal to initiate criminal proceedings, the termination of criminal proceedings on the grounds that the act constitutes a contravention, as well as in cases of release from criminal liability of the person with the contravention liability brought	art.396 para.(2) Contravention Code	
6.					
7.	Victim hearing minutes	Examination	Examination stage of the contravention case	Republic of Moldova Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering
8.	Witness hearing minutes	Examination	Examination stage of the contravention case	art.388 para.(4) RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering
9.	Suspect hearing minutes	Examination	Examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering
10.	Explanations of the person against whom the contravention procedure was initiated	Examination	Statements of participants in the contravention process, which may serve as evidence in the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering

11.	Minutes of the road accident scene investigation	Finding	Examination of the circumstances of the accident at the scene, carried out at the examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (CER)
12.	Sketch of the road accident	Finding	Graphic representation of the road accident, examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (SAR)
13.	Minutes of technical inspection of the vehicle	Examination	Checking the technical specs of the vehicle involved in the road accident, at the investigation/examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (IAS)
14.	Minutes of the examination and verification of the technical condition of the transport unit	Examination	Examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering
15.	Proof of technical breakdown of vehicles in road accidents	Examination	Evidence gathered during the examination procedure of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (DOV)
16.	Minutes of removal of registration plates	Finding	Removal of plates in cases specified in the Contravention Code	art.439 para.(7) RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (NUM)
17.	Provisional driving license	Finding		art.429 para.(7) Contravention Code	
18.	Minutes of retention and bringing the vehicle to the special parking place	Finding	Action taken in the context of the finding of a contravention and the circumstances requiring the application of this measure.	art.439 para.(3) RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering (VEH 01)
19.	Minutes of on-the-spot investigation	Finding		art.426 para.(5) and art.430 Contravention Code	
20.	Minutes of removal of objects and documents	Finding, Examination	Action carried out in the process of examining the contravention case, which may subsequently serve as evidence in the contravention proceedings	art.426 para.(5) and art.430 RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	With special numbering (PRO)
21.	Removal order	Finding, Examination	Action taken in the process of examining the contravention case, which may subsequently serve as evidence in the contravention proceedings	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	With special numbering (ORD)
22.	Request for the submission of a declaration of the identity of the driver of the vehicle at the time of the contravention.	Examination	Action taken in the process of examining the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	With special numbering

23.	Referral to the medical institution	Examination	Examination stage of the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	No special numbering
24.					
25.	Conclusions on the basis of medico-legal examinations, forensic, auto-technical and transcription investigations	Examination			
26.	Expert report	Examination	Expertise and findings	art.425 para.(2) Contravention Code	
27.	Minutes on the apprehension of the person			art.434 para.(1) and art.433 para.(3) and (4) Contravention Code	
28.	Minutes of the body search			art.429 and art.430 Contravention Code	
29.	Authorization of the court of law for the search of the domicile	Examination		art.426 para.(2) and art.428 para.(2) Contravention Code	
30.	Order for house search	Examination		art.426 para.(3) and art.428 para.(2) and (3) Contravention Code	
31.	Order for handing over for storage	Examination		art.426 para.(5) Contravention Code	
32.	Order for the attachment of corpus delicti	Examination		art.427 para.(1) Contravention Code	
33.	Decision of the court to seize documents containing information constituting a state secret	Examination		art.427 para.(2) Contravention Code	
34.	Authorization of access to the materials of the contravention case	Examination		art.451 Contravention Code	
35.	Outgoing letters	Examination	Addressed to the participants in the proceeding		
36.	Consent to verification of personal data	Finding, Investigation	The stage of finding and examining the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022 Law No. 133/2011 on Personal Data Protection	No special numbering
37.					

38.	Decision to examine the contravention on the basis of the personal finding of the reporting officer	Decision	Issuing the decision on the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	Blanks of strict record with special numbering (DCA)
39.	Decision on the contravention case	Decision	Issuing the decision on the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	Blanks of strict record with special numbering (DAC)
40.	Decision to terminate the contravention proceedings	Decision		RM Contravention Code No. 218/2008, Government Decision 517/2022	
41.	Cooperation agreement	Decision	Issuing the decision on the contravention case	RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	Blanks of strict record with special numbering
42.	Minutes of the contravention	Decision	Issuing the decision on the contravention case	art.382 RM Contravention Code No. 218/2008, Government Decision 517/2022, MIA Order 195/2020, GPI Order No. 95/2022	Blanks of strict record with special numbering (MIA)
43.	Minutes of the finding of refusal to sign the minutes				
44.					
45.	Outgoing letter with reasoned decision to reclassify the contravention case	Referral according competence	Reclassifying the contravention into a criminal offence	art.424 and art.449 para.(1) Contravention Code	
46.	Outgoing letter with reasoned decision to refer the contravention case to the competent authority	Referral according competence		art.399 para.(2) and art.440 para.(5) Contravention Code	
47.	Reasoned refusal report	Referral according competence		art.399 para.(1) Contravention Code	
48.	Appeal against the contravention minutes	Appeal		art.448 para.(2) Contravention Code	
49.	Decision of the court issued in the context of examining the appeal against the decision of the reporting officer	Appeal			
50.	Court judgement		The contravention judgment	art.462 Contravention Code	
51.	Summons			art.382 Contravention Code	

52.	Summons with request for the submission of a statement on the identity of the driver of the vehicle			art. 443^1 p. (1), Contravention Code, Government Decision 517/2022, annex 2. p.26	
53.	Recourse	Appeal		art.465, art.467 para.(1) Contravention Code	
54.	Judgement of the recourse court	Appeal		art.473 and art.474 Contravention Code	
55.	Accompanying letter of enforceable documents for enforcement	Enforcement			
56.	Receipt for collection of the fine at the place of the contravention	Enforcement		art.446 para.(1) let.a) Contravention Code	
57.	Receipt for payment of the fine	Enforcement		art.34 Contravention Code	
58.	Letter of referral concerning the removal of the causes of the contravention	Enforcement		art.450 para.(1) Contravention Code	

Data validation rules

Data entered into the WFMS (input data) will be validated based on the following rules, which will be implemented by the system provider:

- Data will be entered in special fields, which will only allow the selection of a content from a predefined list (nomenclature), which will be continuously maintained by an administrator;
- Data will be entered only by the user who is the owner of that data set - the owner of the data will be identified at person and compartment/subdivision level of MIA.

Reports

Two groups of reports are present in the management of the contravention process in WFMS:

1. Thematic reports. Thematic reports are part of the user's work process and are configured on the basis of the information related to the contravention process entered in the system.
2. Workflow reports. Workflow reports refer to the status of WFMS processes and objects.

The main thematic reports considered are:

No.	Name of report	Description
1	Register of referrals of findings of contravention (external register)*	Register of referrals of violations classified as contraventions received from the "Event Management" system
2	Register of contravention cases (external register)**	Register of contraventions, offenders and results of the examination of contravention cases
3	Register of contravention minutes	Register of the numbered forms of the minutes of the contravention case associated with the contravention files.
4	Report on the limitation period	Report on the expiry of the limitation period for a contravention case whose file is not closed
5	Report on the status of payment of the fine	Report synchronized with the Billing system of the MIA and MPay on fines paid and not paid in time.
6	Case transfer report	Report on the request of the Reporting Officer to transfer the file to another Reporting Officer or according to the competence. The report is received by the Chief of the Reporting Officer as part of the monitoring activities.

*Note: Registers are contained and accessed from the Event Management system.

Reports related to the workload can be obtained using specific WFMS tools and can refer to any object or/and process and its status. Based on industry practice the following groups of reports are most commonly used:

1. Workflow status reports - indicate the status of processes by executors, time, activity, etc.

2. User activity reports, by process, for a given period. The Reporting Officer's report on the contravention cases handled over a period of time and their status is a particular value of the overall WFMS report(s).

The list of reports can be extended according to the needs of the beneficiary.

Nomenclatures

The following main nomenclatures will be used in the computer system:

1. Nomenclature of contraventions;
2. MIA organizational nomenclature;
3. Nomenclature of addresses for locations;
4. Nomenclature of types of referrals;
5. Nomenclature of types of person's participation;
6. Nomenclature of types of involvement of the asset;
7. Nomenclature of types of person;
8. Nomenclature of types of assets;
9. Nomenclature of types of procedural documents;
10. Nomenclature of types of measures;
11. Nomenclature of types of status;

The nomenclatures must be updated regularly by the computer system administrator.

Structure of the nomenclatures:

1. Nomenclature of contraventions;
   Structure: ID, name of the act, description of the act, CC art.
2. MIA organizational nomenclature;
   Structure: ID, MIA subunit, legal address;
3. Nomenclature of addresses for locations;
   Structure: ID, street, number, house/block, floor, apartment, town, district;
4. Nomenclature of types of referrals;

Structure: ID, referral type name, referral type description;

5. Nomenclature of types of person's participation;
   Structure: ID, role description;
   Values: perpetrator, victim, witness;
6. Nomenclature of types of involvement of the asset;
   Structure: ID, role description;
   Values: object of the act, used in the act;
7. Nomenclature of types of person;
   Structure: IDNP, name, surname, patronymic, date of birth, sex, place of birth, nationality;

8. Nomenclature of types of assets;

   Structure: ID, asset type name, brand, model, series, year of manufacture, registration number, asset description;

9. Nomenclature of types of procedural documents;

   Structure: ID, type of procedural document, description of procedural document;

10. Nomenclature of types of measures;

    Structure: ID, name of type of measure, description of type of measure;

11. Nomenclature of types of status;

    Structure: ID, type of status;

Annex. A5
Reusable application capabilities: application architecture artifacts

Platform application capabilities:

These capabilities address the common needs of several processes and activities of the MIA. This facilitates the re-use of platform applications to produce distinct ICT services;

1. Platform capabilities for workflow digitization and registry keeping

The e-Contravention Case Management System will have at least the following capabilities **required to support workflows and case management of contraventions**:

1. Entities Builder:

- Capacity to create custom entities to store and manage specific data or information
- Capacity to define relationships between entities and manage the data associated with them
- Capacity to customize the structure of entities to fit the needs of the organization
- Capacity to import and export entity data and generate custom reports based on it
- Capability to maintain metadata about objects in the system. Every record has an associated set of metadata that describes it and accompanies it throughout its lifecycle. The ability to define metadata sets provides flexibility to define new entities and manage them by the user without intervention at program code level.

2. Workflow Builder:

- Capacity to create complex and customized workflows that meet the needs of the organization
- Capacity to create and manage tasks and activities, including setting workflow automation rules
- Capacity to set priorities and deadlines for tasks and activities
- Capacity to track the status of tasks and activities within the workflow
- Capacity to add conditions and branches to workflow to handle exceptional situations or divergent decisions
- Capacity to add support for different workflow models (e.g. automatic/human decision; sequential/parallel; direct/escalation; etc.);
- Capability to optimize workflow by setting triggers and alerts that notify and direct information to the right people when their action is needed in the compensation process;
- Capability of graphical process modelling - has visual mechanisms/natural language for describing traditional work processes in the form of an electronic workflow (WorkFlow designer) and the ability to export/import workflow (entities, rules, templates, etc..) in the most widely applicable formats for the domain (e.g. BPMN2.0);

2. Form Builder:

- Capacity to create custom forms for collecting specific data or information, including structured data and digital signatures
- Capacity to associate forms with specific workflows, entities or reports
- Capacity to customize the layout and design of forms to match the organization’s branding
- Capacity to validate data entered on forms and generate notifications or alerts if data is incomplete or incorrect
- Capability to visually design forms

- Capability to set validation controls at form and field level. Capability ensures pre-filling of forms.

4. Report Builder:

- Capacity to create custom reports based on data or information stored in entities or forms
- Capacity to customize the layout and design of reports to match the organization's branding
- Capacity to export reports in different formats such as DocX, PDF, Excel or CSV
- Capacity to schedule reports to be automatically generated at regular intervals or on specific events
- Strengthen reporting and control by generating standardized and customized reports and creating mechanisms to monitor activity.
- Capability to configure the usage scenario of the reports according to the dissemination mode (e.g. documents printed on blanks of strict record cannot be printed multiple times, e.g. reports strictly intended for printing cannot be stored as files, etc.)

5. Template/Document Generation:

- Capacity to create custom templates for documents or communications, such as procedural and court documents, standard letters or emails
- Capacity to associate templates with specific workflows or entities
- Capacity to generate custom documents based on data or information stored in entities or forms
- Capacity to customize the layout and design of generated documents to match the organization's branding
- Capacity to export documents

6. Content indexing and search capabilities.

- Capability to store information in a categorized and indexed manner;
- Capability to retrieve and present records and metadata in response to queries. There are two methods by which users can discover entities in a register: (1) by navigating from an entity to associated entities or, (2) alternatively, by searching for entities that match a given search query.
- The e-Contravention Case Management System will provide indexing of at least the following categories of data:

    a. Content of documents created within the workflow
    b. Workflow metadata
    c. Content of records in the Registers;
    d. Metadata of records in the electronic archive.

- The e-Contravention Case Management System will provide a full text indexing solution for documents providing facilities to reduce synonyms, prefixes and suffixes as well as normalizing the relevance of document terms to the size of the document (the calculation of the weight of terms should not depend on the file size) in order to eliminate cases of priority of large documents over small documents.

7. Capabilities for keeping registers

- Storage component (repository) - refers to the capability to store information in a categorized and indexed manner.
- Ability to work with file repository(s) integrated into the common platform. It will be ensured that the images, files included, can be stored/retrieved in/from the file repository;

- Capability to define rules for validating records in the repository. All records and their attributes must correspond to a well-defined set of rules. These will ensure that each record in the registry is complete and logically consistent (record attributes will only be able to take correct values). The rules for validating records will be applied when creating/modifying data via user interfaces as well as application interfaces;
- Classification service- provides the capability to hold a classification, apply it when aggregating records, and link fields within the classification rules to the record keeping model. Each record is classified to facilitate its control and disposition. By classification, each record is linked to the business process that generated it.
- Records Service - provides the capability to group (aggregate) records. Each aggregation represents a grouping of records or a grouping of aggregations. Records are placed in aggregations that relate to: same format, access pattern, business classification, person, place, event, have common metadata, have the same source or format, are managed by the same business unit, have similar disposal conditions, etc.
- Metadata model service - provides the capability to maintain metadata about objects in the system. Every record has a set of metadata associated with it that describes it and accompanies it throughout its lifecycle. The capability to define metadata sets provides flexibility to define new entities and manage them by the user without intervention at the program code level.
- Erasure scheduling service - refers to the capability to hold record erasure rules according to retention rules. A record cannot be retained if the legal basis under which it was made has expired. The erasure schedule is used to manage the life cycles of records according to established legal procedures. Similarly, the service ensures that on disposal a residual record remains for the lifetime of the system. The residual record, demonstrates not only that a record was once active, but more importantly, that the record was properly disposed of in accordance with an appropriate disposal protocol.
- Retention service - the capacity to prevent the application of a record deletion rule in the event of a theme arising. Removal of records does not always mean destruction. According to Law 133/2011 the disposal of records can be: by archiving, depersonalization, or destruction.
- Export-import capability - ensures that entities in a registry can be described in sufficient detail, in a common XML data format, so that metadata values, event history, access controls and content can be preserved and transferred to another registry without loss or distortion.

8. Case management:

- provides specialized functionalities for grouping structured and unstructured content, automating adaptive and multi-person processes and setting deadlines for open cases. Cases can also be completed and closed with associated information stored and audited;

2. Interoperability capabilities

Purpose: "Back end" solution designed to provide the platform needed to implement interoperability between MIA applications, as well as communication with external MIA applications, including government platform services

MIA uses as ESB platform the MConnect service and its semantic catalogue.
The MConnect solution provides at least the following capabilities:

- supported transport protocols (e.g. HTTP, HTTPS, POP, IMAP, JMS, etc.),
- message formats (e.g. JSON, XML, SOAP 1.2, etc.),
- mediation functions,
- routing and transformation and service orchestration,
- authentication and security functions,
- semantic catalogue and service catalogue management functions

Capabilities of specialized applications

ICT capabilities required to support specific activities and processes of the MIA. Specialized capabilities are developed when they cannot be provided by orchestrating generic capabilities. They are also associated with applications already implemented and that will continue to be used

1. IT service for generating payment bills for Billing fines:

- Set up of treasury accounts related to each entity, including according to payment items.
- Ensure traceability in case of changes to treasury accounts
- Design of payment bill templates
- Integration with MPay
- Event tracking (e.g. payment in MPay)
- Reports on payments ordered and made
- Design and implementation of data exchange with the State Treasury in order to track and reconcile the payment made according to the payment bills issued.

2. Application capabilities provided by the e-Data v2 mobile application

Mobile application that will run on the mobile devices supplied to MIA teams. The application will allow the visualization of relevant information within the missions and operations carried out (information about persons, means of transport, orders and indications, etc.), as well as the making of records related to the actions carried out (e.g. verification of means of transport, apprehension, request to pick up means of transport, etc.). Depending on the responsibilities of the person / crew who will use the application, access rights to information and operations can be set.

Capabilities provided:

- Integration with approved mobile devices for the purpose of retrieving data on detected violations:

    1. LTI 20/20 ,,TruCAM" (laser) speed measuring device for vehicles;
    2. Drager Alcotest 7510 breath ethanol concentration analyzer;
    3. Drager Alcotest 6820 breath ethanol concentration analyzer.

- taking photo, video and audio images from non-approved mobile devices for the purpose of being used as samples. As non-approved mobile devices are considered Smartphones and Tablets.
- audio recording of the fact of the communication of the person's rights by the RO (or photo/video recording of the fact that he/she was made aware of them - alternatively it may be required to tick each point on the tablet with a photograph of the moment).
- automatic reading of information from QR code on ID documents (it is expected that ID card, driving license and other documents will contain QR code).
- verification of information to which the MIA has access, about persons and objects (any person identified on the basis of an identification document, drivers and penalty points, means of transport, locations, buildings, weapons, other marked objects);
- receiving targeting information in the context of hot track apprehension operations;
- receiving directions, orders and instructions to the mobile team;
- communication to the operational command center of relevant information on events on the ground, actions taken and relevant requests (authorization of actions, assistance, etc.);
- setting legal actions taken by police officers (e.g. checking person, means of transport, search, detention, etc.);
- signing of the documents with electronic holographic signature;

- capture and identification of the registration number and type of vehicle;
- precise identification of location (geo-referencing capability)
- fingerprint capture
- identification of the person by fingerprint
- facial image capture
- search of person by facial image
- generation and auto-completion of the 'self-report form'.
- Transmission of the "self-report form" to the registration process”

3. IT electronic holographic signature service

This is a specialized service that provides capabilities whereby a person can electronically sign a document or file using a touch screen device. The service is to be reused by the e-Contravention Case Management System and the e-Data v2 mobile application component.

4. IT service for capturing and identifying the vehicle registration number and type;

This is a specialized service that provides capabilities to identify the vehicle registration number based on image or video capture. The service is to be reused by the e-Contravention Case Management System and e-Data v2 mobile application component.

5. IT geolocation service

Provides capabilities for geospatial positioning of objects and events of interest to the MIA. Allows the uploading and use of various purpose-specific maps, including official maps provided by central and local authorities. Capabilities can be integrated through application interfaces into other information systems.
Usage scenarios: obtaining geospatial coordinates by user indicating the location on the map; placing objects and events on the map according to their geospatial coordinates.

6. IT fingerprint capture service

This is a specialized service offering capabilities to capture fingerprint images using specialized devices. The fingerprint image is transmitted to other application components of the e-Contravention Case Management System which ensure its verification in AFIS AIS.

7. IT facial image capture service

This is a specialized service providing capabilities for real-time facial image capture using a mobile device such as a tablet or smartphone. The captured image is then used to identify the person in the specialized application used by the PSA. The format of the captured image must match the requirements of the facial recognition application used by the PSA.

8. IT service for submitting the referral in electronic format

The e-Contravention Case Management System will have capabilities to receive referrals in electronic format.

9. e-Contravention Record service

The e-Contravention Record service reuses the capabilities of the government platform services.gov.md for the IT service for requesting contravention records.
The e-Contravention Case Management System will have capabilities to integrate the Contravention Record request received from the services.gov.md platform solution with the workflow to validate the request, extract the information and issue the Contravention Record based on the stored information.

10. Capabilities provided by the MIA application

Name	Role	Specification
Full name of the architecture component	The role of the component at the large-scale application architecture level.	Key functionality expected to be provided by the architecture component.
IS AFIS	Integrated solution (software & hardware) for fingerprint-based identification of persons based on digital papillary prints, integrated with international databases.	The solution also provides tools for: - searching for matches in the AFIS database; - analyzing fingerprint information and identifying persons whose fingerprints do not match those stored in the AFIS database; - verification of biometric data recorded in AIS SRP. Similarly, there is functionality for query management. It allows the establishment of priority lists
IS Traffic Control	Specialized application existing in the current architecture as part of the PolData application package (IS Traffic Control). The application is intended for the reception of reports of traffic violations and their validation by operators.	CUMC specialists are the primary users of the system. They receive the reports from the video monitoring system, analyze them in order to validate or reject them. Only validated referrals at Traffic Control IS level become available later to the reporting officers (manually indicated) within the ECCRPP IS (in the future GCC IS architecture). In the future architecture, the application is to be developed to be able to receive reports on traffic violations from any external source (e.g. web, mobile applications, email, etc.). The analysis and validation flow will be similar.
AIS RICC	The AIS RICC is intended for the maintenance of the Register of Forensic and Criminological Information, according to the provisions of the Law no. 71-XVI of 22.03.2007 on registers. It also forms the Central Data Bank of the Automated Integrated Information System for the Recording of Offences, Criminal Cases and Offenders, in accordance with Law 216 of 29.05.2003.	Functional specifications: - Performing specific tasks of the automated information system intended for keeping in electronic form the State Register of Forensic and Criminological Information, as provided for by the Law No 71/2006 on registers. - Providing operational information for the purpose of supporting criminal prosecution activities and special investigations of law enforcement agencies. - Supporting a dynamic data model in the forensic and criminogenic domain, to respond to current and future needs of the OD for tactical and strategic analysis in order to define and monitor policies in the domain. - Provide official national information on crimes recorded by law enforcement agencies in Moldova, offenders and other authorized criminal information; - Provide operational information on the crime situation in the country; - Provide information on the performance of law enforcement bodies in the field of crime prevention and control; - Formation of national statistical data bank on criminological and criminogenic phenomenon and provision of statistical data with the application of open standards. The statistical data bank is formed by collecting statistical information, depersonalized and serves as an information support for tactical activities, analysis, development and monitoring of public policies in the field of prevention and fight against crime. - Supporting technological interoperability with the information systems of other DOs, public institutions, external partners and other third parties in order to receive and provide criminal intelligence in an authorized manner
Internal management		
HR management system	The application is intended for the management of personnel resources at the level of the MIA and MIA subdivisions.	Functional specifications: - Organizational structure management and staffing scheme for MIA and subordinate subdivisions (with the possibility of versioning, structure modification in draft and subsequent activation); - management of the MIA's and subordinate subdivisions' staff (hiring, transfer, dismissal, application of sanctions, promotion, awards and rewards, etc.);

		- employee files (personal information, education, family situation, trainees, travel, professional certifications, special ranks held, etc.); - information management on former employees; - management of the scheme for holding special grades; - timekeeping (timesheets, correction tables, rest/sickness/maternity/childcare leave, etc.); - making calculations relating to salary payments and other payments to employees and former employees; - recording events as a result of which MIA employees suffered; - integration with the State Register of Civil Servants; - management of the database of candidates; - management of career development plans (optional); - talent management (optional);
Common use services		
GIS platform service	The service is intended for the management of GIS maps required in the MIA activity, the generation of specialized map layers based on data provided by other MIA applications, according to the specific needs of MIA subdivisions.	Functional specifications: - GIS map loading (roads, streets, buildings, utilities, land, etc.); - real-time access to external GIS services with OGC standard support; - presentation of the overall operational picture on GIS maps; - integration with GPS tracking systems and mapping to map objects; - production of GIS layers according to user settings (events, teams, operations, etc.). Use of custom elements for map elements; - interactive access to information within GIS maps; - scrolling in time the evolution of the overall operational picture on the GIS map; - tools for performing strategic, tactical and operational analysis using GIS maps (e.g. determining areas potentially affected by fire, contamination, etc.); - management of any number of map layers; - the ability to overlay layers and combine information from different GIS map layers;
Billing and settlement service	Platform service for generating payment invoices for services provided by MIA subdivisions and for imposed contravention fines, and monitoring their payment status.	Functional specifications: - Catalogue management of public and government services at MIA level (services, provider, beneficiaries, sub-services/options, prices); - management of administrative sanctions involving the payment of fines; - management of payment receipts related to public and governmental services and fines; - management of payment bills related to services (generation of payment bills according to the algorithm, calculation of payment bill); - management of payments according to accounts payable; - interaction with the MPay service in order to generate and pay invoices; - reconciliation, settlement and reporting;

Government Platform IT Services

ICT capabilities that are characteristic of government services and are intended for common use by public authorities. They may also meet the needs of the MIA, in which case they are co-opted and treated as an integral part of the MIA's application architecture.

Full name of the architectural component	The role of the component in large-scale application architecture.	Key functionalities expected to be provided by the architecture component.

Cloud-based services provided on the common government technology platform (MCloud)[5]		
PaaS MPass	MPass is to be used for user authentication within MIA IIS applications.	MPass is used to control access to public systems hosted in the MCloud and provide authentication procedures via digital certificate and mobile identity
PaaS MSign	MSign is to be used to apply and validate the digital signature on official documents produced by MIA employees.	Key functionalities: - ensures signing of documents with electronic signature and verifying electronically signed documents; - provides the possibility to use all types of electronic signature officially recognized in Moldova in online interactions; - verifies the authenticity of signatures under guaranteed security conditions;
PaaS MLog	The platform service is intended for centralized recording and management of security events occurring in the applications, services and IT systems of the MIA.	MLog is used for logging all critical business events related to MIA IT systems. Functional specifications: - accessibility of the service via API interfaces and standard protocols (e.g. SOAP, JSON, SNMP); - definition of security event categories, possibility of default category assignment when logging events; - security event logging through integration with monitored systems and services; - processing of security events (filtering and correlation); - analysis of security events (generation of reports and views); - generation of security notifications and alarms (through own mechanisms and integration with the platform notification service); - automatic generation and sending of security event reports to predefined recipients;
PaaS MNotify	The platform service is to be used to send notifications and alerts from the MIA IIS to external beneficiaries, through all available channels (SMS, email, web, API, SNMP, etc.).	MNotify is used as a notification mechanism for all computer systems hosted in MCloud. Functional specifications: - sending notifications to designated recipients based on input parameters received from client applications. Notifications will be able to be sent via different channels including: SMS, email, web services, SNMP, etc.; - sending notifications based on events reported by client applications. The notifications application, based on the event information, will generate the content of the notifications, select the recipients and the channels to send the notifications; - integration with external services that provide notification delivery channels (email services, mobile operators, TETRA operator, other MAI applications that have functions for receiving notifications and communicating them to interested users);
PaaS MPay	Government platform service for managing public electronic payments.	MPay is a reusable and shared government platform-level service whose main purpose is to enable payment for any e-Service with any available payment instrument. MPay provides core functionality for: - Generating payment bills to a treasury account; - Making treasury payments by electronic means; - Tracking the settlement of the payment bill;
PaaS PDD	PDD (open data portal data.gov.md) is used for automatic publication of public data disseminated by the MIA	It is the government platform for publishing public datasets held by authorities. It is used by the MIA to publish statistical information by area of competence.
PaaS MConnect	MConnect is used to ensure interoperability with the information systems of the primary data providers for the AIS EAR via the MIA IIS	Ensures semantic and technical interoperability between MIA IIS and external automated information systems. Ensures the setup of and access to the National Semantic Catalogue.
MCabinet	MCabinet is used to view documents and other notifications/messages by participants in the contravention process	MCabinet offers the following functionalities: - displaying official information of public interest; - access by users to documented information about themselves exposed by data providers;

[5] In accordance with GD No 128 of 20.02.2014 on the common government technology platform (MCloud)

		- customization of information exposed by data providers, according to users' interest; - informing users about changes to the documented information about themselves; - guaranteed receipt of notifications sent by service providers via the government electronic notification service (MNotify) to users to notify them of events occurring in connection with the provision of services; - view information related to the provision of an electronic service, displayed by data providers; - access by users to electronic services via the Portal without the need for additional authentication in relation to systems whose information is accessed via the Portal; - transmission of the authenticated user's data to other state information systems for identification of the person and ensuring automated access, in order to exclude additional authentication
Mdoc	MDoc is a centralized platform for storing and sharing documents related to the process of providing public services or generated by public authorities. The e-Contravention Case Management System will use the MCabinet platform service to store documents for parties involved in the process that do not have a user account or do not use an interoperable system with the e-Contravention Case Management System	MDoc offers the following functionality: - centralized data repository containing all documents provided during the provision of public services; - generation of conditions for the creation and management of the electronic archive; - an efficient mechanism for automatic data exchange between the information systems with which MDoc will interact; - a standardized process for sharing documents generated as a result of the provision of public services; - digitization of the document sharing process for public authorities that do not have their own high-performance IT solutions; - reducing the costs of providing public services; - encouraging electronic exchange of documents between citizens and public institutions; - high performance management, configuration and dynamic development facilities
MPower	MPower is used to validate the powers of the reporting officer.	Ensures validation of the powers of the reporting officer
Application solutions owned by public authorities that can be used to create MIA IT services		
Official web pages.	The Government Platform Service is used to create the official websites of the MIA and subordinate subdivisions. Their role is to publish information of public interest for the MIA and its subdivisions on the Internet.	Functional specifications: - publishing information of public interest, in a form convenient for consumption by recipients; - convenient management of published information by information holders; - automatic publication of statistical information taken from the subdivision's internal systems; - the possibility for visitors to generate customized reports from large volumes of information available on the web page and export it in open format for further processing; - the possibility of automatic extraction of information of interest by third-party systems;
PSA electronic services	Government platform IT services provided by the Public Services Agency for MIA services provided through the one-stop shop. By integrating with PSA services, MIA subdivisions are to interact with service beneficiaries. The integration via MConnect with the "front end" applications within MIA that participate in the provision of services (WFMS, Billing, Notifications, etc.) will be ensured.	Functional specifications: - publication of the catalogue of MIA services; - integration of custom modules for each individual service; - end-to-end management of the service: request - communication - payment - service reception; - file management related to the service request (applicant authentication, virtual file creation, file management for the whole life cycle of the file; - access to the file only by the public service beneficiary; - submission of service requests and additional documents (request file); - correspondence with the public authority (actor: service beneficiary);

		- integration with the subdivision's internal workflow applications, where the internal workflows related to the public services provided are expected to be implemented. The subdivision's employees will exclusively use internal systems for the provision of services; - integration with the Billing platform application of the MIA, in order to take over the payment conditions related to the public services provided;
SRP FRS search	Person identification service in the SRP by facial image	Platform service offered by the Public Services Agency to identify the person by comparing the facial image taken with photographs from the State Register of Population
SIC AccesWeb	Application for accessing information from the State Register of Population and State Register of Transport, State Register of Law Units, State Register of Drivers	Key functions (content services): - Search for information about persons and their documents in the RSP, RSUD; - Search for information on means of transport in RST and drivers in RSCV; - Information on the status of foreigners in the country, crossing the state border (AccesWeb.Foreing)

Annex B

Requirements for the implementation of the e-Contravention Case Management System

This chapter sets out the requirements for the stages and deliverables of the e-Contravention Case Management System implementation project. The purpose of these requirements is to ensure that the Tenderer will deliver an IT solution that meets all the specifications set out and that its correct operation in the production environment will be confirmed to a reasonable level of certainty.

The requirements of this chapter are mandatory. The Tenderer shall specify under each of the requirements how it intends to ensure its implementation (if the requirement relates to measures planned after the contract has been signed) or provide the information requested (if the requirement is applicable to the submission stage). The offer must also contain relevant and sufficient information on the Tenderer's ability to meet the requirements set out in this chapter.

B.1. Conventions when formulating non-functional requirements

The requirements for the implementation of the e-Contravention Case Management System set out in this document are marked using the following convention:

- all requirements have a unique identifier consisting of two values X.Y, where X is the category of the requirement described in table B.1 and Y is the unique identifier of the requirement in the category to which it belongs.
- for each requirement, the mandatory nature is mentioned: M - mandatory requirement to be implemented, D - desirable requirement to be implemented, optional, and I - informative requirement.

Table B.1. Categories of requirements of the ToR

Value	Meaning	Interpretation
CSI	Requirement for implementation services	The requirement relates to services provided for the implementation of the e-Contravention Case Management System and the roll-out.
CPI	Post-implementation requirement	The requirement refers to the services for the post-implementation warranty and maintenance of the e-Contravention Case Management System.

B.2. General requirements regarding the implementation of the e-Contravention Case Management System

This section contains general requirements on the organization and execution of the project for the implementation of the e-Contravention Case Management System.

Table B.2. General requirements for implementation of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.1.	I	MIA opts for a strategy of implementing the e-Contravention Case Management System in small steps to increase the chance of success of the project and to facilitate the integration and use of the e-Contravention Case Management System into MIA activities. The approach for the organization of the e-Contravention Case Management System project preferred by MIA is expected to ensure: - The production of tangible results in the shortest possible time from the project launch. - The results produced, in particular the functional capabilities of the e-Contravention Case Management System, will start to be used by the MIA as they are implemented; - Knowledge transfer and training of the MIA's capabilities for installing, setting, using, operating, maintaining and adjusting the e-Contravention Case Management System will occur throughout the system implementation project.
CSI.2.	M	The project for the development and implementation of the e-Contravention Case Management System will last a maximum of 30 months from the date of signing the contract: • 18 months for design/development/implementation/piloting/training/launch into production • 12 months for warranty, maintenance and technical support
CSI.3.	M	The tenderer will describe in its offer the proposed approach (methodology) for the organization of the project for the implementation of the e-Contravention Case Management System. It will argue why the proposed approach (methodology) is the most suitable to support the implementation strategy of the e-Contravention Case Management System selected by the MIA, within the set deadline.
CSI.4.	M	The approach (methodology) proposed by the Tenderer for the organization of the e-Contravention Case Management System implementation project must be independent of the implementation of other applications and components of the future application architecture of MIA.
CSI.5.	M	The approach (methodology) proposed by the Tenderer must ultimately ensure the completion of the key milestones for the implementation of the e-Contravention Case Management System set out in Annex A and produce the deliverables requested in the Terms of Reference.

B.3. Requirements for project management

During the implementation project of the e-Contravention Case Management System solution, the project management activities will produce a set of deliverables that will have to be coordinated, agreed and signed by the MIA and will ensure the smooth running of the project activities.

B.3.1 General requirements

The general requirements for the organization of the project management framework for the implementation of the e-Contravention Case Management System are presented in Table B.3.

Table B.3. General organizational requirements for project management for the implementation of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.6.	M	The Provider is responsible for the management of the implementation project, according to th project plan and practices jointly agreed with the Beneficiary. The Provider is responsible for identifying and mobilizing the resources required to execute the activities in its area of responsibility set out in the project management plan to the agreed quality level.
CSI.7.	I	The Beneficiary is responsible for all procedures and administrative aspects related to the initiation, launch and running of the project, the organization of the internal project team, the preparation of the ICT environment necessary for the implementation of the e-Contravention Case Management System.
CSI.8.	M	The project will be managed with the application of iterative and incremental methodologies according to the development approach described in chapter 4.
CSI.9.	M	The tenderer shall include in its bid the draft Project Management Plan (PMP). The PMP is a comprehensive document that provides a detailed vision of how the project will be planned executed, monitored and controlled and serves as a reference document for all parties involved in the project The document will explicitly mention at least the following: - Implementation approach, - Statement of Work, Objectives and Expected Results - Project management organization chart, including: project steering committee, roles for project team members on the Provider side, roles for project team members on the MIA side. For each role the key tasks in the project (RACI matrix) will be established. The requirements for team members described in chapter 9 will also be considered in this respect; - Communication plan including: communication methods, communication channels, frequency of communication (what, when, how, to whom), responsibilities, escalation mechanism, confidentiality and data security rules, etc. procedures and special situations. - Practices applied to project interaction and collaboration, including: project plan management, detailed planning of activities based on prioritized requirements, resource management, change management, risk management, deliverable quality management, progress monitoring and reporting, exception management, project library management. - Change Control Procedures and Approval procedures that indicate: how changes to the project will be managed and approved and who is responsible for approving them
CSI.10	M	MIA and the Provider will each appoint a project manager, who will report to the project teams from MIA and the Provider respectively.
CSI.11	M	The Provider's project manager will have the necessary authority for the execution of the project activities and will bear primary responsibility for the production and presentation of deliverables in accordance with the established terms and quality criteria.

ID	Compulsoriness	Requirement
CSI.12	M	In case the Provider is represented by an association or subcontracts another company to participate in the execution of the project, the roles and responsibilities of each member of the association/subcontractor shall be clearly specified.
CSI.13	I	MIA may contract external consultants to whom part of MIA's project management functions and the quality assurance function for the whole project will be delegated.
CSI.14	D	The Provider will demonstrate the maturity of the practices applied to the implementation of the e-Contravention Case Management System by presenting relevant conformity certificates (*e.g.: ISO 9001, ISO 20000, ISO 27001 etc.*).

B.3.2 Requirements for project management activities

The requirements for the project management activities for the implementation of the e-Contravention Case Management System are presented in Table B.4.

Table B.4. Requirements for key project management activities

ID	Compulsoriness	Requirement
CSI.15.	M	For the management of the project the Provider will perform at least the following activities: • Preparation and agreement with MIA of the Project Management Plan (PMP) document. The PMP is expected to be developed in stages. The initial draft, presented at the inception stage of the project, coordinated in principle with the Beneficiary, is to be developed and signed in full form by the end of the "analysis and product definition" stage; • Preparation and agreement with MIA of the Project Plan as part of the PMP; • Definition of the solution back-log; • Elaboration of detailed activity plans - sprint planning; • Coordination of activities according to detailed activity plans; • Keeping project management records throughout the project. Mandatory registers: deliverables register, risk register, change register, communication register, events register; • Progress reporting on the project according to the Project Management Plan; • Organization of project management meetings according to the agreed communication plan; • Presenting end of sprint reports and supporting presentations in project management meetings at the end of stages; • Closing the main project stages and submitting acceptance documents to MIA; • Placing all project management deliverables in the project library.

B.3.3 Requirements for project management deliverables

The requirements for the deliverables resulting from the project management activities are presented in Table B.5.

Table B.5. Requirements for project management deliverables

ID	Compulsoriness	Requirement
CSI.16.	M	All communication and deliverables within the project management activities will be in Romanian.
CSI.17.	M	For the project initiation stage, the Provider shall deliver at least the following deliverables: - Draft Project Management Plan coordinated and signed by the Beneficiary; - Initial Project Plan including Work Schedule, Stakeholder Engagement Plan, Change Management Plan and Risk Management Plan;
CSI.18.	M	During project implementation, the Provider will deliver at least the following deliverables related to project management: • Updated Project Initiation Plan document; • Coordinated Project Management Plan and amendments thereto; signed by the Beneficiary. • Project Plan Updates; • Detailed activity plans per project for each sprint, stage; • Project progress reports and project logs maintained and updated as per the Project Management Plan. • Stage Completion Reports which will contain at least the following information: overview of the completed stage, presentation of the project plan for the next period, update of the register for risk analysis project problem setting, progress registration and project quality level record. • Exception reports, which will contain at least: description of causes of deviations in the project, impact produced, proposed solutions for resolution and overall impact on the project, options recommended by the Project Manager or Provider.
CSI.19.	M	Project management deliverables presented at the final acceptance stage: - Project Closure Report: summarizing the entire project, including achievements, lessons learned, problems encountered and any recommendations for future projects - Requirements Traceability Matrix - Acceptance Test Plan - Project Closure Checklist which ensures that all activities required for project closure have been completed and all deliverables are submitted. - Lessons learned

B.3.4 Acceptance criteria for project management deliverables

The acceptance criteria for deliverables resulting from project management activities are set out in Table B.6.

Table B.6. Acceptance criteria for deliverables of project management activities

ID	Compulsoriness	Requirement
CSI.20.	M	Deliverables resulting from project management activities will be accepted if: • the deliverables are submitted within the time agreed by the Beneficiary and the Buyer of the project. • the Beneficiary has no comments on the completeness and correctnes of the deliverables. • the deliverable is accepted by the Buyer of the project

B.4. Stagess of the e-Contravention Case Management System implementation project

The stages listed in this section are for information purposes only. The activities mentioned within each stage represent minimum requirements. The deliverables indicated and the acceptance criteria of the deliverables are mandatory. As per the requirements in Section 4, MIA encourages the Tenderer to propose its approach for the implementation of the e-Contravention Case Management System.

The Tenderer shall specify in the offer the implementation stages and deliverables produced. For each stage, the objectives, key activities, responsible persons and tools used to perform the activities will be defined.

B.4.1 Product analysis and definition stage (product backlog):

This compartment contains the requirements for the key activities of the analysis and product definition stage in the development and implementation processes of the e-Contravention Case Management System.

Key activities:

Table B.7 contains the requirements for the key activities of the analysis and product definition stage.

Table B.7. Requirements for key activities of the product analysis and definition stage

ID	Compulsoriness	Requirement
CSI.21.	M	The provider will validate the business needs for the e-Contravention Case Management System during the business analysis stage and develop the solution backlog - the total list of tasks to be solved. For this purpose, the Provider will perform the following activities: • Validation of the correct understanding of Project Requirements and Objectives: Clarifying and understanding the overall project objectives and requirements is the first step. This involves working closely with the Beneficiary, stakeholders and team members to establish the correct direction. • Review the stakeholder list, specified in Annex A, in order to ensure that the interests of all stakeholders will be considered when developing the product and obtaining confirmation of their commitment to participate in the project. • Define the High Level Product Vision (HLD) aligned with the ICT architecture concept of the MIA and the requirements of the e-Contravention Case Management System solution described in the ToR. This should include a description of the value and benefits that the product brings to customers or end users. The vision should provide a clear direction for the entire project. Similarly, the HLD document should include a description of the proposed system architecture, implementation specifics of the presentation layer, application layer, data layer and technology layer, creating prototype input forms (form design). Using solutions such as Figma is considered an advantage, - Definition of input/output forms and documents. - Decomposition of Requirements into Smaller Elements: Backlog tasks should be defined in a way that facilitates their management and implementation. Breaking down complex requirements into smaller, manageable and independent elements helps to clarify individual tasks. - Organization of workshop sessions between the MIA and the Provider on the subject of backlog definition and prioritization; - Prioritization of tasks. Priorities are set by the Beneficiary. The Provider, using specialized methods such as MoSCoW (Must have, Should have, Could have, Won't have) or/and other relevant factors will advise the Beneficiary on the order of implementation of the requirements, so that tasks with hig value and significant impact are placed at the top of the backlog for consideration as soon as possible. - Estimation of Effort: Each task must be evaluated in terms of the effort required to complete it. Estimation can be done by applying techniques such as Planning Poker or by using units of measurement such as effort points. - Adding Descriptive Details: Each task must be accompanied by clear and descriptive information. This may include details of functional requirements, acceptance criteria, design references or any other relevant information.

ID	Compulsoriness	Requirement
		- Assignment of Responsibilities: Each task must have a clear person responsible. In case of need for involvement/allocation of resources from the Beneficiary, these will be stated in advance and justified. The assignment of responsibilities helps to clarify who is responsible for carryin out the work. - Review. Defining the requirements for the ICT infrastructure (software, hardware and network) in order to establish requirements for development, testing and production environments. Provider will argue the requirements for hardware, software, where applicable licenses proposed for these 3 environments; - Update the Project Management Plan, coordinate and sign the final version with the Beneficiary. - The work will be executed through interviews of responsible persons in the business and IT subdivisions, and analysis of relevant documentation.

Deliverables

Table B.8 contains the deliverable requirements for the product analysis and definition stage.

Table B.8. Requirements for deliverables of the product analysis and definition stage

ID	Compulsoriness	Requirement
CSI.22.	M	As a result of the business analysis, the Provider will deliver as a deliverable: 1. A high level vision document (HLD) of the future product; 2. A document describing the ToBe model of the processes subject to digitization including: data architecture (data source analysis and entity-relationship model), BPMN diagrams, RACI analysis, state diagrams and CRUD matrix, security model and role management, output document templates 3. A document including the total list of tasks to be solved - the product backlog, with the prioritized tasks 4. A document describing the infrastructure of the development, test and production environments that the Beneficiary must provide to the Provider; 5. Updated Project Management Plan.
CSI.23.	I	Based on the refined SRS (Software Requirements Specification), MIA may accept adjustments to the functional and non-functional specifications according to the terms of reference.

Acceptance criteria for deliverables:

Table B.9 contains the requirements for deliverable acceptance criteria for the product analysis and definition stage.

Table B.9. Requirements for acceptance criteria for deliverables of the product analysis and definition stage

ID	Compulsoriness	Requirement
CSI.24.	M	Acceptance of the deliverables of the analysis stage of the project will be carried out according to the following criteria: • the deliverables are submitted to the Beneficiary and Buyer of the product; • the Beneficiary and Buyer have no comments on the completeness and correctness of the deliverables; • the acceptance of the deliverables is signed by the Provider, Beneficiary and Buyer of the product.

B.4.2 Product iterative and incremental development stage:

B.4.2.1. Sub-stage: Sprint planning

The given compartment contains the requirements for the activities and deliverables of the product iterative and incremental development stage and sprint planning sub-stage, performed according to the Agile approach to the development of the e-Contravention Case Management System.

Key activities

Table B.10 contains the requirements for the key activities of the sprint planning sub-stage:

Table B.10. Requirements for key activities of the sprint planning sub-stage

ID	Compulsoriness	Requirement
CSI.25.	I	At this stage the provider will select priority requirements from the product backlog, set targets for each sprint and estimate the effort required to implement them. At the beginning of each sprint, the most important items that fit into a sprint are selected and a sprint backlog is created from them. The items in this sprint backlog are further detailed by the Provider, coordinated with the Beneficiary to approve the implementation model and distributed to the developers for implementation.
CSI.26.	M	At this stage the provider will at least perform the following: • Setting the sprint backlog - The provider reviews the product backlog and identifies which requirements are priorities for the current sprint. This involves assessing the value of each requirement and considering technical dependencies and constraints. • Presenting sprint objectives - The provider shares with the customer the planned objectives for the current sprint. This includes a discussion of the requirements and functionality the team intends to deliver during the sprint. The provider and the beneficiary jointly set delivery targets for the end of the sprint. • Task detailing and coordination: The selected requirements are further detailed by the Provider. Detailed tasks should be clear and specific enough to assign to team members and allow them to estimate the

		effort required to complete them. Each detailed task is described and coordinated with the Beneficiary. • Participating in the Estimation Session: The Beneficiary will be invited to participate in the session to estimate the effort and resources required for each requirement. This provides transparency and shared understanding of the effort required to implement the requirements. • Approving the sprint plan: the Beneficiary will be proposed for approva the final sprint plan, including requirements, priorities and delivery targets. This confirms that the beneficiary agrees with the proposed direction and plan for the sprint and expresses confidence in the provider's ability to deliver the agreed values.
CSI.27.	M	Resolving debates and problems: During the sprint planning process, disagreements or problems may arise. Provider and beneficiary work together to resolve them and reach consensus. This may include clarifying requirements, adjusting priorities or identifying and managing risks. All disagreements and consensus agreement are documented. If members of the Provider and Beneficiary project teams cannot reach consensus on an issue it is reported to the Project Steering Committee.
CSI.28.	I	The Provider forms the sprint backlog. The sprint backlog does not change during the sprint process.

Deliverables

Table B.11 contains the deliverable requirements for the sprint planning sub-stage:

Table 0.11. Requirements for deliverables of the sprint planning sub-stage

ID	Compulsoriness	Requirement
CSI.29.	M	As a result of the sprint planning, the following will be delivered: • Sprint Plan: This is a document containing details of the sprint objectives, selected requirements, set priorities, effort and resource estimates, task schedule and any other relevant information related to the sprint.

Acceptance criteria for deliverables

Table B.12. contains the requirements for the acceptance criteria for deliverables of the sprint planning sub-stage:

Table B.12. Requirements for acceptance criteria for deliverables of the sprint planning sub-stage

ID	Compulsoriness	Requirement
CSI.30.	M	Acceptance of the deliverables of the analysis sub-stage of the project will be carried out according to the following criteria: • the deliverables are submitted to MIA and Buyer of the product; • MIA and Buyer of the product have no comments on the completenes and correctness of the deliverables;

B.4.2.2. Sprint execution sub-stage:

The given compartment contains the requirements for the activities and deliverables of the sprint execution sub-stage for development/configuration of the e-Contravention Case Management System.

Key activities

Table B.13 contains the requirements for the key activities of the sprint execution stage.

Table B.13. Requirements for key activities of the development sub-stage (sprint execution)

ID	Compulsoriness	Requirement
CSI.31.	M	At this stage the provider will configure and adjust (in case of developed solutions or universal platforms used) or develop and configure (in case of development from scratch of the IT system) the e-Contravention Case Management System, according to the specifications of the tasks included in the sprint backlog. Depending on the tasks performed in the sprint, the provider will perform the following activities: • installation of the production, testing, training environments of the e-Contravention Case Management System (Operating System/SGBD/applications, etc.); • development, deployment and configuration of the e-Contravention Case Management System according to the specifications of the tasks included in the backlog of the sprint; • internal testing of the developed components; • testing with the beneficiary of the developed components; • deployment of the e-Contravention Case Management System components in the prepared operating environments.
CSI.32.	M	Each sprint ends with a functional product, which is submitted to the Beneficiary for acceptance on the last day(s) of the sprint. The functional product shall meet the agreed criteria.
CSI.33.	M	The Provider will ensure the testing together with the Beneficiary's team of the delivered functional components. For this purpose, the Provider will delive the following test scenarios: • unit testing; • integration testing; • stress testing; • load testing • performance testing
CSI.34.	M	At the end of each sprint, the Provider shall perform a retrospective analysis of the sprint. Based on the objections and additional requirements formulated by the Beneficiary, after coordination with the Beneficiary, the product backlog is completed.

		As the introduction of new requirements/features/tasks may influence the order of priorities, each time the backlog is modified it will be coordinated with the Beneficiary.

Deliverables

Table B.14 contains the deliverable requirements for the sprint execution sub-stage.

Table B.14. Requirements for the deliverables of the sprint execution sub-stage

ID	Compulsoriness	Requirement
CSI.35.	M	The provider will develop and configure the components of the e-Contravention Case Management System according to the functional and non-functional specifications in: • production environment; • test environment; • training environment.
CSI.36.	M	The provider will prepare and deliver complete technical documentation related to the implemented components. Where appropriate, the Provider will update the High Level Vision Document (HLD) and the document describing the ToBe model of the processes subject to digitization
CSI.37.	M	The Provider will deliver the source code of the developed/implemented e-Contravention Case Management System components within the sprint;
CSI.38.	M	The Provider will deliver the test scenarios and perform the testing of the e-Contravention Case Management System components: • unit testing; • integration testing; • stress testing; • load testing • performance testing
CSI.39.	M	Revision of the product backlog in case of addition of new requirements/functionality/characteristics.
CSI.40.	M	Submission of project progress reports and project registers maintained and updated according to the Project Management Plan

Acceptance criteria for deliverables

Table B.15 contains the requirements for the deliverable acceptance criteria of the sprint execution sub-stage.

Table B.15. Requirements for acceptance criteria for deliverables of the sprint execution sub-stage

ID	Compulsoriness	Requirement
CSI.41.	M	Components of the e-Contravention Case Management System are implemented and configured according to functional and non-functional specifications in the following environments: • production environment; • test environment; • training environment.
CSI.42.	M	The complete technical documentation related to the implemented components of the e-Contravention Case Management System is delivered
CSI.43.	M	The Beneficiary and the Buyer of the product have no comments or objections regarding the quality of the deliverables.
CSI.44.	M	The act of acceptance of the deliverables of the development/configuration stage is signed by the Provider, Beneficiary and Buyer of the product.

B.4.3 Data population stage:

The given compartment contains the requirements for the activities and deliverables of the initial data populate stage and the migration of data from the AIS REC and AIS RAR to the e-Contravention Case Management System

Key activities

Table B.16 contains the requirements for the key activities of the initial data population and data migration stage:

Table B.16. Requirements for key activities of the data population stage

ID	Compulsoriness	Requirement
CSI.45.	D	The provider will include in the technical offer detailed information on the proposed approach, method and tools for performing the initial data populating and data migration from existing systems into the e-Contravention Case Management System
CSI.46.	I	MIA will prepare the data sets required for the initial data population of the e-Contravention Case Management System, within the limits of the existing data. The format of the data will be mutually agreed.
CSI.47.	M	The tenderer will ensure the migration of all data sets into the e-Contravention Case Management System and at the level of detail requested by the MIA. As a minimum, the migration of data from the AIS REC and the AIS RAR to the e-Contravention Case Management System will be ensured.
CSI.48.	M	In the process of populating the e-Contravention Case Management System with data, the Provider will be responsible for: • establishing the methodology applied to the initial data population; • developing detailed plans for initial data population; • providing the software tools to be used for the initial data population;

ID	Compulsoriness	Requirement
		• establishing the quality rules for the preparation of the data sets for the initial data population and their implementation in the tools used i the process; • mapping the data made available by the MIA to the data structures of the e-Contravention Case Management System; • establishing data reconciliation criteria; • participating in data cleaning and enrichment activities; • checking and validating the quality of the import data sets; • importing the prepared data into the e-Contravention Case Management System; • identifying exceptions and errors when importing data.
CSI.49.	M	The provider will propose to the MIA the methodology for populating the initial data. The methodology must contain at least the following elements: • how the data will be prepared; • how to map the data structures; • how to clean the data and ensure data quality; • how to complete the types of data or attributes required by the e-Contravention Case Management System and which are missing in the data sets held by the MIA; • how to import the data; • how to reconcile migrated data; • the recovery plan (at each key step in the migration process); • the release to production plan.
CSI.50.	M	The provider will prepare and propose to the MIA the detailed plans for data population. The detailed plans will be aligned with the implementation plan of the e-Contravention Case Management System.
CSI.51.	M	The provider will provide specialized software tools such as ETL (Extract Transform Load) to be used in the data population process and will provide full documentation for the use of these tools, ensuring the training of the responsible persons from the MIA to use these tools.
CSI.52.	M	All activities related to data population will be carried out in operating environments controlled by MIA, located in the local MIA network. The data will never leave the MIA information system.
CSI.53.	M	In the data population process, the Provider undertakes to adhere to the security policies and standards approved and applied by MIA.

Deliverables

Table B.17 contains the requirements for the deliverables of the population and data migration staged.

Table B.17. Requirements for data population stage deliverables

ID	Compulsoriness	Requirement
CSI.54.	M	The provider will develop and deliver the Methodology to populate with data the e-Contravention Case Management System.
CSI.55.	M	The provider will develop and deliver the Plan to populate with initial data the e-Contravention Case Management System.
CSI.56.	M	The provider will develop and deliver the Plan to migrate data from AIS REC and AIS RAR to e-Contravention Case Management System.
CSI.57.	M	The provider will deliver the data migration/population scripts or/and ETL tooling operating configuration procedures
CSI.58.	M	All relevant data sets held by MIA must be fully and correctly populated in the e-Contravention Case Management System.
CSI.59.	M	The provider will deliver the updated semantic catalogue of the date of the e-Contravention Case Management System

Acceptance criteria for deliverables

Table B.18 contains the requirements for the deliverable acceptance criteria of the data population and migration stage.

Table B.18. Requirements for acceptance criteria for deliverables of the data population stage

ID	Compulsoriness	Requirement
CSI.60.	M	The Strategy and the Plan for Data Population are delivered and accepted by the Beneficiary.
CSI.61.	M	All data provided by the MIA, as required by the mutually agreed migration plan, are fully and correctly migrated into the e-Contravention Case Management System.
CSI.62.	M	The act of acceptance of the deliverables of the data migration stage in the e-Contravention Case Management System is signed by the Provider, Beneficiary and Buyer of the product.

B.4.4 Acceptance testing stage:

The given compartment contains the requirements for the key activities in the acceptance testing of the e-Contravention Case Management System.

Key activities

Table B.19 contains the requirements for key activities in the acceptance testing stage.

Table B.19. Requirements for key activities of the acceptance testing stage

ID	Compulsoriness	Requirement
CSI.63.	M	At this stage all components of the e-Contravention Case Management System are implemented and configured according to the functional and non-functional specifications.

ID	Compulsoriness	Requirement
		The e-Contravention Case Management System is available and operational in all environments where it has been implemented. The provider will organize acceptance testing of the system. For this purpose, it shall perform at least the following activities: • definition of the test strategy and test procedure; • - preparation of detailed test plans, including test scenarios; • - receiving detected errors and removing them; • - preparing the final test results plan, including the status of all identified errors.
CSI.64.	M	Unit test coverage for the e-Contravention Case Management System capabilities will be a minimum of 90%.

Deliverables

Table 8.20 contains requirements for deliverables of the acceptance testing stage.

Table B.20. Requirements for deliverables of the stage for acceptance testing of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.65.	M	The provider will deliver the acceptance test plan to MIA for coordination and acceptance;
CSI.66.	M	The provider will deliver for coordination and acceptance to MIA the test scenarios for all test categories (unit testing, integration testing, stress testing, load testing, *etc.*).
CSI.67.	M	The provider will deliver for coordination and acceptance to MIA the report on the testing results of the e-Contravention Case Management System.

Acceptance criteria for deliverables

Table B.21 contains the requirements for the acceptance criteria of the deliverables of the acceptance testing stage of the e-Contravention Case Management System.

Table B.21. Requirements for the acceptance criteria of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.68.	M	The provider will perform all planned tests according to the Test Plan and their final results are acceptable to e-Contravention Case Management System.
CSI.69.	M	Acceptance of deliverables will be made if zero critical non-conformances and less than 3 major non-conformances are found.
CSI.70.	M	Acceptance will be dated the day all non-conformities discovered at delivery ar rectified.
CSI.71.	M	The acceptance act of the e-Contravention Case Management System is signed by the Provider, Beneficiary and Buyer of the product.

B.4.5 Training and documentation stage:

The given compartment contains the constraints, activities, deliverables and acceptance criteria of the deliverables related to the training activities on the use of the e-Contravention Case Management System.

Start-up constraints

Table B.22 contains the totality of the constraints required to train MIA staff in the use of the e-Contravention Case Management System.

Table B.22. Requirements for the start-up constraints for training in the use of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.72.	I	The beneficiary will provide all the necessary facilities to organize the training o the MIA users in the operation of the e-Contravention Case Management System: • training room; • workstations with network connection;

		• technical equipment necessary for training;
CSI.73.	M	The provider will provide: • prepared training (testing) environment; • training support materials (in Romanian); • tests to verify the effectiveness of the training (in Romanian).

Key activities

Table B.23 contains the requirements for the key activities of the training and documentation stage.

Table B.23. Requirements for key activities of the training and documentation stage

ID	Compulsoriness	Requirement
CSI.74.	M	The provider will develop and deliver training programs for all categories of MIA users.
CSI.75.	M	The provider will agree with MIA the plan for the organization of training sessions.
CSI.76.	M	The provider will carry out the training of users according to the plan and the training programs jointly agreed with MIA. The training will be conducted in Romanian.
CSI.77.	M	The provider will train a target group of users - trainers who will provide support and continue the training after the production of the e-Contravention Case Management System
CSI.78.	M	The provider will prepare and deliver a draft for the Continuity (maintenance) Plan for the e-Contravention Case Management System. This will cover at least the following: - Risk and impact assessment: Identify potential threats that may affect the operation of the software solution and assess the impact of these threats on the business continuity of the beneficiary. - Define continuity objectives and KPIs: Establish recovery objectives such as maximum tolerated recovery time (MTR) and recovery point of failure (RPO). - Backup and recovery plan: A detailed plan for backing up data and software code; procedures for restoring them if necessary; and procedures for periodically testing backups. - Backup Infrastructure: A description of the backup infrastructure and resources required to ensure continuity of processes and/or restore the software solution to operation in a disaster recovery environment. - Communication and coordination: Definition of clear procedures for communication and coordination of efforts in the event of an incident. - Recovery procedures: Detailed, step-by-step procedures for restoring data, applications and infrastructure according to established objectives and testing their functionality. - Definition of roles and requirements for specialists involved in systems maintenance and recovery

		- Continuity plan testing: plan for conducting periodic tests, responsible parties, objectives and content of the tests. - Staff testing and training requirements: Ensures that staff are trained and prepared to implement the continuity plan in an efficient and effective manner in the event of a real incident. - Continuous review requirements for the continuity plan - When drafting the Continuity Plan, the requirements for support and maintenance services and service levels described in Annex C will be taken into account
CSI.79.	M	- The Provider will organize and conduct a test of the proposed continuity plan with the participation of the responsible persons from the Beneficiary.

Deliverables

Table B.24 contains the requirements for the deliverables of the training and documentation stage.

Table B.24. Requirements for deliverables of the training and documentation stage

ID	Compulsoriness	Requirement
CSI.80.	M	The training and documentation stage involves providing the following categories of deliverables: • training on the business use of the e-Contravention Case Management System (non-administrator role users); • training on the administration and configuration of the e-Contraventio Case Management System (users with administrator role); • comprehensive guides for all categories of users of the e-Contraventio Case Management System for the operation and administration of the e-Contravention Case Management System.
CSI.81.	M	The provider shall prepare and deliver the following supporting documents to the e-Contravention Case Management System: - Technical Architecture Document (TDD) of the e-Contravention Case Management System; - Database Architecture Document including ERD (Entity-relationship diagram) and CRUD matrix for data categories/information objects. - Document describing digitized business processes, including: BPMN diagrams, state diagram, RACI matrix, etc. - API (Application Programming Interface) documentation; - SDK (Software Development Kit) for custom developed and other open source delivered application components; - Security documentation of the e-Contravention Case Management System.
CSI.82.	M	The provider will prepare and deliver the following categories of operational instructions of the e-Contravention Case Management System: • the administration guide for the e-Contravention Case Management System; • the users' guide of the e-Contravention Case Management System;

ID	Compulsoriness	Requirement
		• the installation guide for the e-Contravention Case Management System; • the guide for the configuration and operational maintenance of all components of the e-Contravention Case Management System; • developer guides, within the limit of the components allowed for internal development on the MIA side; • Use Manual for Help Desk service • Guides for backup and restoration of data in the e-Contravention Case Management System; • Documentation of the process of archiving and restoring data from the archive of the e-Contravention Case Management System.
CSI.83.	M	The guides must be comprehensive, detailed and up-to-date for all user groups
CSI.84.	M	The guides for non-administrative users will be in Romanian.
CSI.85.	D	The presence of guides also in Russian will be considered an advantage.
CSI.86.	M	The provider will deliver the guides in electronic format. The guides should be easy to access and navigate and the information needed should be easy to identify.
CSI.87.	M	The provider will deliver the source code related to the custom developments done for the e-Contravention Case Management System. The source code will contain sufficient comments to be understood by MIA employees.
CSI.88.		The provider will deliver the Register of suggestions/requests for improvement of the e-Contravention Case Management System received during the training period.
CSI.89.	M	A draft document for the "e-Contravention Case Management Sytem Continuity (Maintenance) Plan" including: - Business Continuity Plan, - Disaster Recovery Plan, - Backup Plan - Other relevant information security procedures in accordance with national legislation and industry best practices.
CSI.90.	M	Following the testing of the Continuity Plan (maintenance) of the e-Contravention Case Management System, the Provider will prepare a repor that includes the identified problems and proposals for process improvement.

Acceptance criteria

Table B.25 contains the requirements for the acceptance criteria of the deliverables of the training and documentation stage of the e-Contravention Case Management System.

Table B.25. Requirements for acceptance criteria for deliverables of the training and documentation stage

ID	Compulsoriness	Requirement
CSI.91.	M	The provider must carry out all training sessions according to the Plan agreed upon with the Beneficiary.
CSI.92.	M	The documentation of the e-Contravention Case Management System must be complete and delivered in the form requested by the Beneficiary.
CSI.93.	M	The source code for custom developments made to the e-Contravention Case Management System shall be delivered.
CSI.94.	M	The act(s) of acceptance of the training and documentation must be signed by the Provider, Beneficiary and the Buyer of the product.
CSI.95.	M	Draft Continuity Plan for the e-Contravention Case Management System and test report accepted and signed by the Beneficiary

B.4.6 Launch into production stage:

The given compartment contains the requirements for activities, deliverables, and acceptance criteria for deliverables of the production launch stage of the e-Contravention Case Management System

Key activities

Table B.26 contains the requirements for the key activities for production release of the e-Contravention Case Management System.

Table B.26. Requirements for key activities of the launch into production stage

ID	Compulsoriness	Requirement
CSI.96.	M	The provider will propose its approach for the production roll-out of the e-Contravention Case Management System (e.g. sequential, big-bang, paralle run, pilot) and justify this approach.
CSI.97.	M	The provider will participate in all stages of the production roll-out of the e-Contravention Case Management System. To this end, the Provider shall perform at least the following actions: • will develop the Production Release Plan (cut-over plan); • will develop the roll-back plan (where applicable); • will update the datasets that have been generated/modified in the current systems after the execution of the initial data population procedure; • will support the execution of the Production Release Plan; • will operationally remove errors and malfunctions in the operation of the e-Contravention Case Management System

Deliverables

Table 8.27 contains the requirements for launching into production the e-Contravention Case Management System.

Table B.27. Requirements for the deliverables of the production launch stage of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.98.	M	The provider will refine and coordinate with the MIA the plan for the production launch of the e-Contravention Case Management System.
CSI.99.	M	The e-Contravention Case Management System is launched in production.

Acceptance criteria

Table B.28. contains the requirements for the acceptance criteria of the deliverables of the production launch stage of the e-Contravention Case Management System.

Table B.28. Requirements for acceptance criteria for deliverables of the launch in production of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.100.	M	The system is available and functional for all authorized users of the Beneficiary
CSI.101.	M	The act of acceptance into production of the e-Contravention Case Management System is signed by the Provider, Beneficiary and the Buyer o the product.

B.4.7 Production testing stage of the e-Contravention Case Management System

The given section contains the requirements for the production testing stage of the e-Contravention Case Management System. Table B.29 contains the requirements for the production test period of the e-Contravention Case Management System.

Table B.29 ~~30.~~ Requirements for the production test period of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.102.	M	The provider will provide on-site support for a period of at least ~~6~~ 4 months after the release to fix errors and deficiencies in the operation of the e-Contravention Case Management System. During this period the e-Contravention Case Management System shall be considered as tested in production
CSI.103.	M	During the production testing period of the e-Contravention Case Management System, the Provider shall perform development activities to remove errors and deficiencies, analyze logging records to prevent possible problems, make adjustments to the user interface and critical modules of the e-Contravention Case Management System.

B.4.8 Final acceptance stage of the e-Contravention Case Management System

The given compartment contains the requirements for the final acceptance of the e-Contravention Case Management System. Table B.30 contains the requirements for the final acceptance of the e-Contravention Case Management System.

Table B.30 ~~29~~. Requirements for final acceptance of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CSI.104.	M	Final acceptance of the implementation of the e-Contravention Case Management System will be recorded on the basis of the Final Acceptance Act signed by the Provider, the Beneficiary and the Buyer of the product, provided the following conditions are met: • the production test period has expired; • all errors, deficiencies and problems of severity 1 are removed; • there are less than 10 errors and problems of severity 2 not removed. • no test scenario will corrupt data integrity
CSI.105.	M	An error or problem related to the e-Contravention Case Management System is considered of severity 1 if it blocks or makes it difficult to use key functionalities of the information system. An error or problem related to the e-Contravention Case Management System is considered to be of severity 2 if it blocks or makes difficult the use of functionalities for which workarounds are available.

Annex C

Requirements for warranty, maintenance and post-implementation support

The purpose of the post-implementation support and maintenance services of the e-Contravention Case Management System is to ensure the following objectives for the MIA:

- The functionality provided by the system will be aligned over time to the changing business needs of MIA;
- Incidents and problems arising in the process of operating the e-Contravention Case Management System will be addressed and resolved in a timely manner, with minimal impact on MIA's activity;
- Difficulties in the operation of the e-Contravention Case Management System will be overcome correctly and in a timely manner, without affecting the functioning of the IT system.

In order to achieve these objectives, post-implementation support and maintenance services are to be provided by the Provider according to the requirements set out in this ToR.

The Provider must describe the activities it will carry out to meet these requirements, providing sufficiently detailed information on how it intends to perform the required services to the required level, as well as information on its technical, organizational and competence capabilities, confirming its ability to perform to the required level.

MIA expects the offer for post-implementation support and maintenance services to be based on best practices in project management and IT service management (*e.g.: ISO 20000, ITIL etc.*).

C.1. General requirements for warranty, maintenance and post-implementation support

The given compartment contains the general requirements of the warranty, maintenance and post-implementation support processes of the e-Contravention Case Management System. Table 9.1 contains all the general requirements for the warranty, maintenance and post-implementation support of the e-Contravention Case Management System.

Table 9.1. General warranty, maintenance and support requirements

ID	Compulsoriness	Requirement
CPI.1.	M	As part of the initial contract for the delivery and implementation of the e-Contravention Case Management System, the Provider will provide warranty, maintenance and support services for the applications of the provided IT system for a term of 12 months from the date of final acceptance of the IT system.
CPI.2.	M	The initial contract price for the development and implementation of e-Contravention Case Management System will include all post-implementation support and maintenance services except development services.
CPI.3.	M	The price of the initial contract for the development and implementation of the e-Contravention Case Management System will also include the provision

ID	Compulsoriness	Requirement
		by the provider, at the request of the Beneficiary, of 100 man-days of development services as defined in these Terms of Reference.
CPI.4.	M	All malfunctions of the e-Contravention Case Management System detected during the warranty period will be remedied at the Provider's expense (these activities will not be considered development activities and will not be included in the 100 man-days dedicated to development during the warranty, support and maintenance period).
CPI.5.	M	After one year of providing warranty, maintenance and post-implementation support services, MIA may request an extension of service provision. The Provider is obliged to accept the subsequent provision of services, for at least 5 years, under the conditions resulting from these Terms of Reference and the Provider's offer (e.g. service level, service price, *etc.*).

C.2. Post-implementation support and maintenance service specifications

This section defines the types of post-implementation support and maintenance services required. Any subsequent reference to these terms shall have the meaning given in this section. It also sets out the MIA requirements for each type of service.

C.2.1 Support services for the e-Contravention Case Management System during the warranty period

The support services are provided by the Provider in order to overcome incidents caused as a result of the operation of the e-Contravention Case Management System, in order to solve problems detected during the operation of the e-Contravention Case Management System and in order to ensure the correct and efficient use of the e-Contravention Case Management System by the MIA.

An incident related to the e-Contravention Case Management System is any event that has affected or could have affected the normal functioning of the computer system. A problem related to the e-Contravention Case Management System is a cause that has led or may lead to the occurrence of an incident.

A consultancy request is a request from the MIA to the Provider for advisory support in the use, configuration and maintenance of the e-Contravention Case Management System.

The support services are intended to ensure the timely use of the e-Contravention Case Management System within the quality parameters required by the MIA. The quality parameters for the functioning of the System are:

- **Availability -** the ability of the information system and its components to receive queries from authorized entities and to respond to these queries in a timely manner;
- **Usability -** the ability of the information system to function correctly, delivering the expected services to users and authorized entities;
- **Performance -** the ability of the IT system to respond to legitimate queries within set parameters;
- **Security -** the ability of the information system to ensure the confidentiality, integrity and availability of stored and managed data.

This section sets out the requirements for support services using the above terminology. Table 9.2 contains the requirements for the support services to be provided by the Provider during the warranty period.

Table 9.2. Support service requirements for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.6.	M	The provider will offer support to MIA in resolving incidents related to the e-Contravention Case Management System, regardless of the causes that led to the incident (e.g. errors in the application, system software problems, problems in external applications). To this end, depending on the specifics of each incident case, the Provider may take the following actions: • receiving information from MIA about the incident and the context of its occurrence; • locate the incident and identify the immediate activities to be undertaken to mitigate the impact of the incident; • identify the causes of the incident and determine the actions to be taken to mitigate the incident; • guiding MIA to undertake actions to mitigate the impact of the inciden and resolve it within the established time limit; • providing detailed information to the MIA on the causes of the incident, the rationale for the actions taken and the actions planned to prevent the recurrence of similar incidents; • examining the need to register a new problem related to the e-Contravention Case Management System (in case of registration of the problem, the Provider will manage it according to the requirements of the problem resolution support service)
CPI.7.	M	The provider will offer support services to resolve problems with the applications. To this end, depending on the specifics of each case, the Provider may take the following actions: • receiving and collecting information related to the problem, symptoms effects, specific conditions; • analyzing and locating the problem at the level of the components of the e-Contravention Case Management System, identifying the interdependencies contributing to the problem or affected by the problem; • identifying temporary solutions to mitigate the effects of the problem and guiding the MIA in their implementation; • identifying solutions to the problem, communicating regularly with the MIA on the progress made in identifying solutions; • if solutions are related to application level configurations, guiding the MIA in their implementation; • in case the solutions involve changes to the program code of the e-Contravention Case Management System, these will be operated by the Provider and implemented within the Maintenance services within the established time limit.
CPI.8.	M	The Provider will offer advisory support services on the use of the e-Contravention Case Management System by the MIA. For this purpose,

ID	Compulsoriness	Requirement
		depending on the specifics of the MIA's advisory needs, the Provider may undertake the following actions: • receiving the consultancy request from MIA and the information related to the context in which the consultancy is needed; • identifying solutions and validating them in the Provider's test environments; • providing complete and correct answers on how MIA should act when operating the e-Contravention Case Management System, as requeste by the consultancy request.

C.2.2 Maintenance services for the e-Contravention Case Management System during the warranty period

Maintenance services must be provided by the Provider in order to maintain the applications at optimal operating parameters over time. To this end, the Provider may come up with updates and changes to the applications and new versions of the applications.

Updates to the e-Contravention Case Management System are changes to the applications, submitted to the MIA at the Provider's initiative and intended to improve the performance of the applications, remove problems, errors and vulnerabilities known to the Provider.

New releases are software packages related to the e-Contravention Case Management System, submitted to the MIA at the initiative of the Provider and containing all the changes previously made to the applications. In addition, they may contain changes and updates, new application components that were not present in the old versions of the applications.

Table 9.3 contains the maintenance service requirements to be provided by the Provider during the warranty period.

Table 9.3. Requirements for maintenance services for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.9.	M	The provider will deliver services to update the e-Contravention Case Management System and deliver new versions.
CPI.10.	M	For this purpose the Provider shall prepare the software packages and documentation related to the updates and new versions.
CPI.11.	M	The implementation of all updates and new versions will be carried out in accordance with the requirements set out in the "Change Management" section of this ToR.

C.2.3 Development services for the e-Contravention Case Management System during the warranty period

Development services are provided by the Provider at the request of the MIA for the purpose of aligning the e-Contravention Case Management System to the changing business needs of the MIA.

A change/development request is a request from the MIA to the Provider for the purpose of obtaining changes to the functionality of the e-Contravention Case Management System or for the purpose of delivering new functionality to the IT system.

A request from the MIA will be considered as a modification/development request only if the requested functionality is not provided by the e-Contravention Case Management System or is provided differently than requested by the MIA. The last category does not include requests related to the correction of functionalities presenting a problem related to the e-Contravention Case Management System (as defined above).

Development services exceeding 100 man/days per year will be paid by MIA in addition to the contract amount, depending on the volume of services provided.

Table 9.4 contains the requirements for development services to be provided by the Provider during the warranty period.

Table 9.4. Requirements for development services for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.12.	M	The provider will deliver services for the modification and development of the e-Contravention Case Management System. The scope of modifications will include at least: • changes to the level of presentation of the e-Contravention Case Management System; • changes to the business logic level of the e-Contravention Case Management System; • changes to the data layer of the e-Contravention Case Management System.
CPI.13.	M	As part of the modification and development services of the e-Contravention Case Management System, the Provider will perform: • the reception of the modification request with the description of the related functional specifications; • - development of the technical project (SRS+SDD) related to the request and its coordination with MIA; • - carry out modifications and developments to the components of the e-Contravention Case Management System.
CPI.14.	M	The implementation of changes and developments at system level will be carried out in accordance with the requirements set out under 'Change management'.
CPI.15.	M	The provider will describe in its offer the proposed model for the management of change and development requests and the methods applied for the estimation of effort and price submitted to MIA The information included in the offer must be sufficient to assess that the relationship between the Provider and MIA in the process of providing development services will be transparent and fair.
CPI.16.	M	The Provider will provide development services for the e-Contravention Case Management System as part of the operational maintenance and

ID	Compulsoriness	Requirement
		development services for the e-Contravention Case Management System. Development services will include: • modification of existing functionality within the e-Contravention Case Management System; • - implementation of new functionalities within the e-Contravention Case Management System.
CPI.17.	M	Any development of the application software for the e-Contravention Case Management System will be initiated based on a request from the MIA. The request will be accompanied by the functional specifications for the requested change. The implementation of any change related to the e-Contravention Case Management System will go through the change management process agreed with the MIA. For changes to the application software, the process will at least include: • implementation in the MIA test environment with unit testing by MIA; • implementation in the MIA test environment and acceptance testing with the involvement of the users of the e-Contravention Case Management System; • implementation in MIA's production environment according to the established change management procedure; • final review and final acceptance of the change.
CPI.18.	M	The provider will include in its offer 100 man-days of development services during the 12-month post-implementation warranty.
CPI.19.	M	Development services in addition to those included may be requested by MIA and provided by the Provider under additional agreements signed between the Parties.

C.3. Level of service related to the e-Contravention Case Management System

The service level of post-implementation support and maintenance sets the requirements for the parameters at which these services must be provided by the Provider.

C.3.1 Support services

The parameters characterizing the level of support services are as follows:

- **Response Time (TR)** - is the time in which the Provider will react to a support request, diagnose the situation and determine the actions required to resolve it;
- **Settlement Time (TS)** – is the objective time in which the Provider is expected to take the actions within its area of responsibility to fully resolve the MIA request.

MIA requests for post-implementation support and maintenance services are categorized in terms of their importance to MIA. The importance for MIA is assessed according to the impact (actual or likely) of the event that triggered the need to place the request on quality parameters for the operation of the e-Contravention Case Management System.

Table 9.5 contains the classification of MIA requests according to their importance.

Table 9.5. Classification of the importance of MIA support requests

Classification	Impact on quality parameters for application operation
Critical	*Availability:* the IT system is unavailable to all or most users. Important transactions need to be carried out as soon as possible (in hours). *Usability:* key business functions cannot be used. There are no alternative procedures and functionalities. *Performance:* response time to user queries makes the IT system virtually unavailable. *Security:* there are major risks of compromising confidentiality, integrity or availability of data
High	*Availability:* the IT system is unavailable to a large number of users. Important transactions and operations need to be carried out by the beginning of the next day. *Usability:* key business functions can be used to a limited extent. *Performance:* response time to user queries significantly affects the performance of key business processes. *Security:* there are high risks of compromising confidentiality, integrity or availability of data.
Ordinary	*Availability:* the IT system is unavailable to some users. There are transactions and operations to be executed within the next three days. *Usability:* the business functionality of the system can be used to a limited extent. *Performance:* response time to user queries moderately affects business processes. *Security:* there are risks of compromising confidentiality, integrity or availability of data.
Low	*Availability:* the IT system is unavailable to a limited number of users. There are no transactions and operations to be executed within up to three days. *Usability:* the business functionality of the IT system is insignificantly affected. There are alternative procedures and functionalities. *Performance:* response time to user queries is higher than usual. Business processes are not affected. *Security:* there are minor risks of compromising confidentiality, integrity or availability of data.

When placing a request for post-implementation support and maintenance services, MIA determines the classification for the request. MIA will attach brief information to explain the classification made. MIA will be able to reclassify the placed requests according to changes in the context of the requests.

- The provider will provide 24x24x365 support services
- The level of support services provided by the provider must meet the requirements specified in Table 9.6.

Table 9.6. Duration of the resolution of MIA support requests

ID	Compulsoriness	Classification of the request placed by MIA	Response Time (TR)	Settlement Time (TS)
CPI.20.	M	Critical	5 min	60 min
CPI.21.	M	High	60 min	the end of the day
CPI.22.	M	Ordinary	24h	3 days

CPI.23.	M	Low	3 days	Best effort*

* The provider will make every effort to resolve the request for service as quickly as possible, operating under normal conditions. The time limit for the resolution of the request will be communicated and accepted by MIA. Subsequent changes to the time limit are permitted only with MIA's acceptance.

C.3.2 Maintenance services

The parameters characterizing the level of maintenance services provided by the Provider during the warranty period of the e-Contravention Case Management System are described in Table 9.7.

Table 9.7. Requirements for maintenance services of the e-Contravention Case Management System during the post-implementation period

<table>
<tr><th>ID</th><th>Importance</th><th>Requirement</th></tr>
<tr><td>CPI.24.</td><td>M</td><td>The provider will apply a policy of minimizing the frequency of issuing application level updates. The policy applied by the Provider will allow MIA to apply new updates on a monthly basis. The exception may be updates intended to remove critical and security issues in the e-Contravention Case Management System.</td></tr>
<tr><td>CPI.25.</td><td>M</td><td>The Provider will apply a no obligation policy to implement new application versions. The policy applied by the Provider will allow MIA to implement new versions of the applications every three years.</td></tr>
<tr><td>CPI.26.</td><td>M</td><td>Provider will communicate to MIA its schedule for issuing updates and new versions. For updates, the Provider shall notify MIA at least one month in advance. For new releases, the Provider shall notify MIA at least 6 months i advance.</td></tr>
<tr><td>CPI.27.</td><td>M</td><td>In order to maintain the e-Contravention Case Management System in a functional state, the Provider may carry out maintenance work on the IT components related to the IT system. The type of maintenance works and the Provider's commitments regarding their coordination with the MIA, their period and duration are set out in the following table:
<table>
<tr><td>Type of maintenance works</td><td>Notification of the Beneficiary</td><td>Period and duration of works</td></tr>
<tr><td>Ordinary maintenance works</td><td>5 days in advance.</td><td>They are made outside the guaranteed availability period for the e-Contravention Case Management System. The duration of this work will not exceed 4 hours.</td></tr>
<tr><td>Major maintenance works</td><td>10 days in advance.</td><td>They are carried out outside the guaranteed availability period for the e-Contravention Case Management System. The duration of this work shall not exceed 24 hours.</td></tr>
</table></td></tr>
</table>

ID	Importance	Requirement
		Urgent maintenance works: With notification as soon as the need for their initiation arose. They may be carried out at any time. Their duration will not exceed 2 hours.

C.3.3 Development services

The parameters characterizing the level of development services offered by the Provider during the warranty period of the e-Contravention Case Management System are described in Table 9.8.

Table 9.8. Requirements for development services of the e-Contravention Case Management System in the post-implementation period

ID	Compulsoriness	Requirement
CPI.28.	M	The provider will respond to a development request from MIA within 3 days.
CPI.29.	M	The provider will come up with budget estimates and solution concept in maximum 10 days.
CPI.30.	M	The provider will deliver the solution within the time agreed with MIA, applying the "best effort" principle.
CPI.31.	M	The provider will allow MIA to set priorities for the development requests and review them later. The review of the request priorities will make it possible for the Provider to review the solution delivery deadlines.

C.4. Support services management

The way support services are organized, including after the expiry of the warranty period of the e-Contravention Case Management System are described in the non-functional requirements included in Table 9.9.

Table 9.9. Requirements for the management of support services of the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.32.	M	The provision of services by the selected Provider to MIA will be carried out considering ISO 20000 standards and the ITIL v3.0 set of practices. The Provider must have the ability to interact with MIA according to established best practices. It must also have internal processes and capabilities to deliver operationally according to the stated practices in the field.
CPI.33.	M	Support services will be provided under a Service Level Agreement (SLA), which will be annexed to the Contract signed between the Parties. The SLA will set out the level of post-implementation support and maintenance services based on the requirements included in this ToR.

ID	Compulsoriness	Requirement
CPI.34.	M	The Provider will have a Customer Support Centre to which all requests from the MIA will be directed. The work schedule and organization of the Support Centre's activities must ensure the provision of post-implementation support and maintenance services at the level set out in this ToR.
CPI.35.	M	The Provider must be able to demonstrate timely access of the Support Centre to specialists certified by the manufacturers of the provided application solutions.
CPI.36.	M	Support services will be provided remotely. If necessary, the Provider's specialists will travel to MIA's premises.
CPI.37.	M	For the provision of post-implementation support and maintenance services, the Provider will offer MIA an application platform, available to MIA via the Internet. The application platform will be adequately secured. All interactions between the Provider and MIA within the framework of the provision of post-implementation support and maintenance services will be carried out through the respective platform.
CPI.38.	M	The Provider will monitor the quality of the post-implementation support and maintenance services and will react to any deviations in order to prevent them.
CPI.39.	M	The Provider will submit monthly reports to the MIA on the services provided and their level. The reports will also contain information on the actions taken by the Provider or planned to improve the quality of the services.
CPI.40.	M	The provider will submit quarterly to the MIA the act of acceptance of post-implementation support and maintenance services. The act of acceptance will contain the volume and amount of services provided. The act of acceptance will be accompanied by the report on the services provided and their level.
CPI.41.	M	Payment for post-implementation support and maintenance services will be made quarterly, after the services have been provided, on the basis of the acceptance act and the report on services provided.

C.4.1 Change management

All changes applied to the e-Contravention Case Management System applications in the context of the provision of post-implementation support and maintenance services will be managed according to a mature change management process. Table 9.10 contains the change management organizational requirements for the e-Contravention Case Management System.

Table 9.10. Change management requirements for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.42.	M	The Provider will include in its offer information on the proposed approach to change management at application level.

ID	Compulsoriness	Requirement
CPI.43.	M	The Provider will propose to MIA the change management procedure for the applications. The procedure will be coordinated and accepted by MIA.
CPI.44.	M	The change management procedure shall provide for at least the following activities under the responsibility of the provider: • testing of changes in the MIA test environment; • preparation of the change implementation plan; • preparation of the roll back plan in case of failed changes; • preparation of technical documentation related to changes, including: scope of changes, affected components, implementation guide, roll back plan application guide, change follow-up guide; • preparation of detailed technical documentation related to changes (documentation will include description of changes, affected components, installation instructions, rollback plan in case of failure, follow up procedures to ensure correct implementation of changes); • update the user documentation and technical documentation related to the applications and submit it to MIA; • provision of software packages related to the change; • provision of files containing the source code for the changes (authenticity and integrity of the software packages and source code must be ensured by applying the provider's digital signature - code signing); • immediate reaction in case of detection of errors in the implemented changes and their correction in the shortest possible time.
CPI.45.	M	In the process of operational maintenance and development of the e-Contravention Case Management System, the Provider will make a number of changes to the components of the e-Contravention Case Management System (system components and application software). All changes made by the Provider to the System will be implemented according to a commonly agreed change management process. Changes that may have a significant impact on the quality parameters of the e-Contravention Case Management System will be authorized by the MIA. Mandatory elements for this type of changes will be: • testing in the test environment; • implementation plan for the change; • the roll back plan; • post-implementation review. The provider will keep track of all changes related to the e-Contravention Case Management System in a Change Register. MIA will have read access to this Register.

C.5. Quality assurance

The quality of post-implementation support and maintenance services directly influences the quality of use of the e-Contravention Case Management System by the MIA. The provider must be able to demonstrate that these services will be delivered at the agreed quality level. Table 9.11 contains the quality assurance requirements for post-implementation support services for the e-Contravention Case Management System.

Table 9.11. Quality assurance requirements for post-implementation support and maintenance services for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.46.	M	The provider will submit a quality assurance plan for post-implementation support and maintenance services at the beginning of the year. The plan will contain the performance indicators for the services, the risks that may affect the performance indicators, the preventive actions implemented to manage the risks and the measures to mitigate residual risks. The plan submitted by the Provider must subsequently be accepted by MIA. The Quality Plan will be reviewed by the Provider at least annually, or in cases where significant deviations in the delivery of services at the agreed level are identified.
CPI.47.	M	The Provider shall include in the offer information on its approach to the quality assurance plan for post-implementation support and maintenance services
CPI.48.	M	The provider will conduct annual audits of its ability to deliver post-implementation support and maintenance services to the agreed level. The audits shall be conducted by entities independent of the Provider. The audit methodology applied must be aligned with best practices in the field (e.g. SAS 70, ITIL, ISACA standards, etc.). Audit reports will be submitted to the MIA together with action plans to remedy the shortcomings identified by the auditor.
CPI.49.	M	The provider must develop and maintain an up-to-date Quality of Service Plan for the operational maintenance of the e-Contravention Case Management System. The plan must consider the following risk categories: • Operational risks (loss of the Provider's ability to perform at the established level, risks to the Provider's internal processes); • Technological risks (risks that may affect the availability, accessibility, performance and security of the e-Contravention Case Management System). The Quality Plan must contain detailed information about the identified risks, the measures to be implemented by the Provider in order to prevent them, the residual risks and the planned response measures in case of realization of residual risks. The Quality Plan is to be updated at least annually, or at any major change in the components of the e-Contravention Case Management System or in the processes related to the maintenance of the e-Contravention Case Management System. The Tenderer shall submit to MIA the Quality Plan in its last update.

ID	Compulsoriness	Requirement
		At the offer submission stage, the Provider must describe how it will produce the Service Quality Plan. The offer will have a competitive advantage if the Tenderer attaches the Quality Plan to the offer and it meets the needs of MIA.

C.6. Performance guarantees

The Provider must guarantee the provision of maintenance and support services provided during the post-implementation period in accordance with the SLA signed with MIA. Table 9.12 contains the requirements for guaranteeing the quality of maintenance and support services provided by the Provider in the post-implementation period of the e-Contravention Case Management System.

Table 9.12. Quality assurance requirements for the maintenance and support services provided during the post-implementation period for the e-Contravention Case Management System

ID	Compulsoriness	Requirement
CPI.50.	M	The provider will submit a bank letter of guarantee, according to the UNDP template, for the provision at the agreed level of post-implementation support and maintenance services.
CPI.51.	M	The amount of the bank guarantee will be 10% of the value of the provided services.

C.7. Termination of contract

If the parties decide not to extend the contract for post-implementation support and maintenance services, MIA's activity shall not be affected. MIA must have the option to contract with another Provider or take over the support and maintenance of the e-Contravention Case Management System internally.

Table 9.13 contains the requirements related to the conditions of termination of the contractual relationship between the Provider and the Beneficiary for maintenance and support services during the post-implementation period of the e-Contravention Case Management System.

Table 9.13. Requirements for termination of the contract for the provision of maintenance and support services in the post-implementation period for the e-Contravention Case Management System

ID	Importance	Requirement
CPI.52.	M	In the event of expected loss of contract effect for post-implementation suppor and maintenance services, the Provider must ensure at a minimum: • all source codes (or configuration files in the case of COTS solutions) related to the e-Contravention Case Management System are transmitted to the MIA. • the transmitted source codes/configurations must be those on the basis of which the e-Contravention Case Management System components have been produced and are running at the time of contract termination in the MIA production environment (the authenticity and integrity of the mentioned files will be confirmed by the Provider's digital signature); • all the documentation related to the e-Contravention Case Management System is updated and transmitted to MIA; • all records related to MIA requests made on the Provider's side (for incidents, problems, consultancy, modifications, developments, etc.) are exported in a jointly agreed format (e.g. CSV, XLS, etc.) and transmitted to MIA; • The Provider will keep for a period of one calendar year all records produced during the provision of services, source codes and related e-Contravention Case Management System.
CPI.53.	M	For a period of one calendar year after the expiry of the support contract, the Provider will be willing to cooperate with third parties authorized by MIA to provide MIA with post-implementation support and maintenance services. To this end the Provider will at least ensure the provision of all information held that would help improve the services.
CPI.54.	M	The Provider shall include in its offer information on the proposed approach for the termination of post-implementation support and maintenance services taking into account MIA's requirements and needs.
CPI.55.	M	The contract signed under this tender is to be for a term of 30 months. Either party may at any time request the termination of the signed contract. To this end, the party wishing to terminate the contract will notify the other party of its intention at least 3 months in advance.
CPI.56.	M	All the data stored in the databases related to the e-Contravention Case Management System are the property of MIA. In the event of termination of the contract, the Provider shall offer the MIA a procedure for exporting the data in a format jointly agreed with the MIA. The selected format must allow MIA to fully import the data into other similar solutions.