

# **REQUEST FOR EXPRESSIONS OF INTEREST (CONSULTING SERVICES – FIRMS SELECTION)**

Republic of Armenia  
Fourth Public Sector Modernization Project  
Loan No.9338-AM

**Assignment Title:** Modernization of the Criminal Case Pre-Trial Proceedings e-Management System (CCPTEMS)

**Reference No.** (as per Procurement Plan): PSMP4-CQS-1.2.7

The Republic of Armenia has received financing from the World Bank toward the cost of the Fourth Public Sector Modernization Project, and intends to apply part of the proceeds for consulting services.

The consulting services (“the Services”) include modernization and ensure the eventual operation of the electronic system of pre-trial proceedings in order to bring the system into line with the existing regulations and the operational requirements for the beneficiaries.

Within the framework of the proposed services, an analysis of legal and operational requirements, digitization of recent legislative changes, and an integration of the system with various interoperability systems must be carried out. In particular, it is necessary to design, implement, test, and localize the current System in a real (operational) environment, modified and finalized on the basis of existing regulations, the requirements described in this document, and other related legal norms regulating the sphere.

More details on the Services are provided in the Terms of Reference attached to in this REOI in APPENDIX A.

Duration of the assignment: 12 months.

The Office of the Prime Minister of the Republic of Armenia now invites eligible consulting firms (“Consultants”) to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. Interested Consultants must provide information demonstrating that they have the required qualifications and relevant experience to perform the above-mentioned Services.”

The Consulting firm must have sufficient resources and capacity to carry out the Services. In particular, the Consulting firm must meet the following minimum requirements:

- Experience in the design, development, and implementation of information systems for criminal cases or pre-trial proceedings in at least one country;
- Experience in carrying out tasks of similar scale and complexity,
- Experience in developing e-government systems,
- Experience in system architecture design and system integration,
- Technical support and training experience,
- Experience in implementing programs funded by international development organizations.

**The Consultant's core staff/experts will not be evaluated at this stage.**

More specifically, the Expression of Interest should provide the following information:

*A detailed description of the company's main business and years of activity, including services provided, completed projects (with implementation dates, addresses, contact details, as well as the number of the company's main staff and other data), as well as substantiation of the company's experience with documentary evidence. The documents should be accompanied by a list of relevant tasks, indicating the name of the project, the client, the year and duration of implementation, the role of the consultant, the scope of services provided and the source of financing.*

The attention of interested Consultants is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" November 2020 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

Consultants may associate with other firms to enhance their qualifications, but should indicate clearly whether the association is in the form of a joint venture and/or a sub-consultancy. In the case of a joint venture, all the partners in the joint venture shall be jointly and severally liable for the entire contract, if selected.

The detailed Terms of Reference (TOR) for the assignment are presented in Appendix A to the REQUEST FOR EXPRESSION OF INTEREST.

A Consultant will be selected in accordance with the Consultant Qualification Selection method set out in the Procurement Regulations.

Further information can be obtained at the address below during office hours from 09:00 to 18:00.

Expressions of interest must be delivered in a written form to the address below (in person or by e-mail) by October 7, 2025 (18:00 local time).

Attn: Mr. Aharon Mkrtchyan  
PSMP4 Project Manager  
Office of the Prime Minister of RA  
Address: Government House 1, Republic Square  
(1-st Floor, Room 115, 117)  
Country: Republic of Armenia  
Telephone: (+374 10) 515931

## **APPENDIX A**

### **TERMS OF REFERENCE**

#### **Modernization of the Criminal Case Pre-Trial Proceedings e- Management System (CCPTEMS)**



# 1. INTRODUCTION

The Electronic System for Pre-Trial Proceedings of a Criminal Procedure (Criminal Case Pre-Trial Proceedings Electronic Management System – CCPTEMS) has been developed and introduced with the view of improving the efficiency of pre-trial proceedings in criminal litigation, increasing their efficiency and saving financial and human resources. The main objective of the system is to ensure electronic implementation of the pre-trial processes, increase effectiveness of the analysis and reporting, and improve the work of the main beneficiaries including investigators, pre-trial authorities, prosecutors, etc.

Following the introduction of the CCPTEMS, a number of legislative changes took place, which, *inter alia*, require alignment with the level of functional capabilities of the system. In this context, it has become necessary to make certain updates and improvements in order to bring the system into line with the new regulations and to ensure its continuous development.

Implementation of the present ToR for improving the electronic system of pre-trial proceedings will provide new opportunities, first of all for its main users, investigators and prosecutors, with the view to increasing the effectiveness of pre-trial investigations with the help of digital tools.

The overview of the existing information system is presented in Appendix 1 attached to this paper.

## 2. ToR OBJECTIVE(S)

The objective of the ToR is to modernization and ensure the eventual operation of the electronic system of pre-trial proceedings in order to bring the system into line with the existing regulations and the operational requirements for the beneficiaries.

## 3. SCOPE OF SERVICES

3.1 Within the framework of the proposed services, an analysis of legal and operational requirements, digitization of recent legislative changes, and an integration of the system with various interoperability systems must be carried out. In particular, it is necessary to design, implement, test, and localize the current System in a real (operational) environment, modified and finalized on the basis of existing regulations, the requirements described in this document, and other related legal norms regulating the sphere.

3.1.1 The system must be used to digitize the entire chain of pre-trial proceedings, ensuring full automation of business processes, and to ensure human-machine interoperability where it is not operationally feasible.

3.1.2 The system must be tested and updated to comply with current legislative requirements, furthermore, it should introduce new processes, enhance interoperability with other systems, provide for statistical module, and carry out other necessary improvements.

Ultimately, the System must enable at least the following functions:

- electronic execution of the functions of investigators and prosecutors, and, where possible, automation of certain processes among them;

- electronic document circulation among participants of the pre-trial proceedings, such as the defendant, the victim, their representatives, and other users, including through automated means;
- notifications to internal and external users of the system, as well as to non-users;
- provision of two-dimensional automated interoperability with internal and external systems, based on the requirements of operational feasibility;
- ensuring accountability on the basis of data collected or obtained due to interoperability of the system with the help of automated tools;
- during the implementation of the above-mentioned functions, it is necessary to ensure:
  - ✓ processing data in machine readability mode;
  - ✓ effective access to data and information for the public, policy-makers, and all other beneficiaries in line with their functions;
  - ✓ security of data storage and prevention of unauthorized access;
  - ✓ interoperability with the internal and external systems,
  - ✓ a wide range of reporting tools.

3.1.3 Additions and necessary changes must be made to the modules available in the system, and in some cases additional modules must be added as needed.

### 3.2 Adding New Roles

Some of the external users need to be given clear roles in the System, set up their own personal office and provide access to:

- (a) personal office from the public domain; and
- (b) works and materials that internal users will make available to them.

As an example, we may consider the accessibility provided to external users within the framework of civil proceedings via the platform *cabinet.armlex.am*.

Here, it is necessary to define new roles and create personal offices for the following entities:

External users		
	Name	Description
1	<b>Defendant</b>	A person against whom criminal prosecution has been initiated and there is no final decision either on the termination of the criminal prosecution, conviction or acquittal.
2	<b>Defender</b>	A lawyer who assumes and carries out protection of the detainee or defendant during the criminal proceedings
3	<b>Legal representative of the defendant</b>	A parent, caregiver, guardian or trustee of a minor, physically or mentally incapacitated defendant; within his or her jurisdiction, an employee of the guardianship and trusteeship

		body; a close relative of the deceased defendant or the alleged perpetrator of a crime who deceased.
4	<b>Victim</b>	A natural or legal person, state, community or international organization in respect of which there are sufficient grounds to assume that the alleged crime has caused harm to them or could have been caused in the event the alleged crime was completed.
5	<b>Representative of the victim</b>	An authorized representative, i.e. a lawyer who has been duly authorized by the victim to represent his or her legitimate interests during the proceedings, as well as a duly authorized employee of the victim who is a legal entity.
		Legal representative: a parent, caregiver, guardian or trustee of a minor, physically or mentally incapacitated defendant; within his or her jurisdiction, an employee of the guardianship and trusteeship body; as well as the head of the legal entity that is a victim.
6	<b>Expert</b>	<p>A person assisting the proceedings, who is not interested in the subject matter of the proceedings and who, through the use of special knowledge or skills, provides assistance to the proceedings through:</p> <p>( 1) conducting research and drawing a written conclusion;</p> <p>( 2) giving a written opinion without conducting research;</p> <p>(3) participating in the performance of an evidentiary or other procedural action.</p>
7	<b>Body of Inquiry</b>	<p>Within the scope of their powers defined by law, the following bodies have the right to carry out operative-intelligence activities and, in cases and procedures prescribed by law, conduct inquiry within the framework of criminal proceedings:</p> <ol style="list-style-type: none"> <li>1. The Police <ol style="list-style-type: none"> <li>1.1) military police</li> <li>1.2) the authorized state administration authority in the field of internal affairs — with respect to employees of its structural subdivisions and subordinate state bodies</li> </ol> </li> <li>2. National Security Authorities</li> <li>3. Tax Authorities</li> <li>4. Customs Authorities — for the purpose of preventing and detecting smuggling and other crimes</li> <li>5. Penitentiary Service — only within penitentiary institutions</li> <li>6. Anti-Corruption Committee</li> <li>7. Foreign Intelligence Service</li> <li>8. State Protection Service</li> </ol>
8	<b>User</b>	<p>A government body exercising judicial authority during criminal proceedings:</p> <ul style="list-style-type: none"> <li>- First Instance Court of General Jurisdiction for Criminal Cases,</li> <li>- Criminal Court of Appeal,</li> <li>- Criminal Chamber of the Court of Cassation,</li> </ul>

		<ul style="list-style-type: none"> <li>- Anti-Corruption First Instance Court,</li> <li>- Anti-Corruption Court of Appeal,</li> <li>- Anti-Corruption Chamber of the Court of Cassation.</li> </ul>
9	<b>Other external user</b>	The other external user can be used by any other person no listed above, such as property defendant, their legal representative and authorized representative, the witness, the legal representative and lawyer of the witness, the interpreter, the psychologist, the attesting witness, etc.

### 3.3 User Account Management

The management of user accounts is carried out by the system administrator. Each user account must be assignable to one or more roles. Assigning a role to a user account means that the account receives the set of permissions associated with that role. It must be possible to assign multiple roles to a single user account. If a user temporarily requires access rights corresponding to a different position, this must be possible by adding the relevant role to their account.

In addition to assigning permissions, it must also be possible to restrict those permissions based on specific attributes. For example, an investigator's authority must be limitable to cases being handled by that specific investigator. The use of attributes must allow for the restriction of a user account's permissions to particular functions and data access related to a specific role. Furthermore, it must be possible to restrict the operations available under a given role based on certain parameters.

Whenever an authenticated user accesses any module of the System, the system verifies the full set of access rights and attributes associated with the user, based on which it either permits or denies execution of the operations and access to data defined by the functional logic. If the user has multiple roles and attribute-based permissions for the same module, those permissions are aggregated, and the system grants access to any allowed operations under those combined permissions. Importantly, the system considers which attribute corresponds to which role, and if no specific role is selected, the attribute applies to all of the user's permissions.

The system administrator is authorized to manage the permissions of all users within the system. They are responsible for creating new user accounts, assigning roles and attributes, editing accounts, and activating or deactivating them.

User accounts can also be generated automatically during the registration process of individuals entering through the public domain.

#### 3.3.1 Identification

Access to the public and non-public domains of the system is possible only by identifying the person through integration with the national identification systems used in the Republic of Armenia "YES EM" (IT'S ME).

After authentication, access is provided based on designated functions.

Identification in the system is carried out on a single sign-on (SSO) principle, with management of a certain active period of inactivity. Navigation between modules is carried out in accordance with the principles of using centralized authentication service (CAS-Central Authentication System).



### **3.3.2 Personal office**

For all users of the system (administrator, internal and external users) a "Personal Office" domain must be designed in the interface, where they will be able to see and manage the information and modules/sections available to them.

- Add or edit their personal information (e-mail, phone number, etc.),
- Present or see the cases available to them, follow their progress,
- Attach and view the available documents,
- Manage all the other modules available to them,
- The rights granted to external users in the personal office and the fields to be developed must be based on the procedural powers of the specific new external users.

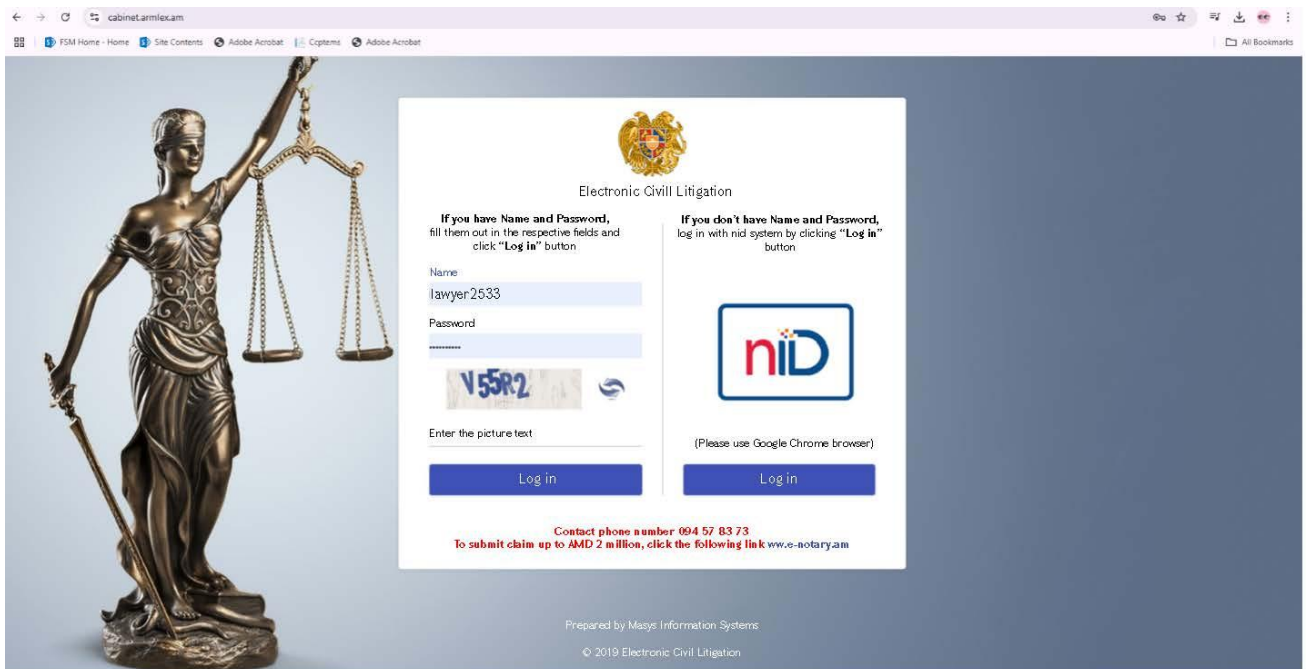
In particular, the rights and duties of the defendant are defined by Article 43 of the Code of Criminal Procedure and the rights of the victim by Article 50 of the Code of Criminal Procedure. Based on specific rights and obligations, the System must contain appropriate tools for carrying out actions to ensure the exercise of these rights and the performance of duties. Based on the rights of the defendant as defined in Article 43 of the Code of Criminal Procedure, they can be divided into the following groups from the point of view of the System:

1. the right to receive notifications, procedural acts, and other documents;
2. the right to present evidence;
3. the right to submit motions, recusals, objections;
4. the right to appeal procedural acts of public participants in the proceedings.

### **3.3.3 Display in the Public Domain**

A special interface must be designed in the public domain from which external users can access their personal office only after identification. Access to the system through the web site for external users from the public domain can be done in two ways: in the case of professional external users (lawyer, expert, court), by importing the name and password of the user's account formed after receiving initial approval by the administrator of the system, and in the case of non-professional external users (defendants, victims, their non-lawyers), access can be granted only after identification by the "YES EM" system. In this way, the System will also distinguish between specialized external users in what role they entered the system: as a specialized entity (e.g., lawyer) or as a non-specialized entity (e.g., victim)

The image below displays the first page of the public domain of the civil cases system cabinet.armlex.am, which displays the ways to access the system for entities that already have a user account and those that do not.



### 3.3.4 Accessibility

After access to the System by external users from the public domain, access to a specific proceeding must be requested from the body conducting proceedings, the investigator or the prosecutor. An external user must request this access by defining his or her specific role, be able to attach documents, submit applications, and gain access to specific cases and individual files. The tasks to which the person has access must be grouped and displayed on their personal office page.

Non-professional external users (defendant, victim) may also involve other users who are representatives, whose approval is made by the body conducting proceedings. Removal of representatives can also be done by non-professional external users.

External users may have access to the case, document or materials from their Personal Office Notifications Section in the System, as well as through an active link to the notification received through other methods of notification.

## 3.4 Development of new functions, processes, forms

As a result of the legislative amendments made after the development phase of the system, in 2021-2022, a number of changes are necessary in the System. Below are the changes needed as a result of these amendments.

### 3.4.1 Addition of new units as a result of the transfer of the preliminary investigations function from the NSS to the Investigative Committee

From January 1, 2024, the implementation of the investigative function has been transferred from the National Security Service to the Investigative Committee, due to which the General Department for the Investigation of Crimes Against the State, the Fundamentals of the Constitutional Order and Public Security was established within the Investigative Committee, with 47 positions, 39 of which are investigators. As a result of this change, a similar department has been created in the Prosecutor General's Office for the exercise of prosecutorial supervision over these cases. This change has created a need for appropriate changes to the System. The same change has also taken place in the Anti-Corruption Committee, where a new unit has been created.

It is necessary to add the relevant units in the hierarchical structure of the Prosecutor General's Office, the Investigative Committee, and the Anti-Corruption Committee and to separate the relevant investigators and prosecutors and attach them to the appropriate departments. To carry out this function, it is necessary to obtain information from the beneficiary about all structural changes, with clear names and new positions, their role in the hierarchical structural tree, and to make the appropriate structural changes.

In addition, it is necessary to restructure this module in such a way that it is possible to make such changes by the Client in the future without a significant change in the software code, as structural changes are a continuous process.

### **3.4.2 Protocol on imposing a fine by consent**

A new protocol on imposing a fine by consent must be introduced, within the framework of which the investigator, upon receiving the written consent of the supervising prosecutor, may refer a procedure for imposing a fine by consent to a defendant who has committed a crime for the first time and is accused of a minor crime. A new process and form must be added to the Processes Subsection of the current Criminal Cases Section of the system, which relates to the proceeding of imposing a fine by consent. The Consultant must develop the form and formulate the process in the same format as other processes and forms developed in the System. Below are the rules of the protocol for imposing a fine by consent.

The actions of the protocol to impose a fine by consent are as follows:

1. The investigator applies to the supervising prosecutor to obtain written consent to impose a fine:
2. System Checks
  - The system must allow the investigator to refer to the supervising prosecutor if there are positive terms defined in Article 464.6 of the Code of Criminal Procedure and there are no exceptions envisaged by Article 464.7.
3. Positive terms (Article 464.6)
  - The investigation has been completed
  - Committing a crime for the first time
  - Being charged with a minor crime
  - The system checks for the presence of these three conditions and only then allows the investigator to refer to the supervising prosecutor.
4. Negative terms (Article 464.7)
  - The defendant is a minor
  - Defendant charged with more than one offence
  - There is no penalty envisaged for the defendant's actions in the Criminal Code
  - Damage to the interests of a private person
  - A property claim has been filed against the defendant or a person related to them
  - The supervising prosecutor objected to the imposition of a fine
  - The defendant has refused from the proceedings to impose a fine by consent
  - Violation of the rules provided by Article 464.6
  -

- The system checks the negative terms set out in points 1, 2 and 5 and, if present, prohibits the investigator to proceed.
5. The actions of the Supervising Prosecutor:
    - The prosecutor gives written consent to the investigator to initiate the proceedings.
  6. The investigator's actions:
    - Notices the Accused of imposing fine by consent
    - Defendant provides his or her standing
    - If it is positive, a protocol is drawn up, which is signed by the investigator, the defendant and his or her defender.
  7. Final stage
    - The record is attached to the indictment
    - The supervising prosecutor sends the indictment and the attached record to the court.

### **3.4.3 Possibility of submitting electronic documents, applications and cases to the court**

Interoperability with the court must be ensured in two ways:

- Creating an external user role for the court and providing appropriate functions,
- Creating an interface for interoperability with the electronic platform for judicial procedures (e-criminal court).

The task of creating an external user role for the court has been described in paragraph 3.2 of this document. In parallel, the possibility of providing the court with access to a specific case or files through a generated link sent via email or other means should continue to exist.

After the introduction of the e-criminal court system, the system must become interoperable with the electronic system of pre-trial proceedings, so the system must have the opportunity to become interoperable with the electronic system of judicial procedures after the latter has been introduced. After becoming interoperable, the documents sent to the court by the prosecutor and the investigator will be transferred to the electronic judicial procedure system, which will make it available to the court. During the full provision of interoperability, the beneficiaries will decide to terminate the functions of the court as an external user of the System or to leave the possibility of both the transfer of information with interoperability and the use of the System by the court as an external user.

In this regard, the Consultant shall study, analyze and, as a result of discussions with the beneficiary, record the information that must be transferred from this System to the electronic court system, as well as vice versa - the information that must be received from the electronic criminal court to this System as a result of interoperability. After recording this information, the Consultant must compile the API with which this two-way interoperability can be implemented. The uncertainty of information regarding the electronic criminal court system cannot be a reason for not developing the required API. Under these circumstances, the Consultant is obliged to anticipate what the requirements for the design of the future Electronic Criminal Court must be and to prepare an API that will operate and ensure interoperability.

Hence, the Consultant has to develop

- in the event of the creation of an API electronic criminal court system, the system will become interoperable, clearly identifying what information must be sent and what

information must be received within the framework of two-way interoperability, in what way - by request or automatically, etc.,

- a new role for the court and its composition as an external user, where cases, documents or other materials addressed to the court by other users within their competence will be available to the court and the court may also submit certain electronic documents and materials;
- as a separate external user for the court, provide the court with access to a specific case or files via e-mail or other active link.

#### **3.4.4 Presentation of new types of motions by the prosecutor and the investigator to the court**

When presenting charges in court, in a number of cases, the prosecutor has the authority to present a position, motion, etc.. In the event that there is an opportunity in the System to submit a motion or other relevant document to the court, it is necessary that these documents be generated in the System itself, and those generated documents be sent to the court. This will allow for electronic access not only to documents generated during the pre-trial hearing, but also to those generated during the judicial hearing. This applies both to all actions and motions already in the System that must be sent to the court, as well as to some new actions that are not described in the System. Such actions include.

- Statement of position on the defendant's motion for accelerated proceedings
- Statement of position on the defendant's motion for the use of consent proceedings
- Submission of a motion for the application of a special procedure for the trial of a defendant who has signed a cooperation agreement
- Statement of position on the punishment to be imposed
- Withdrawal from the court of various motions submitted by the investigator, if the latter has that authority under the Criminal Procedure Code
- Other motions, standings.

In particular, new processes and forms relating to the submission of the above-mentioned motions and positions to the court must be added to the Processes subsection of the current Criminal Cases section of the system. The Consultant must develop the form and formulate the process in the format of other processes and forms developed in the System.

The investigator also has the authority to present certain motions or applications to the court. This means that in all cases where a relevant action has to be notified to the court, the System must provide the opportunity to do so. Among the functions already available in the System, we have identified certain new ones that are not described in the System, but the investigator must also be able to send them to the court. These include:

- Filing a motion to have a deposition of evidence taken in court;
- Filing a motion to confirm the legality of the investigator's decision to freeze property;
- Other motions, standings, and other procedural documents.

### **3.4.5 Submission of the investigator's objections to the actions of the supervising prosecutor**

The System must also establish a form for objection by the investigator against the decision of the supervising prosecutor to initiate criminal prosecution.

In particular, new processes and forms must be added to the Processes subsection of the current Criminal Cases section of the system, which relate to the filing of the above-mentioned motions and positions to the court. The Consultant must develop the form and formulate the process in the format of other processes and forms developed in the System.

### **3.4.6 Provision of a Special Protection Measure**

It is necessary to add to the system the process of applying a special protection measure by the body conducting the proceedings.

The law provides for nine special protections:

- ( 1) Restrictions on approaching or interacting with a protected person;
- ( 2) Confidentiality of data that identifies the protected person;
- ( 3) Supervision of the protected person, his or her house and property;
- ( 4) Providing personal protection to a protected person;
- ( 5) Transportation of a protected person to another place of residence;
- (6) Replacement of documents confirming the identity of the protected person or changing the appearance of the protected person;
- (7) A change in the place of employment, service, or education of a protected person;
- (8) Removal from the courtroom or holding a closed court hearing;
- (9) Interrogation of the person defended in court in a special manner.

These measures are applied by the investigator's decision and are terminated by the investigator's decision. For all these decisions, it is necessary to add two processes in the "Processes" section of the Criminal Procedure: "On the Application of Special Protection Measure" and "On the Termination of Special Protection Measure." The creation of these two processes also requires the development of two forms with the same names. From the dropdown list of protections already selected in the forms, the specific protection measure that is applied or discontinued will be selected. It must be possible to deliver this decision to the Police through an interoperability platform.

### **3.4.7 Record of the Impossibility of a Procedural Action**

According to the Code of Criminal Procedure, the recording of administrative actions is carried out electronically, except if it is impossible. In various unpredictable situations, it may be impossible to record criminal proceedings electronically, and the conducting body will do it in a paper version. In order to ensure the integrity of the criminal case and later include the paper record in the System, it is necessary to create a process by which the conducting body records that a process has been carried out in paper form and the scanned (digitized - OCR) version of that paper document is downloaded to the System in a readable version for the System.

To carry out this action, it is necessary to add a new process and form to the "Processes" section of Criminal Proceedings, where one must fill in the information about the action and its data (the

content of the form must be clarified with the beneficiary), why its recording was impossible electronically (reasonable), scanning the paper medium of the investigative action carried out through OCR (Optical Character Recognition) embedded in the system, from which basic information is automatically extracted and stored in a database with a unique identifier.

#### **3.4.8 Creation of the Prosecutors' Group**

The system must provide an opportunity to create a group of prosecutors who carry out supervision over the legality of pre-trial proceedings.

The rules for the creation of the group are:

1. Actions of the Supreme Prosecutor:
  - Instructs the creation of the Prosecutors' Group.
  - The assignment must specify the protocol by which the group is created, the prosecutors included in the group, as well as the head of the group.
2. Actions of the head of the Prosecutors' Group:
  - defines the framework for the exercise of the powers prescribed by Articles 38 and 39 of the Code of Criminal Procedure of the Republic of Armenia by each prosecutor included in the group.
3. System Actions

The system must keep the following processes active with the criminal proceedings in which a group of prosecutors has been created, and for other prosecutors in the group, the implementation of these processes must be frozen:

- A decision to initiate criminal prosecution against a person, to suspend or resume the deadline for criminal prosecution, not to initiate criminal prosecution, or to terminate it;
- on the basis of the materials of the proceedings, decides at its discretion whether to initiate, not to prosecute, or to terminate criminal prosecution;
- decides on the recusal of the investigator, the head of the investigative body, the supervisor of the investigative body, as well as their self-recusal;
- repeals illegal or unsubstantiated decisions of the head of the investigative body, the investigator, or the supervisor of the investigative body, as well as the illegal or unsubstantiated assignments of the supervisor or investigator of the investigative body;
- removes the head of the investigative body, the investigator, or the investigator is removed from participating in the proceedings;
- confirms or does not confirm the indictment or the final act by returning the materials of the proceedings with an instruction, and hands over the materials of the proceedings to the court, confirming the investigator's decision to terminate the criminal proceedings;
- eliminates any unlawful restrictions on the rights or freedoms of a person, may release unlawfully detained persons;
- expresses a position on the sentence to be imposed after a guilty verdict.



### **3.4.9 Providing for Video Call Function**

It is necessary to add video call option to the system to ensure the implementation of investigative, prosecutorial, and other actions. The implementation of the video call should be ensured through integration with any video call system that meets the technical requirements of Appendix 4 of this document. The ToR does not contain a requirement to develop a new video call system. Under the ToR terms, the Consultant should create a solution to have a corresponding field in the System, where the reference to the use of the video call system and other parameters necessary for the implementation of the video call (implementation day, time, access rules) will be displayed. Internal users of the system should be able to generate video call links and grant access to other internal and external users, as well as to individuals who are not participants in the system. These video call links should be integrated with the calendar module, so that both the scheduling of the video call and its link can be recorded within the calendar. The video call system should be interoperable with the repositories fs1.e-criminal.am and fs2.e-criminal.am, which store audiovisual recordings of investigative activities, in order to allow the conducted video calls to be preserved in those repositories.

### **3.4.10 Other new processes and forms**

During the implementation of the ToR, as a result of discussion with the beneficiaries and at the request of the Client the Consultant must create and introduce new processes in the System and provide the distribution of their respective roles, functional, forms, and so on, which are aimed at achieving the purpose of the ToR set out in Section 2 of this document. Beyond the processes and forms detailed in this document, the ToR also provides for the development and implementation of up to 20 additional new processes and forms within the System.

## **3.5 Change in modules or functions in the operating system**

### **3.5.1 Change of Forms**

The forms available in the System Processes section need to be fully reviewed and modified in the following main ways:

- updating the list of forms, which implies the formation of new forms if necessary,
- reviewing and cleaning the fields of the existing forms, particularly from unnecessary mandatory fields, whereby the existing fields must be made more convenient for use and brought into line with the practice of the bodies carrying out the proceedings.

### **3.5.2 Updating the list of forms**

The testing and practical application of the system shows that in a number of situations, the 145 forms already introduced in the System do not ensure the performance of the investigative action in all situations, so it is necessary to first add a general form for all types of forms, whereas currently there is only a general decision form available. There is a need to create a form of protocol, motion, writing, and notice general. As a result of discussion with the beneficiaries general forms must include fields that are common to such documents. As a result of discussions with the Investigative Committee,



the need to define a general format for the Protocol of Examination was also raised, since four different types of examination records have been presented.

1. Protocol on conducting an inspection without video recording
2. Protocol on conducting an inspection with video recording
3. Protocol on examining the corpse without video recording
4. Protocol on examining the corpse with video recording

In this context, the Investigative Committee has presented an observation to have a general inspection protocol so that further to these four types all other inspection situations can be recorded (such as a document). In order to accomplish this processing, it is necessary to agree on the fields with the beneficiary and to create a new form to ensure the implementation of the general investigative action.

In addition to the above, it is necessary to carry out a detailed study with the main beneficiaries, the Prosecutor General's Office, the Investigative Committee, and the Anti-Corruption Committee, and to add processes and forms necessary to achieve the purpose of this task. In addition to the above, the task also envisages the development and application of an additional 20 new processes and forms in the system.

### **3.5.3 Review and Cleaning of the Fields of the Existing Forms**

In the completion of approximately 145 forms described and configured in the System's applications module, as well as during the execution of several actions, value entry is required in certain fields, many of which must not be mandatory. Unnecessary mandatory fields must be removed in coordination with the stakeholders.

In addition, all forms must be reviewed with the beneficiaries and, in coordination with them, the necessity, description, and values and scope of all form fields must be changed as necessary.

Below is an example of a decision form to initiate medical coercion proceedings, reproduced from the System. The red asterisk next to the fields in the photo means that these fields are required to be completed, but not all criminal cases and not all stages require these fields to be completed.

**Information about the form: Decision to initiate medical coercion proceedings****Time and place**

Day, month and year of the decision

20.02.2025

Place of the decision

Select

**Details**

Description: What is the decision about?

Decision to initiate medical coercion proceedings

Serial number of the criminal proceedings

16-0042-23

Introductory part

Findings

Circumstances ascertained

Reason for initiating criminal proceedings

Factual circumstances of the alleged crime

**Data of the person against whom medical coercion proceedings are being conducted**

Name

Surname

Patronymic

-

-

-

**Decision details**

What I decided

The actual decision

**Details of the officer initiating medical coercion proceedings**

Name

Manuk

\* Surname

Manukyan

2/20/25, 12:23 PM

Ccptions

Place	Malatia-Sebastia district of Yerevan	Position	Senior Lieutenant of Justice
Authority name	Investigative Committee		

Reason for initiating medical coercion proceedings

Details of supervising prosecutor

Cancel

Save

The service to be performed includes:

- As a result of the review of the legislation and as agreed with the beneficiaries, leave only those fields subject to mandatory completion in all forms that are mandatory at all stages of the proceedings and based on the necessity of the proceedings;
- As a result of the review of the legislation and as agreed with the beneficiaries, clear the irrelevant fields in all forms, and align the values of the given fields with the needs of the Client and other beneficiaries. In particular, the Investigative Committee has submitted an observation that in almost all forms that are sent to a private participant in the proceedings (the defendant, their legal representative, the defense attorney, the victim, the property defendant, the legal representative of the victim and the property defendant, and the authorized representative) or the person assisting in the proceedings (witness, his/her legal representative and attorney, expert, translator, psychologist, interpreter, attesting witness, secretary of the court session) must be provided with the warnings and explanations defined by the legislation regarding the right to remain silent, the criminal liability for refusing to testify and giving false testimony, etc.
- Rebuild the module in such a way that it will be possible to perform the actions specified in this paragraph by the Client in the future without a significant change in the program code.

### 3.5.4 Change of Statistical Module

Statistical module must enable the Prosecutor's Office, the Investigative Committee, and the Anti-Corruption Committee to produce the necessary statistics. The collection of statistics is envisaged by relevant legal norms, particularly in Article 5 of the Law on the Prosecution, Article 4 and Article 8(4) of the Law on the Investigative Committee, and Article 7(2.1) of the Law on the Anti-Corruption Committee. Detailed statistics are defined each body independently. The Prosecutor's Office presents various data related to crimes in its annual report, the collection of which should be possible through the System. Such reports and collected statistics are presented on the official website of the Prosecutor's Office (<https://www.prosecutor.am/dynamicWebPages/report>).

Statistics are kept in the Investigative Committee pursuant to the Investigative Committee's Resolution No. 169-L dated 29.10.2018 (as amended by Resolution No. 88-L dated 27.07.2021 and

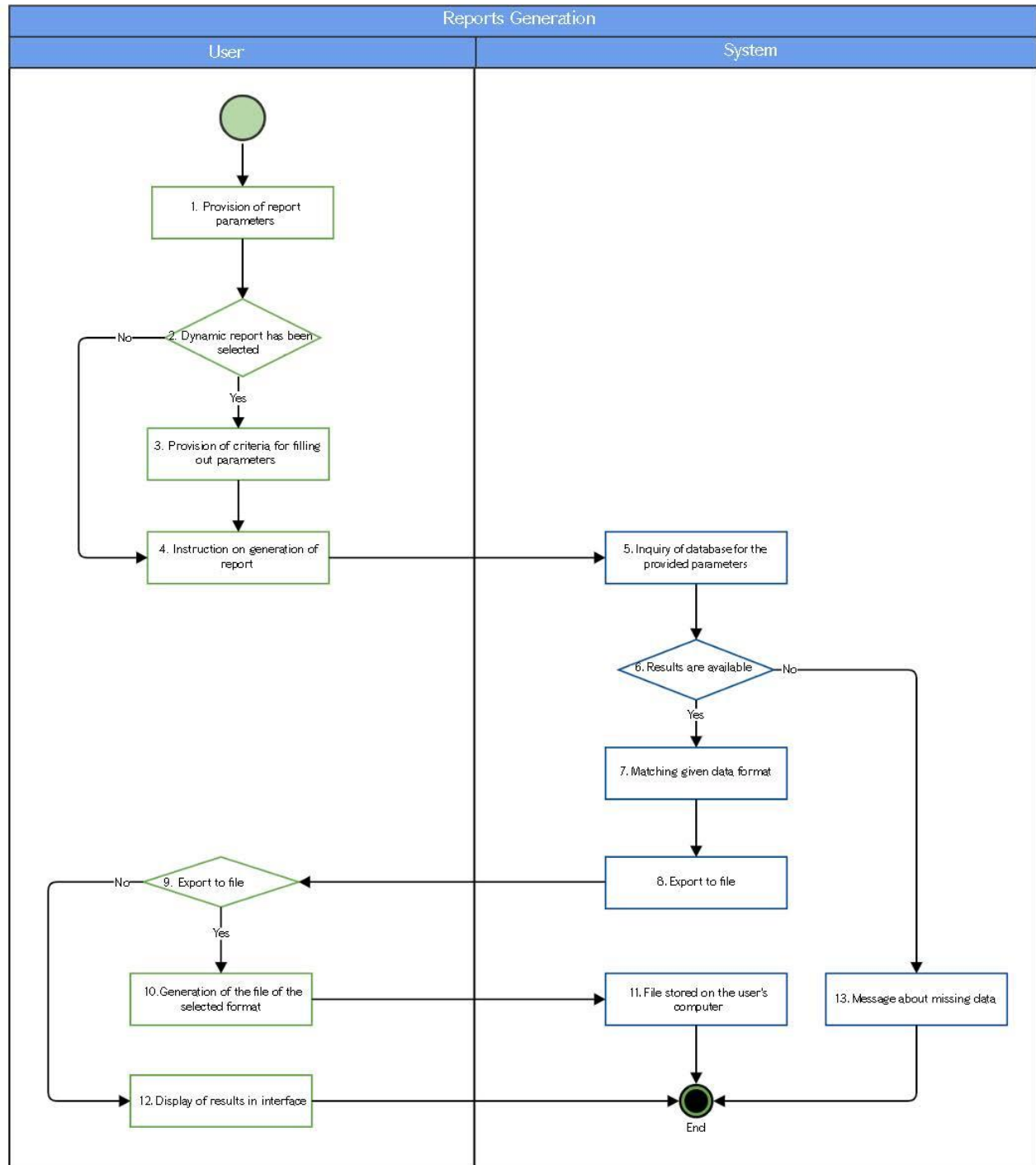
amended by Resolution No. 101-L dated 10.08.2021) and Resolution No. 180-L dated 22.12.2021 (as amended by Resolution No. 96-L dated 26.06.2022). The Resolution sets out the criteria for collecting data from all departments through mechanical completion. During the implementation of the system modification work, the information subject to collection under these Resolutions must be considered and studied and must serve as the basis for the formation of static statistical reports.

The Statistics Division of the Anti-Corruption Committee carries out records of initiating/not initiating proceedings by investigators of the Anti-Corruption Committee, as well as criminal proceedings redirected from other investigative bodies, sending criminal proceedings to court with an indictment, terminating or otherwise completing the investigation, initiating criminal prosecution against a person, suspending or resuming criminal prosecution, not initiating or terminating criminal prosecution, arresting or releasing of the detainee, applying injunction changing, eliminating, or using coercive measures, the prosecutor's decision not to approve the indictment, to revoke or not to approve the decision to dismiss and to return the criminal proceedings to preliminary investigation, etc. The Anti-Corruption Committee carries out the collection of statistics on a regular basis: weekly, monthly, quarterly, semi-annually, nine-month, and yearly.

Below are the requirements for the formation of the statistics module and reports.

### **3.5.5 Report Generation Module**

The display in the reporting interface must be user-friendly, it must be possible to group according to logical groups, and to perform a search in the list by the name of the report. Output forms and views of reports may contain: a text part typical of the form template, graphs, tables, diagrams, summaries, and other views. The reports are generated in real time, based on all the data available in the database at the time of the data request, without time deviation. During the implementation of the task, the Consultant must assess the operational workload of the System and propose the use of other servers synchronized in real time with the operational server for accountability based on the assessment. The workflow for the formation of reports, the types of modules, their functions and the ways in which they are implemented is presented below.



Step	Action	Condition	Executor	Description
1	Completion of the Report Parameters		User	The user selects the report and fills in the parameters defined for it, as needed at the moment.
2		A dynamic report has been selected	User	If the selected report is dynamic, the next step is taken, otherwise system proceeds to step 4.
3	Adding Parameter Application Criteria		User	For each filled-in variable, the user specifies the logical action applied to it: large, small, equal, contains, range, etc.
4	Report Generation Instruction		User	The user instructs generation of the report
5	Database Request as per Completed Parameters		System	The system, with the filled variables, performs a data request to the database in accordance with the predefined logic for the selected report.
6		Results Available	System	If data is found as a result of the data request, the next step is performed, otherwise system proceeds to step 13.
7	Matching the format of the received data		System	The data obtained as a result of the data request is brought to the specified form and format for export.
8	Transmitting the result to the user interface		System	The results are transmitted to the user interface

9		Export to file	User	If the user has specified the output to file checkbox in the report formation instruction, the next step is taken, otherwise the transition is made to step 12
10	File design for the selected format		User	The results are output to a file in the relevant format.
11	File stored on the user's computer		System	The system stores the file on the user's computer.
12	Displaying Results in the Interface		User	The results obtained are displayed in the user interface in a predefined form for the report: paginated data tables, graphs, or other graphical display methods.
13	Missing Data Message		System	The system displays a missing data message

### 3.5.6 Static Reports

Static reports consist of standard reports that originally have a defined amount and formats of input data, reporting time intervals (day, month, quarter, semester, year, period, etc.), and predetermined output formats. During their generation, data collected in several modules of the System at once and data obtained on the basis of their interconnection can be used.

After the user has selected the predefined parameters of the report or some of them (e.g. serious crimes, crimes against a person, completed investigation, time interval, and exported file format, PDF, DOCX, XLSX, as well as CSV, XML, JSON formats), the instruction to configure is issued. The system returns the result file according to the selected parameters or generates a message that there are no matches/no matches found.

During the task, up to 30 general and individual reports identified by the Client at the present time should be ready to be handed over by the task Consultant. During the implementation of the task, the number of them can be increased by another 10.

This list does not include the interface of each business process implementation module, nor interfaces designed for searching and deriving e-documents.

### 3.5.7 Receiving Dynamic Reports

In dynamic reports, unlike static reports, the same search parameters can be applied more than once. In addition to the search parameter, it is also possible to specify the attribute of the search execution: equal, large, large equal, small, small equal, range, contains, and so on.

Dynamic reports are also designed in accordance with the list agreed by the Consultant with the Client.

During the introduction of the ToR, up to 10 dynamic reports must be created, and the number of them can be increased by another 5 during the implementation of the ToR.

This list does not include the interface of each business process implementation module, nor interfaces designed for searching and exporting e-documents.

### **3.6 Change in the Interoperability Platform**

#### **3.6.1 Requirements for Interoperability**

The system must be equipped with a complete independent module that provides interoperability with external electronic platforms. The platform must provide the process of exchanging data with other information systems. A signal for data exchange can be both the circumstances that have arisen from the point of view of any operational logic of the System, as well as the call of a command (request) made by the user at the time of data entry. Data exchange signals can also be received from external systems. The data exchange must be carried out through the RESTfull API, the data structure, the method of exchange, and the time of occurrence of which must be designed by the Consultant during the execution phase. If the external party is not ready for interoperability for the exchange of the above-mentioned data, it must be implemented in the System in such a way that later, if possible, the interoperability will be ensured, and before that, by providing the possibility of manual data entry in the appropriate role, from the System interface. Interoperability with each platform is carried out according to a clear business process logic, specially agreed formats and data structure. For each interaction, a document describing it is presented, where the structure, validations, request, response, error messages, and examples of the data exchanged are described for each call.

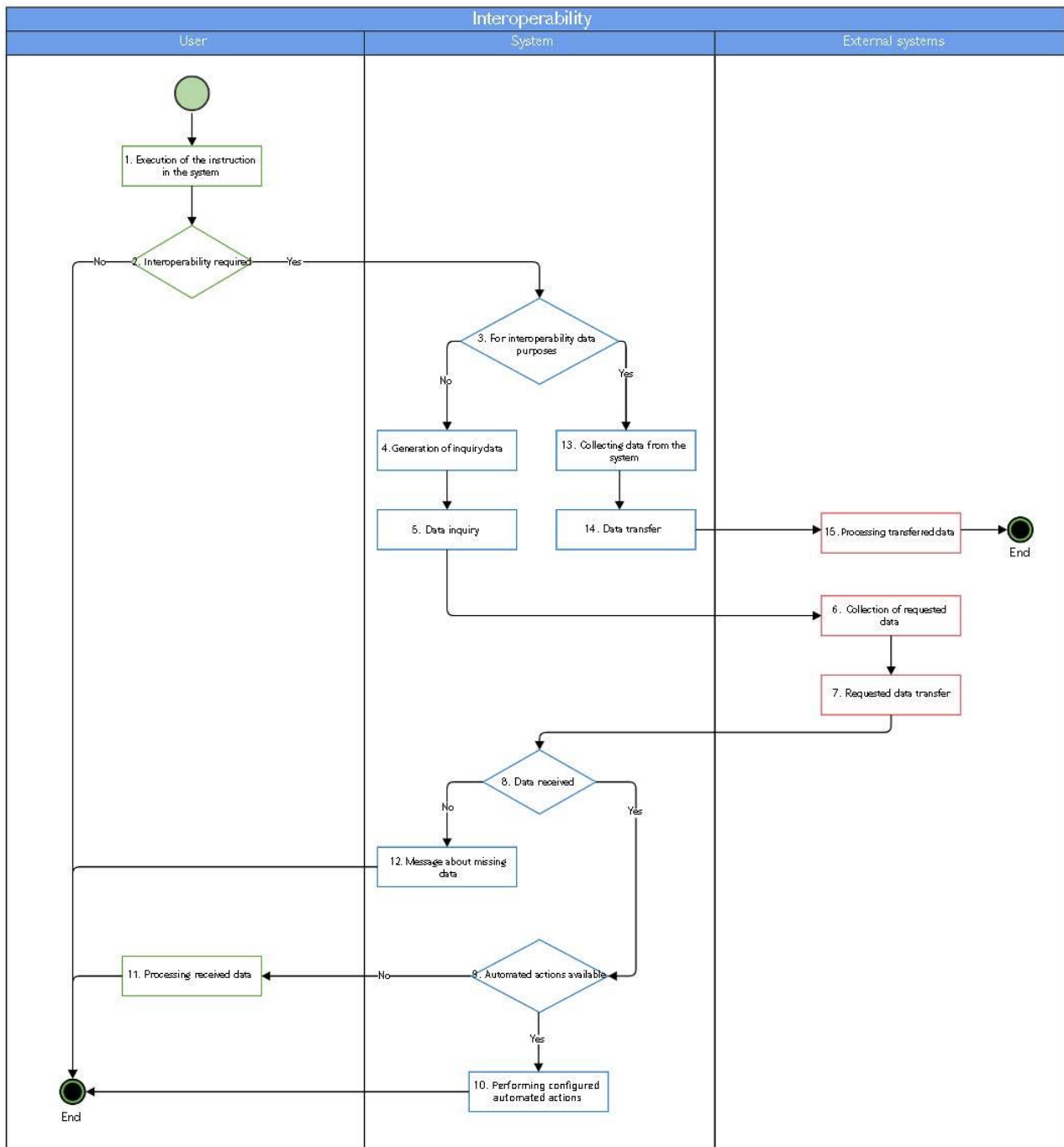
Below are the list of agencies and information systems with which interoperability must be ensured at least:

	<b>Platform</b>
1.	State Population Registry (SPR)
2	State Register of Legal Entities (SRLE)
3	Information System of the Cadastre Committee
4	Ministry of Internal Affairs Information Center
5	Traffic Police Information System
6	Movable Property Registry
7	Electronic system of the Civil Status Acts Registration Agency
8	Compulsory Enforcement Service Information System
9	E-penitentiary.am System of Penitentiary Service



10	Unified E-Notification System.
11	Central Depository
12	Judicial Department (DATALEX system)
13	Official website for public notifications
14	Statistical Committee
15	Central Bank Financial Monitoring Center
16	E-request.am
17	E-Verify.am system for issuance, archiving, and verifying the authenticity of official documents of the Republic of Armenia
18	SRC Taxpayers' Database
19	Unified Electronic Justice Platform (if present)
20	fs1.e-criminal.am and fs2.e-criminal.am system for video recording of investigative actions

If other platforms, information systems, and/or databases emerge during the implementation of the ToR, with which interoperability that is necessary for the implementation of the objectives of the ToR may lead to the automation of any action carried out by the System or automatic exchange of data, it must also be designed and implemented by the Consultant within the framework of the Contract.



Step	Action	Condition	Executor	Description
1	Implementation of the Instruction in the System	-	User	Instructions are executed by the user in the system
2	-	Interoperability Required	User	If the instruction or the action taken as a result of the instruction triggers interoperability, the next step is taken, otherwise the function is not provided.
3	-	Interoperability for Data Transfer	System	The system verifies whether interoperability is aimed at transmitting data to the electronic systems of external preferences: <ul style="list-style-type: none"> <li>• If yes, system proceeds to step 13,</li> <li>• otherwise, the next step is taken.</li> </ul>
4	Generation of Requested Data	-	System	The system receives data in a predefined format and layout for issuing the request.
5	Data Request	-	System	Data is being requested from electronic systems of external agencies
6	Collection of Requested Data	-	External Systems	Electronic systems of external preferences carry out the collection of requested data
7	Transfer of the requested data	-	External Systems	The electronic systems of the Foreign Ministries transmit the requested data to the system in accordance with the defined format and format.

8	-	Data Received	System	If data has been received as a result of the request, the next step is taken, otherwise step 12 is taken.
9	-	Automated actions are available	System	If the processing of the received data results in automatic actions in the System, the next step is performed, otherwise the transition to step 11 is made.
10	Configured Automatic Actions	-	System	The system implements the functional process logics that are designed to perform automated actions as a result of data receipt.
11	Processing of Retrieved Data	-	User	The user sees data obtained through interoperability, where the logics of the functional process for which the data were obtained are processed.
12	Missing Data Message		System	The system displays a message that no data was found as a result of the request. No further action is taken.
13	Collection of data from the system		System	The system collects data derived from the function logic in a predetermined format for transfer.
14	Data transfer		System	The system performs data transfer.
15	Processing of transmitted data		External Systems	The electronic systems of the foreign ministries carry out the processing of the data received.

### 3.6.2 State Population Registry (SPR)

SPR system is considered the only valid database of central and local population registers in Armenia. The system now has one-way interoperability with it, but in some cases this information is transferred partially or often an error occurs in the system and the data is not transferred. Interoperability must be carried out in the form of data request and must provide at least the following:

Obtaining Passport Data	<u>Data request</u> <ul style="list-style-type: none"> <li>• passport series, number</li> <li>• TIN</li> </ul>
-------------------------	--

	<ul style="list-style-type: none"> <li>• Name, surname</li> </ul> <p><u>Answer</u></p> <ul style="list-style-type: none"> <li>• All documents ever received by a person</li> <li>• Their status</li> <li>• Data stored according to the type of each document: name, last name, patronymic, date of birth, issued, valid, nationality, gender, etc.</li> <li>• Photo</li> </ul> <p><u>Result</u></p> <p>The data from the document with a valid status is filled in the relevant fields of the interface</p> <p>Data from other documents is stored as related information and can be viewed</p>
--	--

### 3.6.3 State Register of Legal Entities (SRLP)

The SRLP electronic system is the owner of the data of registered legal entities. The system has one-way interoperability with the SPR, but in some cases this information is transferred partially or partially or often an error occurs in the system and the data is not transferred. In addition, the new SRLP system is in the development phase, which means that interoperability should be applicable to the system when a new system is launched. Interoperability should be carried out in the form of data request and should provide at least the following:

Obtaining Organizational Data	<p><u>Data request</u></p> <ul style="list-style-type: none"> <li>• User passport serial, for the SRLP must include any company data, such as TIN</li> <li>• Social Card Number (Public Service Number)</li> </ul> <p><u>Answer</u></p> <ul style="list-style-type: none"> <li>• TIN</li> <li>• Name</li> <li>• Legal form</li> <li>• Legal &amp; Business Address(es)</li> <li>• Statuses</li> <li>• SEO Data</li> <li>• Beneficial Owner(s)</li> <li>• Shareholders</li> </ul> <p><u>Result</u></p>
-------------------------------	---

	The received data is filled in the appropriate fields of the interface
--	--

### 3.6.4 Cadastre Committee

The registration of real estate in Armenia is reserved for the Cadastre Committee. In criminal cases, it is often necessary to obtain information about real estate. One-way interaction with the System is necessary.

Obtaining data on the registration of property(s)	<p><u>Data request</u></p> <ul style="list-style-type: none"> <li>• Registration certificate number</li> <li>• Cadastral Code</li> <li>• Address</li> <li>• Unique Request Code</li> </ul> <p><u>Answer</u></p> <ul style="list-style-type: none"> <li>• Registration address is the address where the property is located, not the registration address.</li> <li>• Cadastral Code</li> <li>• Surface</li> <li>• Land Code (if present)</li> <li>• Surface of the plot (if present)</li> <li>• Owner(s)</li> <li>• Property Restrictions (Attachments)</li> <li>• Other</li> </ul> <p><u>Result</u></p> <ul style="list-style-type: none"> <li>• The received data is filled in the appropriate fields of the interface</li> </ul>
---	---

### 3.6.5 Police Information Center

Police Information Center is equipped with an electronic system that processes all data related to crimes and reports of individuals.

The system must receive data related to crimes from the electronic system of the Police Information Center and register the relevant crimes. Two-way interoperability between the system and the electronic system of the Police Information Center must be ensured.

Receiving data on a person's criminal record from the Police Information Center	<p><u>Data Request</u></p> <ul style="list-style-type: none"> <li>• Users' passport series, number or</li> <li>• Social Card Number (Public Service Number)</li> </ul>
---	--

	<p><u>Answer</u></p> <ul style="list-style-type: none"> <li>• Transfer of Crime Data</li> <li>• Information About Being Under Investigation</li> </ul> <p><u>Outcome</u></p> <ul style="list-style-type: none"> <li>• The received data is filled in the appropriate fields of the interface</li> </ul>
Transfer of Crime Reporting Data to the IC	<p><u>Question</u></p> <ul style="list-style-type: none"> <li>• Transfer of Crime Data</li> <li>• user passport series, number</li> <li>• Social Card Number (Public Service Number)</li> </ul>

### 3.6.6 Ministry of Internal Vehicle Registration System

The registration of vehicles in the Republic of Armenia is reserved for the Registration Unit of the Ministry of Internal Affairs. The system should be integrated into the vehicle registration system.

Receiving Vehicle Data	<p><i>Data request</i></p> <ul style="list-style-type: none"> <li>• License plate number</li> <li>• Registration number</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>• Right Registration number</li> </ul> <p><u>Answer</u></p> <ul style="list-style-type: none"> <li>• Vehicle Identification Number</li> <li>• License plate number</li> <li>• Registration number</li> <li>• Brand</li> <li>• Model</li> <li>• Year of production</li> <li>• Color</li> <li>• Owner's Name, Surname</li> <li>• Owner's Passport Data</li> <li>• Owner's Address</li> <li>• Date of Property Registration</li> <li>• Property Registration Number</li> <li>• Information about bans/restrictions</li> </ul>
------------------------	--

	<u>Result</u> The received data is filled in the appropriate fields of the interface
--	---

### 3.6.7 Civil Acts Registration Agency (CARA)

The function of the CARA is the registration of civil acts in Armenia (birth, death, marriage, divorce, etc.). The interoperability of the system with the CARA system should ensure the receipt of information about the legal registered acts of the participants during the processing of the application. The system should have one-way interoperability with the CARA .

Receipt of Registered Acts	<u>Data request</u> <ul style="list-style-type: none"> <li>• Passport series, number</li> <li>• Social Card Number (Public Service Number)</li> </ul> <u>Response</u> <ul style="list-style-type: none"> <li>• All civil acts ever registered by a person and personal data of the participants: parents, siblings/brother(s), marriage/divorce, birth of a child, recognition of paternity, adoption, renaming, death registration</li> </ul> <u>Result</u> <ul style="list-style-type: none"> <li>• The resulting data is filled in the appropriate fields on the interface.</li> </ul>
----------------------------	---

### 3.6.8 Enforcement Service (ES)

The system must ensure interoperability with the system for the processing of ES performance sheets. Two-way interoperability is necessary in order to transfer the injunction order.

Request for Information on Enforcement Proceedings	<u>Question</u> <u>On Enforcement Proceedings</u> <u>Response</u> On the materials and content of enforcement proceedings <u>Result</u> Initiation of enforcement proceedings
Transfer of information about the injunction	<u>Question</u> <u>Transfer of data for the purpose of imposing injunction</u> <u>Response</u> Initiation of Enforcement Proceedings <u>Result</u>



	Initiation of enforcement proceedings
--	---------------------------------------

### 3.6.9 Interoperability with the health system

If an individual fails to appear for a procedural investigation and cites illness as the reason, the only acceptable proof of such illness is a document issued in accordance with the format and procedure approved by the Minister of Health. On July 26, 2024, by Order No. 237-N, the Minister of Health established the official format and issuance procedure for such documentation. Under this procedure, the document should be provided with a physical signature. The healthcare sector currently uses the ARMED system. If interoperability between the ARMED system and this system is established, it will be possible to process such certificates electronically. Therefore, it is necessary to establish one-way interoperability with the ARMED system, allowing for the transfer of the electronic certificate from ARMED to this system.

Transfer of Information to the System	<p><u>Transfer</u></p> <ul style="list-style-type: none"> <li>• Medical Certificate Regarding Illness</li> </ul> <p><u>Response</u></p> <p>Response from the system regarding received information</p>
---------------------------------------	--

### 3.6.10 Unified E-Justice Platform

Ministry of Justice plans to develop and implement a unified electronic justice platform that will provide interoperability, communication, identification, management (users, rules, etc.), navigation, and so on at the highest level between all existing and designed systems. In view of this, the overall architecture of the e-criminal case system should be envisaged with the logic of expanding it into part of a larger system in the future. In particular, the user management, identification, information tables, and all other modules must be designed in such a way that it is possible to carry out an uninterrupted transition to the e-criminal case system by identified users of other electronic justice systems, review of permissions, and provision of access, taking into account the transferred data and sessions. It should also be envisaged, if necessary, for the automatic transfer of the same data from the e-criminal case system to other systems.

### 3.6.11 fs1.e-criminal.am and fs2.e-criminal.am system for video recording of criminal proceedings

The system should ensure interoperability with the fs1.e-criminal.am and fs2.e-criminal.am platforms, which store video and audio recordings of investigative actions. Two-way interoperability is necessary so that the data of criminal proceedings created in the System are automatically displayed in the system, and the access to video materials on the relevant case is automatically displayed in the corresponding section of the System on specific criminal proceedings.

Retrieval of video access from the fs1.e-criminal.am and fs2.e-criminal.am systems by the System.	<p><u>Question</u></p> <p>Criminal Proceedings Number</p> <p><u>Response</u></p>
---	--

	<ul style="list-style-type: none"> <li>• Display of the video obtained within the framework of the criminal proceedings, or the link to its access, in the relevant section of the criminal case.</li> </ul>
Transfer of criminal proceedings information from the System to the fs1.e-criminal.am and fs2.e-criminal.am systems.	<p><u>Question</u></p> <ul style="list-style-type: none"> <li>• Transfer of criminal proceedings information after initiation</li> </ul>

### **3.6.12 Correcting all system processes, including previously introduced, testing, and problem solving**

Following the handover of the System, during both the warranty period and operational use, several instances have been identified where specific actions were not executed by the System, with errors being displayed. Such cases have occurred in areas including data retrieval via the interoperability platform, execution of certain processes, and publication during form completion. Comprehensive testing of all processes is required, and all internal errors in the System should be identified and resolved.

For example, according to an observation submitted by the Anti-Corruption Committee, the System is currently inaccessible, displaying an “Internal Server Error” upon login attempt. Such issues and similar cases should be thoroughly investigated and resolved.

## **4. DELIVERABLES**

This section defines the results to be presented, the procedure and mechanisms for the implementation of the service, the format of interaction with the Client, the requirements for documentation and reporting, as well as other mandatory conditions that must be observed by the Consultant.

### **4.1. Documentation and verification**

The Consultant is obliged to submit the following documents to the Client during the program for prior approval and verification:

1	<ul style="list-style-type: none"> <li>• TOR implementation plan, including a timeline, resources, and risk management;</li> <li>• Quality Management Plan (QMP) by defining quality assurance procedures,</li> <li>• Testing plan, including test case characteristics, deliverables, and results reports. Testing results should be documented in accordance with the <a href="#">usability testing guide</a> of Ministry of High-tech Industry.</li> <li>• Change management plan in the order of registration and approval of changes,</li> <li>• Administrator and user manuals for system management and use,</li> <li>• A training plan with a description of the groups and content of the participants,</li> <li>• Deployment Plan (DP) with system installation and operation steps,</li> <li>• Reports, including minutes of meetings, interim and final reports.</li> </ul>
---	---

#### 4.2. Quality Management and Testing

2	Quality management must be carried out in accordance with a pre-developed Quality Management Plan (QMP) and Testing Plan. The quality management plan is an integral part of the program implementation plan. The test plan must include the characteristics of the test cases and the deliverables.
3	According to the timetable for the performance of the service, the Consultant should submit a version of the System that provides the full functionality of the entire portfolio of requirements.  The software must be tested in the System test environment. According to the results of the Client's user acceptance test, if the software (or part of it) tested by the Consultant lacks deficiencies and/or problems (blocking bugs) incompatible with the operation and regular operation of the part tested by the Consultant, the software may be transferred to the Client's production server.
4	For the testing of the system, an appropriate testing plan should be drawn up that will define the sequence of testing steps and actions according to the use cases and scenarios of the system, taking into account the usability guidelines developed by the Ministry of High-Technological Industry of the Republic of Armenia.
5	The Client/beneficiary independently performs acceptance testing with the help of the Consultant's business analysts to validate the full functionality and workability of the System.

#### 4.3. Implementation of Training

6	The Consultant should conduct training on the System. The training should be carried out by business analysts, architects, and the project manager for the task.
7	The Consultant should submit a training plan prior to the introduction of the system.

	<p>The training program should consist of:</p> <ol style="list-style-type: none"> <li>1. Based on the principle of training investigators, prosecutors, lawyers, and other government bodies that benefit from the system – 3,000 people.</li> <li>2. Based on the principle of training of trainers - up to 50 people to organize the training of investigators, prosecutors and lawyers.</li> <li>3. Based on the principle of training administrators responsible for system maintenance - up to 5 people.</li> </ol>
8	<p>The course description should include, but not be limited to, the following:</p> <ul style="list-style-type: none"> <li>• Course Name</li> <li>• Purpose of the Course</li> <li>• Duration of the course and the number of participants per course</li> <li>• Description of the course content and plan</li> <li>• Qualifications and experience of the trainer</li> </ul>
9	<p>During the training, the system user and administrator manuals should be presented, which should include at least the following:</p> <ul style="list-style-type: none"> <li>• description of the system/subsystem (module),</li> <li>• description of the functions,</li> <li>• practical examples/images,</li> <li>• description of the procedures for installing, issuing, restoring, backing up modules and relevant instructions.</li> </ul>
10	<p>The training shall be conducted either at the premises provided by the Consultant or, upon the Client's request, at an alternative location designated by the Client, including at the trainees' workplaces. The training language should be Armenian. If the Consultant involves a foreign expert to conduct training, translation services are paid by Consultant.</p>
11	<p>All types of information and knowledge transmitted should be documented, and the Consultant should provide all documents to the Client in both printed and electronic media.</p>

#### 4.4. Compliance with the Legislation

12	<p>The system should comply with all legislative and legal regulations regulating the sector, including the requirements set by the Ministry of High Technology of the Republic of Armenia, as well as the requirements for cloud storage, particularly the decision of the Government of the Republic of Armenia of June 14, 2024, "On the Development and Implementation of the Cloud First" policy.</p>
----	--

#### 4.5. Applied Technologies

13	During the development, modifications, and additions of the system, the Consultant should take into account the structure of the current system's data and the opportunities it offers.
14	The currently functioning system, if given the opportunity, requires the Consultant to work with software codes through a local repository (a code storage depot), on a separate software server (development server), which will also be accessible to the Client. The Consultant should upload the completed work to the software server. After testing and agreeing with the Client, the software code must be localized in the testing environment of the System for final testing, after which it will be transferred to the production server. Final testing should be conducted with the participation of both parties.
15	A unified user management system should be implemented.
16	The classifiers used should be for modules operating within the unified e-criminal case system.

#### 4.6. Productivity

17	The system should be able to provide 24/7 operation. The time for the system to be in an operational state should be more than 99.3 percent. This means that the total annual downtime of the system can be no more than 2 days. For maintenance and updates, system shutdowns should be planned and agreed upon with the General Prosecutor's Office. Emergency shutdowns of the system should not exceed a continuous 4 (four) hours, unless the reason is the lack of new equipment for the replacement of faulty equipment.
18	<p>The system should be able to efficiently serve a minimum of 50,000 users per year.</p> <p>The minimum threshold for simultaneous active users is set at 5,000 users.</p> <p>The number of simultaneous queries that should be processed through the web services designed in the system and do not affect the system's functionality is set at 500 received and responded to queries per second, including queries made in the context of data exchange with other state bodies. The aforementioned quantitative indicators need to be calculated with a growth trend of 30% for each year. The period to be accounted for is 10 years.</p>
19	At maximum load, the response time of 95% of the system's functionality must be a maximum of 5 seconds.
20	The system must be developed on the principle of one-time data entry (each subsystem must receive the data required for the job without the requirement to double enter the same information).
21	Changes and updates to the system configuration must be easily implemented and have no impact on the operation of the system.

22	The Consultant must be able to make adjustments to the system, the methods and boundaries of which will be agreed upon during the implementation of the Project.
----	--

#### 4.7. Expansion

23	<p>The system must be equipped with the possibility of expanding functionality, be equipped with dynamic scalability, load balancing for optimal use of the Client's server resources.</p> <p>It must be possible to expand the default capabilities up to 100% by horizontal and/or vertical scaling (Horizontal and Vertical scaling).</p>
----	--

#### 4.8. Interoperability

24	The system must be able to work with newly designed modules without significant structural changes.
25	The design of the system must be carried out in such a way that, in addition to entering data through the system's interfaces, users can do so through web services without directly accessing the system, as well as enter the information presented by uploading xlsx, csv files in the appropriate format.
26	The system must be designed with the architecture to fully integrate as a component of the unified electronic justice platform and must provide the capability for development in terms of full interoperability and data exchange with other component systems.

#### 4.9. Security

27	Measures must be taken to increase the level of protection against "denial-of-service" attacks (including DDoS attacks).
28	<p>At the program level, a number of access authorization (access/authorization) activities must be implemented that will ensure validated access only for intended users, including access authorization in the form of double identification. There must be specific competencies and opportunities defined for each role.</p> <p>The system must provide access through a unified YES EM platform.</p>
29	Measures must be taken at the data level to ensure the security of personal data through the secure structure of databases, particularly the security of personal data at the data level must be ensured in accordance with the decision of the Government of Armenia of February 16, 2017 "On Establishing the Procedure for the Transfer of Personal Data through the Electronic Information System and Repealing Government Decision 192-N of February 16, 2017." in accordance with the procedure for the transfer of personal data through the Electronic Information System and Regulation (EU) 2016/679 (GDPR).

<b>30</b>	The system's updating must be carried out in a way that provides information and activity logging, error logging, similar to the registration of other System actions.
<b>31</b>	Escrow of a complete copy of the software code must be ensured.
<b>32</b>	An audit of the software code must be provided.

#### **4.10. Usability**

<b>33</b>	The user interface must be user-friendly and easy to adopt. The terms used should be understandable and accessible to the end user.
<b>34</b>	The system installation/update process must be easy for end users.
<b>35</b>	The system must have an effective search mechanism. It must be possible to carry out search and filtering according to a given data element or combination of them.
<b>36</b>	When designing the interface of the system, it is necessary to be guided by the concept described in Appendix 3.

#### **4.11. Report Generation**

<b>37</b>	The system must have report generation tool.
<b>38</b>	The system must provide access to all the data collected in the reporting module for the purpose of generating reports in any combination.
<b>39</b>	Reports could be generated in DOC/X, PDF, XLS/X formats, as well as CSV, XML, JSON formats.

#### **4.12. Language selection**

<b>40</b>	The interfaces of the system must be in two languages: Armenian and English.
-----------	--

#### **4.13. Management of identified deficiencies**

<b>41</b>	<p>The software provided by the Consultant and the services provided by the Consultant must be free of design, software and other deficiencies that may lead to improper operation of the system and/or its components, failure to meet the predetermined requirements, and disruption of performance, reliability, expansion, and productivity.</p> <p>In case of discovery of a deficiency, the Client must notify the Consultant about it by presenting a description of the defect with all available arguments, which the Consultant must study and submit a reasoned proposal on the method of elimination of the defect and a reasonable deadline</p>
-----------	--

	<p>for implementation. The deadline specified by the Consultant must be no more than 5 (five) calendar days, and in case of submission of the relevant justification by the Consultant, if this justification is accepted by the Client, not more than 20 (twenty) calendar days. If it is impossible for the Consultant to carry out the task within the specified deadline, at least 3 (three) working days before the specified deadline, the Consultant must submit a proposal and justification for the extension of the deadline to the Client, and the calculation of the initial deadline and the proposed extension cannot be more than 30 (thirty) calendar days. In case of non-completion of the task within 5 (five) and 30 (thirty) calendar days, respectively, the task is considered unfulfilled.</p>
42	<p>In case of discovery of any deficiencies in the design, programming, or services provided by the Consultant during the warranty service, the Consultant must consult with the Client and eliminate the problem exclusively with his financial resources.</p> <p>The elimination of Blocker or Critical errors that appear during actual operation begins immediately after notification by the Client and cannot last more than 24 hours. In the case of more time-consuming solutions, the Consultant is obliged to propose temporary solutions that do not preclude the implementation of a major solution to the problem.</p>
43	<p>The Consultant will not be responsible for the elimination of the damage or defect in the following cases:</p> <ul style="list-style-type: none"> <li>• Improper operation or maintenance of the system by the Client,</li> <li>• natural wear and tear of infrastructure,</li> <li>• In case of making changes to the system through the Client or a third party that has not been approved by the Consultant.</li> </ul>
44	<p>The results of the system acceptance test will be classified according to the following principle:</p> <p><b>Blocker</b></p> <p>A blocking error that leads to a failure of the system, as a result of which further work with the system or its basic functions becomes impossible.</p> <p><b>Critical</b></p> <p>A critical error that results in an incorrect system logic, a security problem, a server failure, and so on.</p> <p><b>Major</b></p> <p>The main part of the functional logic does not work properly, the defect is not critical, it is possible to continue working with the system being tested.</p> <p><b>Minor</b></p> <p>A minor error that does not violate the functional logic of the part being tested, an obvious visible problem with the user interface.</p> <p><b>Trivial</b></p> <p>A minor problem that doesn't relate to functional logic, a bad reproducible error that is mostly not visible from the user interface, a problem with third-party libraries, services that has no effect on the overall quality of the system.</p>



45	<p>As a result of the testing, the system will not be accepted by the Client in the following cases:</p> <ul style="list-style-type: none"> <li>• The presence of a blocker error,</li> <li>• Critical error,</li> <li>• Presence of 2 or more Major errors, or 1 Major and 4 or more Minor errors, or 1 Major and 7 or more Trivial errors</li> <li>• 5 or more Minor errors or 4 Minor and 5 or more Trivial errors</li> <li>• 10 or more Trivial errors</li> <li>• An error in the actual environment, as a result of an update, in another system, or in another function and (or) attribute of the same system.</li> </ul>
----	---

#### 4.14. Warranty Service

46	<p>The 12-month warranty service of the system begins at the time the Client signs the System's assignment and acceptance record. The warranty maintenance of the system for 12 months begins from the moment the Client signs the Acceptance Act for the handover of the System. During the warranty maintenance period, all current deficiencies must be rectified at the Consultant's expense and through their means.</p> <p>The main maintenance hours for the system are from 9:00 AM to 6:00 PM on working days; however, since the conduct of the preliminary investigation does not imply regulated working hours, there may also be a need for maintenance during non-working hours. If necessary, in order to ensure the uninterrupted operation of the system, the Consultant will also carry out extended maintenance, receiving the relevant notification from the Client.</p>
47	<p>Corrective maintenance - correction of some errors, malfunctions, or improvement in the system's performance identified during the application of the system.</p> <p>Adaptive maintenance - if necessary, the installation of the system in a new environment (other equipment, operating system, data center, cloud, etc.).</p> <p>Perfective maintenance is the introduction and change of new functional requirements that may arise from changes in the law, requirements for the most efficient use of the system, and so on. For example, a certain number of simultaneous transactions were planned, but after a while, their growth is predicted. Changes in the system (in this case, non-functional, productive) must be made in advance to avoid further disruptions.</p>
48	<p>Software maintenance must include at least:</p> <p>Implementation of non-extensive changes necessary to ensure the smooth operation of the system (non-extensive program changes in the system related to legislative changes and not only).</p> <p>Providing advice on the regulation and maintenance of the data exchange network between the system and its users.</p> <p>Providing advice on the regulation and maintenance of equipment that ensures the smooth operation of the system.</p> <p>Investigation and correction of errors/deficiencies in the System, including providing temporary solutions and bypassing deficiencies until System adjustments and updates.</p>

	<p>Developing, testing, installing updates.</p> <p>Providing and installing new software versions, as well as updating relevant documents and materials.</p> <p>Regulating the system when its inoperability is attributed to software defects or errors.</p> <p>Support for restoring and correcting lost, damaged data, correcting incorrect data.</p> <p>Creation and integration of new modules as needed.</p>
--	--

#### **4.15. Control**

<b>49</b>	The Consultant shall work closely with the Client.
<b>50</b>	The Consultant must support the Client and the Beneficiaries in verifying the process and quality of the service provided.
<b>51</b>	The Consultant must submit periodic and final reports to the Client.
<b>52</b>	Reports must be provided in paper and electronic form. The Client is obliged to accept or reject them within 30 calendar days of receipt of the reports. In the event of failure to express a written position on the report after the expiration of the deadline, it shall be deemed accepted.

#### **4.16. Legal Terms**

<b>53</b>	The requirements for intellectual property, other rights and warranties are set out in Appendix 4.
-----------	--

#### **4.17. Additional Conditions**

<b>54</b>	The Appendices to this document set out additional requirements that have equal legal force to the requirements set out in this document. The requirements recorded in the Appendices to this document are mandatory for the Consultant.
-----------	--

#### **4.18. Equipment**

The equipment necessary to install the System changes shall be provided by the Client. Currently, the System is located in the server domain, the description of which is presented in Appendix 5.

#### **4.19. Privacy**

The Consultant and/or the subConsultant providing services on their behalf undertake to keep confidential all information that is not publicly available and will not undertake any other assignment that will lead to a conflict of interest.

The Consultant and/or the subConsultant providing services on their behalf are obliged not to provide any information obtained in the framework of the work without the written consent of any party (except for the persons specified in the organizational structure of the projects), regardless of the form of receipt (written, oral, electronic, etc.).

Within 30 days after termination of the contract, the Consultant and/or the subConsultant providing services on their behalf must destroy the information received within the framework of the contract, regardless of form and content, except in cases where the legislation of the Republic of Armenia requires their retention.

SLA (Service Level Agreement) shall be signed between the Client and the responsible department of the Consultant.

NDA (non-disclosure agreement) shall be signed between the Client and the Consultant.

## 5. REQUIREMENTS FOR CONSULTANT

The Consultant must have sufficient resources and capacity to carry out the Services. In particular, the Consultant must meet the following minimum requirements

A Consultant must have:

- Experience in the design, development, and implementation of information systems for criminal cases or pre-trial proceedings in at least one country;
- Experience in carrying out tasks of similar scale and complexity,
- Experience in developing e-government systems,
- Experience in system architecture design and system integration,
- Technical support and training experience,
- Experience in implementing programs funded by international development organizations.

A Consultant must assemble a team of experts or consultants to achieve the desired Results. A Consultant can recommend the composition of the team to ensure cost-effectiveness and high-quality results. The advisory team must consist of at least the following core experts who will have the minimum qualifications set.

	Name	Description	Quantity (human)
1	Project Manager	<ul style="list-style-type: none"> <li>- Bachelor's degree or higher in higher education in management, information technology, economics, law, public administration, or related fields;</li> <li>- At least 10 years of experience in information technology projects or in a leadership position or in public sector collaboration projects aimed at modernization reforms;</li> <li>- At least one similar project management experience;</li> </ul>	1

		<ul style="list-style-type: none"> <li>- Significant experience of collaboration with various stakeholders in the public and private sectors;</li> <li>- Knowledge of English is required</li> </ul>	
2	Senior Expert in Functional Assessment	<ul style="list-style-type: none"> <li>- Bachelor's degree or higher in higher education in management, information technology, economics, law, public administration, or related fields;</li> <li>- At least 7 years of practical experience in the field of functional, governance or policy reform, with experience in developing laws or regulations;</li> <li>- Skills in classifying active/applicable business processes in legislation on electronic governance,</li> <li>- Experience of participating in at least one similar project,</li> <li>- Knowledge of English is required</li> </ul>	1
3	Quality Assurance Specialist	<ul style="list-style-type: none"> <li>- At least 3 years of experience in IT projects,</li> <li>- Experience in designing the architecture of similar systems and managing a database;</li> <li>- Higher education in the IT industry and/or relevant experience, as well as knowledge of English</li> </ul>	1
4	Senior Programmer	<ul style="list-style-type: none"> <li>- At least 7 years of experience in IT projects,</li> <li>- Experience in designing the architecture of similar systems and managing a database;</li> <li>- Higher education in the IT industry and/or relevant experience, as well as knowledge of English</li> </ul>	1
5	Programmer	<ul style="list-style-type: none"> <li>- At least 3 years of experience in IT projects</li> <li>- Experience in developing similar system(s) or part thereof</li> <li>- Higher education in the IT industry and/or relevant experience, as well as excellent knowledge of English</li> </ul>	1
6	Training Expert	<ul style="list-style-type: none"> <li>- At least 5 years of experience in the field of comprehensive training, preliminary qualification and professional growth in the use and support of TT systems,</li> <li>- At least 3 years of experience in the field of training in project management, criminal case solutions,</li> </ul>	1

		<ul style="list-style-type: none"> <li>- Experience in the transfer of knowledge and skills and knowledge of English,</li> <li>- Higher education in the IT industry and/or relevant experience</li> </ul>	
--	--	--	--

## 6. REPORTING REQUIREMENTS AND SCHEDULE OF RESULTS

The development and introduction of the new system is planned to be carried out in the following stages: within 12 months.

The implementation of each phase is expected to begin after the successful completion of the previous phase. However, the Consultant may, with the consent of the Client, initiate the simultaneous performance of several parallel actions provided for in different stages of the Service Schedule. For example, training can be initiated and carried out in parallel with the implementation of the ToR.

N	Phase	Actions	Timing
1	Starting phase	Meeting with the Client's representatives and stakeholders	2 months
		Study existing needs and legal codes related to the technical task	
		Clarification of basic actions, possible volume of data, volume of actions, volume of changes, etc.	
		Final Development of system specifications (hereinafter, SSP) with a detailed blueprint	
		Presentation of the preliminary report, which will include a description of the system changes, interoperability processes, detailed business processes and user roles related to the system changes, a description of data exchange, and templates for standard documents (intermediaries, decisions, and other documents), recommendations regarding the design of the system changes, software and technical specifications, etc.	
		Other documents relating to the development of changes to the System covered by this ToR.	
		Acceptance of service done in the first phase by the Client	

2	Developing System Changes	Development of the final version of SSP-defined and previously approved software		4 months
		Implementation and integration of data exchange and interoperability between necessary electronic databases		
		Modified System Testing (including functional, security, convenience, and compatibility testing)		
		Modified System Operation in Test Mode		
		Installing a Modified System on Equipment Provided by the Client		
		Submission of a report on the phase, including information on the final System Testing		
		Acceptance of service done in the second phase by the Client		
3	System Operation and Training	System Investment and Final Configuration		6 months
		Development and presentation of a training program for users of the system to the Client		
		Training of employees and trainers on the use and maintenance of the system		
		Running the system		
		After the installation and final configuration of the system, the following tests of the system will be carried out to determine their compliance with the requirements for acceptance:		
		1. All actions taken for the design and construction of each type of business process in the system must meet the requirements of this document and other documents prepared and approved within the framework of the	For each type of business process, the Consultant must demonstrate performance and compliance with the requirements of this document and other documents prepared and approved in the framework of the	

		development of the System.	development of the System	
		Through the signing of the Agreement, the transfer of all intellectual property rights (including exclusive property rights to copyright and patent rights) to the Office of the General Prosecutor in accordance with the rules laid down in this document, without additional compensation.		
		Establishing and implementing safety requirements for the system		
		Providing all software codes (source codes) to the Client in accordance with the requirements set out in this document		
		Provision of Developed User Manual(s)		
		Signing of the Warranty Service Agreement between the Prosecutor General's Office and the Consultant		
		Provision of Complete Source Code for the Completion Report and System		
		Acceptance of the service done in the third phase by the Client		

## 7. ORGANIZATIONAL ISSUES

The Client is the Office of the Prosecutor General of Armenia, as well as the Office of the Prime Minister of Armenia. The Prosecutor General's Office is responsible for accepting the services provided by the Consultant under this Assignment, and is therefore also responsible for signing the relevant acceptance document for those services. The Office of the Prime Minister is responsible for making all payments related to this Assignment, based on the payment request submitted by the Consultant, the acceptance of the delivered service, and the approval of that service (or relevant phase) by the Prosecutor General's Office. All expenses, such as office space, IT and office equipment, communication means, transportation, etc., as well as costs associated with training (e.g., training room, simultaneous translation, coffee breaks, printing materials, etc.), will be covered by the Consultant.

# INFORMATION MATERIALS

## Current Information System

### 1.1. The current state

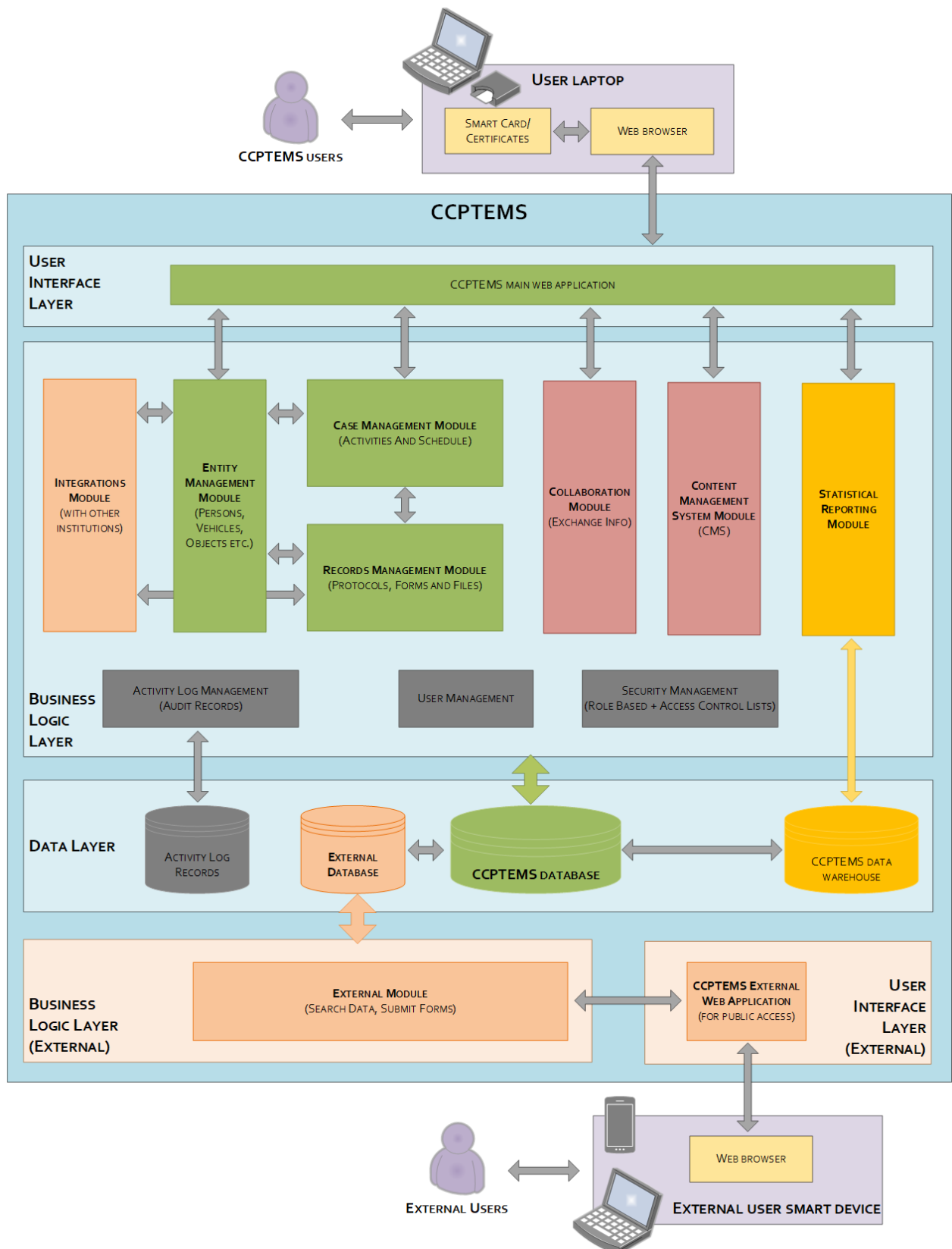
Currently, the system ensures the implementation of all investigative actions when used in the test domain, but there is still a need to carry out service for the development of the system. The need for the development of the system is conditioned by the need to adapt the operation of the System to the legislative changes that have taken place since its introduction, as well as to finalize the operation of some modules and to implement them smoothly.

### 1.2. The modular structure of the system

The system is designed with a modular structure, with each module operating independently in accordance with its functional logics, forming part of the whole with all its connections. Details of the architectural design of the system are presented in Appendix 1. The modules designed in the system are:

1. Interoperability platform module,
2. Confirmation Management Module,
3. Form management module,
4. Case Management Module,
5. User management module,
6. Security management module /role definition and access control/,
7. Statistical reporting module,





### 1.3. Roles Defined in the System

The system has roles and users. The system provides for the following roles:

1. Prosecutor General,
2. Deputy Prosecutor General
3. Headquarters,
4. Senior Prosecutor,
5. Supreme prosecutor and Supervising Prosecutor,
6. Director of the Investigative Authority,
7. Deputy Director of the Investigative Authority,
8. Investigator,
9. Administrator.

#### **1.4. Business Processes and Forms of the System**

The system has digitized 65 business processes. The system contains forms developed for each business process. For example, the process of initiating criminal proceedings has several forms: report from a natural person, report from a legal entity, record of initiating proceedings, etc. The total number of all forms is 145.

Business processes carried out by the system are:

1. Initiation of Criminal Proceedings
2. Forms of Refusal to Initiate Criminal Proceedings
3. Termination of Criminal Proceedings
4. Preliminary investigation progress and completion forms
5. Procedure for not initiating or terminating public criminal prosecution
6. Checking the Evidence on the Spot
7. Taking objects or documents
8. Personal Search
9. Search
10. Seizure
11. Confrontation
12. Investigation
13. Exhumation
14. Experimentation

15. Testing (Sampling)
16. Request for information
17. Examination
18. Questioning of the accused
19. Interrogation of the arrested man
20. Witness/Victim/Expert Interrogation Forms
21. Notifications to Private Participants in the Proceedings
22. Recognition
23. Secret investigative actions
24. Public criminal prosecution and indictment
25. Suspending deadline for public criminal prosecution
26. Arrest in the event of a reasonable suspicion of having committed a crime
27. Arrest to bring defendant at liberty to court
28. Arrest of the defendant for violating the terms of the preventive measure
29. Arrest or detention of a minor
30. Suspension of criminal prosecution
31. Releasing the detainee
32. Compulsory submission to proceedings conducting body
33. Warning
34. Limitation of the exercise of the right
35. Removal from the Proceedings
36. Administrative Supervision
37. Application of the Pledge
38. Return of Pledge
39. Disciplinary supervision
40. Warranty
41. House Arrest
42. Military control
43. Prohibition of absence

44. Injunction, Conservation, and Removal of Property
45. Suspension from office
46. Application of preventive measures or extension of the term
47. Changing or revoking preventive measure
48. Detention
49. Application for lifting detention or applying an alternative preventive measure instead of detention
50. Placement in a medical facility for an examination
51. Family supervision
52. Medical supervision
53. Renewing uninitiated or terminated criminal prosecution
54. Appeal
55. Mediation
56. Consolidation and separation of criminal proceedings
57. Relations between Public Participants in the Proceedings
58. Exemption from Participation in the Proceedings
59. Conducting the preliminary investigation by the investigative group
60. Initiating public criminal prosecution against a legal entity
61. Initiating and Terminating Medical Coercion Process
62. Motion for Special Trial Order against a Defendant Who Has Signed a Cooperation Agreement
63. Preliminary investigation conducted through cooperation proceedings
64. Procedure and resolution for submitting a cooperation petition
65. Removing the investigator/prosecutor from the case

The forms developed in the system are:

1. Report on Crime
2. Reporting - Legal Entity
3. Reporting - State or local self-governing body or its official
4. Transmitter - Physical Person
5. A Record of Initiating Proceedings

6. Scripture
7. Decision to Shorten the Proceedings
8. Decision to Grant/Reject the Motion
9. Decision to Satisfied/Reject the Complaint
10. Decision to Reject the Decision to Abolish Behavior
11. Notice
12. Scripture
13. Decision to Abolish Proceedings
14. Indictment
15. Decision to Grant/Reject the Motion
16. Decision to Satisfied/Reject the Complaint
17. Decision to reject the motion for criminal prosecution
18. Decision not to prosecute or terminate public criminal prosecution
19. Motion for Not Prosecution/Termination of Criminal Prosecution
20. Notice
21. A Record of Checking the Index on Spot Without Video Recording
22. A Record of Checking the Evidence on the Spot
23. Record of taking objects or documents
24. Search Decision
25. Mediation
26. A Record of Conducting an Investigation Without Video Recording
27. A record of a video search
28. Decision of confiscation
29. Mediation
30. A Record of Confiscation Without Video Recording
31. Record of confiscation through video recording
32. Notice
33. A Record of Face-to-Face
34. Notice

35. A Record of Conducting an Examination Without Video Recording
36. Record of Examination by Video
37. A Decision to Make a Mistake in Artaxerxes
38. A Record of Performing Without Video Recording
39. Record of Extraterrestrial Recording
40. A Decision of Experimentation
41. A Record of Conducting a Criminal Trial Without Video
42. A Record of Conducting a Trial by Video
43. Decision of Probation
44. Mediation
45. A Record of Testing Without Video Recording
46. A Record of Testing by Video
47. Decision on Sampling
48. A Record of Sampling Without Video Recording
49. A Record of Sampling by Video
50. Determination of the Requirement for Information
51. Record on the Requirement for Information
52. A Record Without a Video Inspection
53. Decision to conduct an initial examination of the scene
54. A Record of Examination by Video
55. A record of examining the corpse without a video recording
56. A record of examining the corpse by video recording
57. Record of the Defendant's Interrogation
58. Record of the interrogation of the arrested person
59. Record of Additional Witness Interrogation
60. Record of the Victim's Interrogation
61. Record of Witness Interrogation
62. Record of an expert's interrogation
63. Notice

64. A Record of Self-Identification
65. Record of Recognition of the Corpse
66. Record of Object, Document, Animal Recognition
67. A record of recognizing a person outside his or her visual observation
68. Mediation
69. Intervention for Secret Criminal Actions
70. Assignment for Investigative Action
71. Decision on Criminal Prosecution
72. Decision to reject the motion for criminal prosecution
73. Mediation
74. Decision to abolish the decision to prosecute and discontinue criminal prosecution
75. Decision on Victim Identification
76. Decision to Grant/Reject the Motion
77. Decision to Satisfied/Reject the Complaint
78. Decision to suspend the deadline for public criminal prosecution
79. Mediation
80. Decision to release the detainee
81. Record of Arrest of a Person
82. Decision on Arrest
83. Decision on Arrest
84. Decision on Arrest
85. Mediation
86. Decision to release the detainee
87. Decision on Arrest
88. Decision to Terminate Criminal Prosecution for a Crime Attributed to a Minor
89. Motion to Stop Criminal Prosecution
90. Decision to release the detainee
91. Decision on Compulsory Submission of a Conducting Body
92. Protocol on Fixing the Fact of Compulsory Submission

93. Protocol on the Release of a Person
94. Warning
95. Decision on the Restriction of the Exercise of Rights
96. Decision to Satisfy/Reject the Complaint
97. Decision to remove a person from proceedings
98. Decision to Abolish the Investigator's Decision
99. An Intervention for Administrative Control
100. Decision to Use a Pledge
101. Decision on turning the pledge into state income
102. Decision to return the pledge
103. Decision to Change or Eliminate Measure of Restraint
104. Decision on the Use of Disciplinary Supervision
105. A Record on the Use of Disciplinary Supervision
106. Protocol on the Use of Warrant
107. Decision to Use Warrant as a Measure of Restraint
108. Motion for the Use of Home Detention
109. Decision on the Use of Military Surveillance
110. Protocol on the Use of Military Control
111. Decision on the application of the prohibition of absence
112. Decision on Injunction of Property
113. Decision to Remove Property Injunction
114. Protocol on Injunction of Property
115. Decision on Suspension of Administration
116. Application for Use of a Measure of Restraint or Extension of the Deadline for a Measure of Restraint
117. Decision to Change or Eliminate a Measure of Restraint
118. Motion
119. Motion
120. Motion for Medical Supervision
121. Decision on Family Surveillance



122. Protocol on Family Surveillance
123. Motion for Medical Supervision
124. Decision not to prosecute criminal prosecution and to prosecute criminal prosecution
125. Decision to abolish the decision to terminate criminal prosecution and to renew criminal prosecution
126. Decision to Upheld/Reject the Motion
127. Mediation - Extension of Proof Deadline
128. Decision on Merger / Separation of Criminal Proceedings
129. Assignment for Investigative Action
130. Motion
131. Decision to Exempt from Participation in the Proceedings
132. Decision on Investigation by the Investigation Team
133. Decision on Public Criminal Prosecution of a Legal Entity
134. Record of Public Criminal Prosecution of a Legal Entity
135. Decision on the Initiation of Medical Compulsory Proceedings
136. Record of Failure to Participate in Medical Compulsory Proceedings
137. Motion for the application of a special trial order against a defendant who has entered into a cooperation agreement
138. Decision to satisfy or reject a cooperation motion
139. Cooperation Agreement
140. Motion
141. Cooperation Motion
142. Motion not to initiate/terminate public criminal prosecution
143. A record confirming the fact of compulsory submission
144. A record of the release of a person
145. General Form

### 1.5. The current state of the system according to some modules

This Appendix presents the current state of some of the modules available as a result of the testing of the System, mainly presenting in a non-exhaustive way the problems that are addressed in the main text of the ToR.

### 1.5.1. Role Management

#### Internal users

During the design and development phase of the system, two categories of user roles were considered: internal users and external users. Internal users were the prosecutor's office and investigative bodies, primarily for the digitalization of whose functions the System was designed. Disaggregation among investigators and prosecutors:

1. Prosecutor General,
2. Deputy Prosecutor General
3. Head Office,
4. Senior Prosecutor,
5. Supervising Prosecutor and Supervising Prosecutor,
6. Director of the Investigative Authority,
7. Deputy Director of the Investigative Authority ,
8. Investigator.

Some of the internal users will have supervisory and leadership functions in addition to their basic functions as investigators or prosecutors. For example, the Anti-Corruption Committee has the roles of "head of the investigative unit, deputy head of the investigative unit, direct supervisor of the investigator," who perform leadership functions and have the right to give instructions to a specific investigator. In addition, the internal structure of the Prosecutor's Office also implies the implementation of other supervisory and leadership functions in addition to the functions described in these roles. All of this is reflected in the relevant legal codes, particularly in Article 187 of the Code of Criminal Procedure, which defines the order of superiority in the body of<sup>1</sup> investigation, as well as in Article 31 of the Law on the Prosecutor's Office, which defines subordination in the prosecutor's office<sup>2</sup>. The system must provide an opportunity to carry out supervisory and subordinate functions by

---

<sup>1</sup> Article 187. Procedural Superiority in the Investigation Body

1. The supervisor of the investigative body is the direct supervisor of the investigator who is directly subordinate to them.
2. The direct supervisor of the deputy supervisor of the investigative body is the supervisor of the body of inquiry.
3. The direct supervisor of the head of the unit who is not part of any unit of the body of inquiry is the head of the body of inquiry or his deputy under the coordination of that unit.
4. The direct supervisor of the deputy head of the unit of the body of inquiry is the head of that unit.
5. The direct supervisor of the head of the unit, who is not under the coordination of any deputy head of the unit of the investigative body, is the head of that unit.
6. The direct supervisor of the head of the unit under the coordination of the deputy head of the unit of the investigative body is the deputy head of the unit.
7. The direct supervisor of investigators under the coordination of the deputy head of the unit of the investigative body is the deputy, and the direct supervisor of the other investigators in that unit is the head of that unit.
8. The direct supervisor of investigators for the supervisor of the investigative body or the head of any of its units is the head of the body of investigation or the head of its corresponding unit.
9. The investigator has one direct supervisor within the framework of the proceedings.

<sup>2</sup> Article 31. Subordination in the Prosecutor's Office

1. The activities of the prosecutor's office are based on the principle of subordination and unity.
2. The Prosecutor General is superior to all prosecutors.
3. The Deputy Prosecutor General is superior to all prosecutors in his or her system.
4. The head of the structural division of the Chief Prosecutor's Office is superior to all prosecutors in that division.

the appropriate entities. The task of ensuring all of this is presented in paragraphs 3.2 to 3.4 of the Task.

## External users

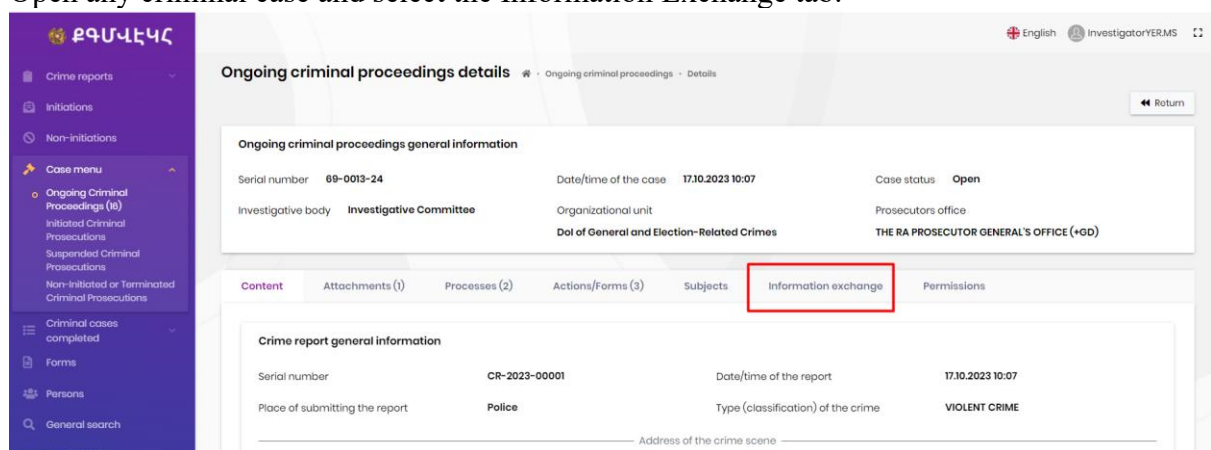
External users are all users who are not internal users and must receive information or materials from internal users in any way. Currently, access by external users to the system is done through a one-time generated link that directs the external user to the file access domain, and access to these files has already been provided by the internal user. The system enables the use of a one-time generated link created for that external user notification via email notification. Such a solution is not convenient, it does not ensure the effective implementation of their functions by external users. The task of providing a more efficient solution for external users is presented in paragraphs 3.2 to 3.4 of the ToR.

### 1.5.2. Interoperability with other external systems

The system has an interoperability module, which, however, is now only interoperable with a limited number of systems. The system is obtained from the following databases: Police State Registry of Population and the State Registry of Legal Entities. Data from these databases automatically comes to the System through a data request. In some cases, that information is moved partially or an error occurs and the data is not moved.

The system has developed an interface for the interoperability platform, which will work only if the appropriate external systems are connected to the system through interoperability channels. Below are the rules for using this platform:

1. Open any criminal case and select the Information Exchange tab.



The head of the structural division of the Central Military Prosecutor's Office is superior to all prosecutors in that division.

6. The Deputy Military Prosecutor is superior to all prosecutors in his or her system.

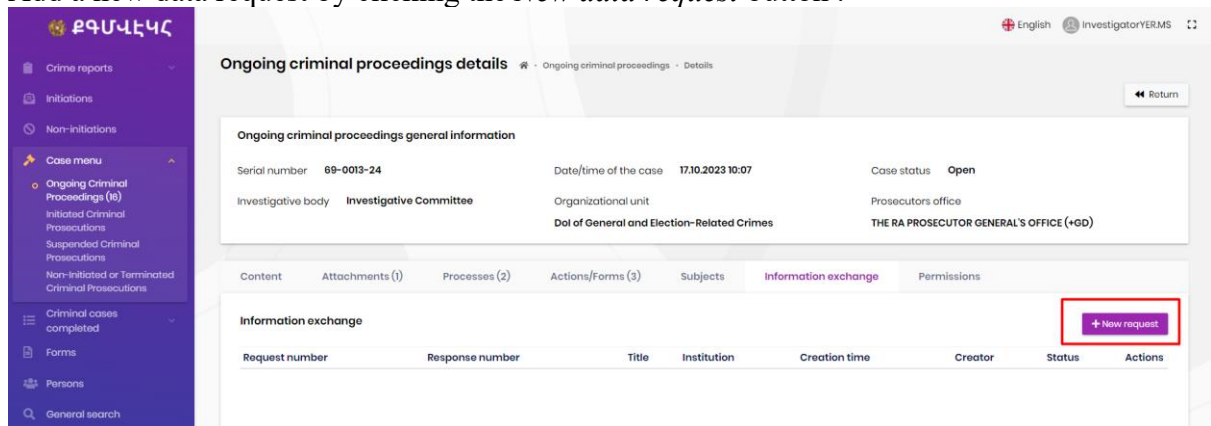
7. The Armenian Prosecutor is superior to the prosecutors of the Armenian Administrative Regions, all the prosecutors of the Armenian and Armenian Administrative Regions.

8. The district attorney is superior to all prosecutors in the district attorney's office.

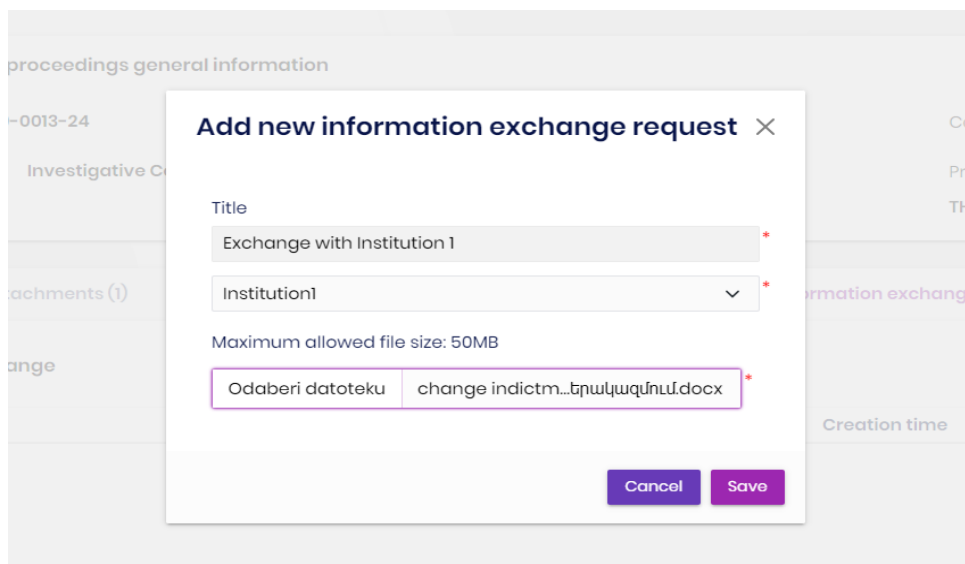
9. The prosecutor of the Armenian Administrative Region is superior to all prosecutors of the Armenian Administrative Region.

10. The military prosecutor of the garrison is superior to all prosecutors of the military prosecutor's office of the garrison.

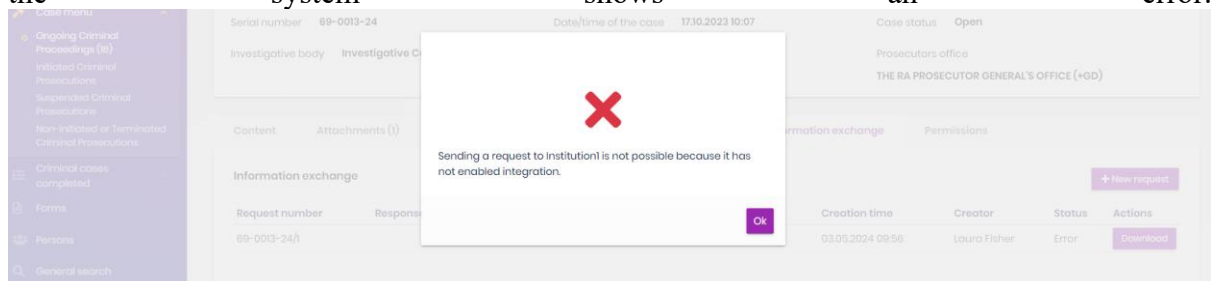
2. Add a new data request by clicking the *New data request* button .



3. Enter the title of the data request, select the institution, select the attached file, and click Save.



4. If the selected institution does not have an information exchange service embedded on its side, the system shows an error.



5. The data request is recorded in the system. If the selected institution introduced information exchange service, the status of the data request will be *Sent*. Otherwise, the status would be *Error*.

Ongoing criminal proceedings general information

Serial number

69-0013-24

Date/time of the case

17.10.2023 10:07

Case status

Open

Investigative body

Investigative Committee

Organizational unit

DoI of General and Election-Related Crimes

Prosecutors office

THE RA PROSECUTOR GENERAL'S OFFICE (+GD)

Content

Attachments (1)

Processes (2)

Actions/Forms (3)

Subjects

Information exchange

Permissions

Information exchange

+ New request

Request number	Response number	Title	Institution	Creation time	Creator	Status	Actions
69-0013-24/1		Exchange with Institution 1	Institution1	03.05.2024 09:56	Laura Fisher	Error	Download

The response sent by the institutions is recorded in the system with the status Received.

### Interoperability with the planned e-criminal court

The system for electronic judicial proceedings (e-criminal court) in criminal cases is not yet available. The requirement for electronic registration of judicial proceedings is envisaged by law from September 1, 2025 (Article 483 (12.1) of the Code of Criminal Procedure), but the tender has not yet been announced. However, electronic pre-trial proceedings cannot be completely effective unless there is a possibility of submitting electronic files to the court. Under these circumstances, this document presents solutions for integration with the court, which are set out below.

The task related to interoperability is presented in Task 3.6. of the ToR.

### 1.5.3. Statistical Module

The statistical module has been developed in the system; however, it is currently not in use due to the absence of full implementation of the system and the lack of agreement on the final report formats with the system developer and key stakeholders.

The task of designing a statistical module is presented in chapters 3.5.4-3.5.7 of the ToR.

## 1.6. Related documents

The following legislative acts and materials have been used in designing the task:

- Criminal Procedure Code (LA-306-N, adopted 30.06.2021),
- Law on the Prosecution (LA-198-N, adopted 17.11.2017),
- Law on the Investigative Committee of the Republic of Armenia (LA-25-N, adopted 19.05.2014)
- Law on the Anti-Corruption Committee (LA-147-N, adopted 24.03.2021),
- Law On Operational-Intelligence Activities (LA-223-N, adopted 22.10.2007),
- ToR of the Electronic Management System for Pre-Trial Criminal Proceedings,
- A report compiled by Sigma Lo Group LLC in 2023 submitted to the World Bank "Digital Infrastructure of the Electronic System: Analysis and Proposals of the Current Situation, Legal and Technical Problems".
- Etc.



# APPLICATION OF PRINCIPLES OF SERVICE DESIGN AND DIGITAL ARCHITECTURE IN THE REPUBLIC OF ARMENIA

In order to comply with the standard "Compliance of the created digital service with user experience (UX) standards," the participant must ensure the implementation of the following functions:

### 1. Non-functional requirements: user experience and design

1. All pages, online forms, and menus of the designed service must utilize the components of the [Henaket](#) (Baseline) official design system.
2. When constructing pages, online forms, and menus, the previously defined "Templates" must be followed. If there is no template available for a specific case, the service page must always be constructed using the components of the "Baseline" official design system.
3. To create clear and consistent web content (text), it is necessary to adhere to the requirements for creating accessible content.
4. The service should have a web page that is as simple as possible, with a clear title.
5. Online forms for the service must be built using a step-by-step approach, focusing on usability and not replicating paper templates. When creating online forms, it is essential to follow the guidelines established by the Ministry of High-Tech Industry.
6. The service must be technically separated from the website of the government body and have its own unique link.
7. The service and accompanying information must be available in Armenian, Russian and English.

### 2. Non-functional requirements: testing of a service prototype with users and presentation of evidence

1. The prototype of the service must be tested with users using [the usability testing guidelines developed by the Ministry of High Technology Industry](#).
2. Users should not only be considered the "experts" involved in the system, but also the users who will use the system in the future.
3. When reviewing user needs, users who need additional support (e.g., the elderly, people with disabilities) must also be considered.
4. When testing the availability of the service, it is necessary to follow the [7th digitization standard](#) developed by the Ministry of High-Tech Industry, which states that the newly created service must meet at least the AA level of the Web Content Accessibility Guide (WCAG 2.1).
5. Proof of usability testing must be submitted as part of the Handover-Acceptance Act. This evidence must also be in the form of actions taken as a result of usability testing to improve the functionality of the system (in the form of notes or documented updates).

The results of the testing must be documented [in accordance with the usability guidelines](#) developed by the Ministry of High Technology.

**3. Non-functional requirements: Evaluation and improvement of service quality within the framework of the implementation of the "Public Administration Reform Strategy" adopted by the government.**

1. The designed service needs to be constantly measured and evaluated. To this end, the following 4 fundamental indicators set out in the Digitalization Guide of the High Technology Industry [must be applied](#):

1. the services (pages) with the most visits,

2. user satisfaction of online services,

3. the proportion of successful transactions,

4. the portion of online transactions of the service.

2. Indicators must be calculated periodically using analytical tools in accordance with the Digitization [Guide of the Ministry of High Technology Industry](#).

3. It is necessary to ensure the transition from old service technology to new technologies without significant service disruptions.

4. It is necessary to carry out quality assurance (QA) testing periodically in accordance with the [10th Digital Standard of the Ministry of High Technology](#).

**4. Non-functional requirements: Creating a reliable and secure service.**

1.To access the service in order to identify users, it is necessary to use the national digital identification platform "YES EM" (IT'S ME).

2.In order to identify and respond to software problems, it is necessary to carry out proper monitoring using one or more of the recommended tools ([Sentry Open source](#), [Prometheus](#), [Grafana](#), [Netdata](#), [Uptime Kuma](#)).

3.It is necessary to carry out security testing of the service at least 2 times a year, identifying potentially vulnerable areas.

4. A member of the service testing team or a test company professional must have at least one of the following certifications, depending on the tested item:

Testing Object	Type of Certificate
Infrastructure	HTB Certified Penetration Testing Specialist (HTB CPTS) Zero Point Security Red Team Operator (CRTO) OffSec Certified Professional (OSCP) EC-Council's Certified Penetration Testing Professional (C PENT) OffSec Experienced Pentester (OSEP)
Web	OffSec Web Assessor (OR) OffSec Web Expert (OSWE) GIAC Web Application Penetration Tester (GWAPT)



	Web application Penetration Tester eXtreme (eWPTX)
Wireless	OffSec Wireless Professional (OSWP) GIAC Assessing and Auditing Wireless Networks (GAWN)

In addition to the above requirements, when creating a new service, it is also necessary to fill in the checklists developed by the Information Systems Agency of Armenia (ISAA) to ensure that the service complies with the requirements of the digitization standards. In order to receive the checklists, it is necessary to contact the ISAA team at the following e-mail address: [info@isaa.am](mailto:info@isaa.am).

# TECHNICAL REQUIREMENTS FOR VIDEO CALL SUPPORT

## Functional Requirements

### 1. Video Call Functions

- One-on-one support for video calls, group video calls, and webinars.
- High-quality video broadcast with customizable image quality depending on network bandwidth (minimum 720p@30FPS).
- Screen sharing for performances, performances, and collaboration.
- Virtual backgrounds, filters, and other video enhancement functions.
- An opportunity to record video consultations.
- Recordings must not be limited in time.
- Recordings must include a timestamp, date/time, and duration of the recording.
- Recording files must be stored in a specified location on the network at the time of installation.

### 2. Meeting Management

- Scheduling, updating, and canceling meetings with APIs with calendar integration (e.g., System Calendar, Google Calendar, Outlook).
- Generate unique links or access tokens for each meeting.
- Send e-mails to participants with reminders, meeting details, and entry instructions.

### 3. Participant Management

- Support for the integration of external identification systems.
- Allow you to join the meeting as a guest or identified user with simultaneous authentication (SSO) support.
- Control participants' voice/camera settings, turn on/off the voice, and manage their roles (e.g., presenter, viewer).

### 4. Security and privacy

- End-to-end encryption of video streams to protect sensitive data.
- Compliance with data protection regulations in the processing of user data and records.
- Role-based access control (RBAC) to restrict access to sensitive functions and content.
- High-level encryption of all recorded files for privacy.
- Recorded files must have a timestamp to protect against altering content.

---

## Non-functional requirements

### 1. Scalability

- Ability to provide multiple users and video calls at the same time without interruptions.

- Reasonable load distribution and automatic expansion to ensure efficient system operation during peak hours.

## **2. Reliability and Accessibility**

- A high-availability architecture with backup servers and disaster recovery mechanisms.
- The solution must be ready for deployment in a cloud environment. Ideally, cloud services should be used.
- Service Level Agreements (SLAs) for work hours, delays, and response times.

## **3. Speed of performance**

- Real-time video communication with low latency and high-quality maintenance.
- Efficient use of network bandwidth with automatic bitstream regulation to maintain the quality of streaming video.

## **4. Compatibility**

- Cross-platform compatibility, supporting all web browsers (Chrome, Firefox, Safari, Edge), desktop apps (Windows, macOS), and mobile devices (iOS, Android).

## **5. Programmer Experience**

- A well-documented API with code examples, SDKs, and guidelines for integration and customization.
- Developer support and collaborative forums to solve problems, offer new opportunities, and exchange best practices.

## **6. Compliance**

- Compliance with industry standards and regulations for accessibility (e.g., WCAG), compatibility (e.g., SIP, WebRTC), and security (e.g., ISO 27001).

## APPENDIX 4

### INTELLECTUAL PROPERTY AND WARRANTIES

Copyright
All property (including exclusive) rights related to the new system belong to the Client.
Software License Agreement
If the system is the subject of a licensing agreement, a license agreement is signed between the Client and the Consultant, whereby all property rights are transferred to the Client without additional compensation.

#### 4.1. Intellectual Property and Other Rights

All exclusive property rights and other intellectual property rights to the new System or changes to the System, including the software codes, graphics, sound elements, databases, preparatory materials (hereinafter also created) necessary for the creation of changes to the System, must be transferred to the Client without additional remuneration, including:

- (a) the right to reproduce creation;
- (b) the right to decompilation of creation;
- (b) the right to distribute creation;
- (c) the right to rent the original or copies of the creation;
- (d) the right to borrow the original or copies of the creation;
- (e) the right to translate creation;
- (f) the right to recycle, adapt, and transform creativity in other ways, including the right to create derivative creations;
- (g) the right to communicate creation to the public ;
- (h) the right to public performance of creation;
- (i) the right to public display of creation;
- (j) the right to broadcast creation;
- (k) the right to rebroadcast creation;
- (l) the right to transmit by cable or similar means;

(m) the right to grant/transfer/alienate the rights to possess, use, and manage creation;

(n) The right to use creation in other ways and ways that do not conflict with the national legislation of the Republic of Armenia.

Exclusive property rights to creation are transferred to the Client to the maximum extent permitted by the legislation of the Republic of Armenia .

The Consultant must be the sole owner of the creation and the sole holder of exclusive property rights to the creation.

If, in the future, the legislation of the Republic of Armenia establishes a new, transferable property exclusive right to a service that is not included in the aforementioned list, then such property exclusive right shall also be considered transferred to the Client.

All property rights to other objects of intellectual property that are part of the system or used within the system (including, but not limited to, objects of patent rights and trademarks) are also transferred to the Client without additional compensation.

The Consultant warrants that all intellectual property and other rights granted to the Client do not and will not infringe the intellectual property rights of any third party, and that the Consultant has all necessary rights and permissions (including from its employees and its subordinates) for the transfer of the intellectual property rights.

The transfer of intellectual property rights to the system will be regulated in more detail by the contract between the Client and the Consultant.

Intellectual property rights for all standard software and materials must remain in the possession of such rights holders. Standard software refers to all ready-made software provided as part of the services offered by the Consultant.

For the purposes of this Agreement, all software that is not considered to have been developed by a third party will be considered as Software developed by the Consultant(Custom Software).

For purposes of this Agreement, "Standard Software" means software that is owned by a third party, not the Consultant, and which is an ancillary element to ensure the work of the final product without restricting the Consultant's right to later adapt such product for other public service applications.

The intellectual property rights to standard software belong to the respective copyright holders.

If it is necessary to issue licenses/permits, the Consultant guarantees that the service provided by the Consultant includes the issuance by the Client of all the necessary permissions/licenses for the use of the Standard Software without additional remuneration, with the maximum possible volume and for a period of at least 7 years. The costs of obtaining such licenses/permits shall be borne by the Consultant. The Client must be able to transfer the rights he has acquired over the Standard Software to other persons.

The contract between the Client and the Consultant must give the Client the right and opportunity to open concepts, writings, projects, algorithms, programming documents, and other specially developed documents and transfer them to any third party with whom the Client will sign a contract for the provision of technical assistance services or the development of additional functions of the New System. Open concepts, writings, samples, algorithms, programming documents, and other specially developed documents to the Client and transfer them to any third party with whom the Client will sign a contract for the updating of technical maintenance services or additional functions of the New System.

Within fifteen (15) days prior to acceptance of Phase 3 of the Services, the Consultant will provide the Client with the source codes of all specially developed software and all relevant documentation related to the specially developed software.

The computer program and the contract between the Client and the Consultant must give the Client the right and opportunity to make the software:

(i) be used or copied on or with computers of the same capacity (for which it was acquired and backup computers) if the main(s) are not working and during a reasonable transition period when the use is transferred from mainstream to backup;

(ii) used and/or copied for use on replacement computers: use on original and replacement computers can be carried out simultaneously for a reasonable transition period;

(iii) if the nature of the New System permits such access, it shall be accessible from other computers connected to primary and/or storage computers through local or broadband network or similar solutions, and shall be used or copied for use on such other computers to the extent necessary for such access;

(iv) be reproduced for security or conservation purposes;

(v) adapted, adapted, or combined with other computer program(s) for use by the Client;

(vi) will be presented to service providers and their subConsultants and copied for use by them according to the volume required for the provision of services. The Client may sublicense such persons to use and copy the Software for the purpose of use.

## **4.2. Guarantees**

Consultant represents that changes to the System, including all software and the Services provided, will be free from any defects in design, development, materials and manufacturing quality or other circumstances that would result:

(1) The complete final System and/or any of its components will not meet the technical requirements set out in this document and other documents approved by the Client; or

(2) The complete final System or its elements will be restricted, the reliability, and/or the possibilities for expanding operations.

The Consultant also represents that the complete final System will be in line with the best solutions used in international practice.

If defects appear in the complete final System during the warranty period, the Consultant must properly and as soon as possible eliminate these defects at his own expense, as well as compensate for the damage caused by such defect.

The procedure for notifying deficiencies and the procedures for their inspection and elimination will be determined by the contract between the Client and the Consultant.

The Consultant shall assist the Client or the third parties specified by the Client in resolving problems arising during software provision, provision of warranty services, elimination of deficiencies, software changes, and other similar circumstances.

The Consultant shall also assist the Client in repurchasing (and/or transferring such rights to the Client) any licenses or warranties granted to the Consultant by the manufacturers and/or licensors to the Client.

The Consultant also guarantees the development/supply, deployment, testing and acceptance of the complete final System. The Consultant guarantees that the System can be used in accordance with this document, other documents established in the framework of the System, and the terms and conditions of the contract between the Client and the Consultant .

The Consultant guarantees the Client that:

(i) The source codes and relevant documents to be provided to the Client will be complete, correct, and final copies that will fully comply with the software release version in force at the time of Phase 3 adoption;

(ii) Within fifteen (15) days of making any changes to the software release copy within the 12-month warranty period, the Consultant will provide the Client with the modified source code and relevant documentation, which will also be complete, accurate, up-to-date and conform to the current released version.

(iii) The source code will contain all the information necessary to enable the programmer or analyst to maintain and/or improve the software. In particular, the source code and the corresponding documentation will contain all lists of programmers' interpretations, data and process models, logical manuals, and block diagrams.

(iv) The source code of the software packages (plugin) available in the system's software code must be provided to the Client, and the build of the software packages will be carried out in the appropriate environment of the Client. The Consultant will provide the Client with a guide detailing the process of building a software package from source code.

(v) Software codes must be open.

(vi) The Client must be provided with:

- used libraries (open),
- the servers of application programs,
- script,
- other files, packages, and other software necessary for the installation, configuration, and operation of the system,
- a document describing the system's investment, which outlines the necessary software for the system's implementation, application servers, the sequence of investment steps, and so on, which will be understandable to skilled professionals,
- technical documents describing the systems.

## APPENDIX 5

### DESCRIPTION OF THE INSTALLATION OF THE SYSTEM IN THE SERVER DOMAIN

Name	State	Status	Managed by	Provisioned Space	Used Space	Host CPU	Host Mem	Guest Mem - %	Active Memory	Guest OS	Memory Size	CPUs	NICs
DB1-PRD	Powered On	Normal		402.56 GB	387.35 GB	68 MHz	46.8 GB	1	532 MB	Microsoft Windows Server 2016 or later (64-bit)	52 GB	8	1
DB-TST	Powered On	Normal		132.11 GB	93.08 GB	119 MHz	32.09 GB	2	655 MB	Microsoft Windows Server 2016 or later (64-bit)	32 GB	8	1
DB2-PRD	Powered On	Normal		402.23 GB	87.1 GB	45 MHz	19.92 GB	1	532 MB	Microsoft Windows Server 2016 or later (64-bit)	52 GB	8	1
MGMT-PRD2	Powered On	Normal		66.18 GB	64.85 GB	45 MHz	15.88 GB	3	491 MB	Oracle Linux 8 (64-bit)	16 GB	8	1
ccptems-test	Powered Off	Normal		108.22 GB	63.72 GB	0 Hz	0 B	0	0 B	Microsoft Windows Server 2016 (64-bit)	8 GB	8	1
APP-TST	Powered On	Normal		63.1 GB	60.79 GB	47 MHz	8.07 GB	5	409 MB	Microsoft Windows Server 2016 or	8 GB	8	2



										later (64-bit)			
APP1-PRD	Powered On	Normal		108.35 GB	52.15 GB	68 MHz	8.07 GB	4	327 MB	Microsoft Windows Server 2016 or later (64-bit)	8 GB	8	2
App-Test-2	Powered Off	Normal		58.22 GB	49.39 GB	0 Hz	0 B	0	0 B	Microsoft Windows Server 2019 (64-bit)	8 GB	8	1
App-Test-1	Powered Off	Normal		58.22 GB	49.37 GB	0 Hz	0 B	0	0 B	Microsoft Windows Server 2019 (64-bit)	8 GB	8	1
Db-Test-2	Powered Off	Normal		402.22 GB	49.37 GB	0 Hz	0 B	0	0 B	Microsoft Windows Server 2019 (64-bit)	52 GB	8	1
Db-Test-1	Powered Off	Normal		402.22 GB	49.37 GB	0 Hz	0 B	0	0 B	Microsoft Windows Server 2019 (64-bit)	52 GB	8	1
APP2-PRD	Powered On	Normal		58.3 GB	38.96 GB	22 MHz	8.07 GB	3	245 MB	Microsoft Windows Server 2016 or later (64-bit)	8 GB	8	2
EXT 2-PRD	Powered On	Normal		54.09 GB	38.55 GB	22 MHz	4.06 GB	7	286 MB	Microsoft Windows Server 2016 or later (64-bit)	4 GB	8	1

EXT 1- PRD	Powe red On	Nor mal		54.09 GB	37.4 3 GB	22 M Hz	4.0 6 GB	5	204 MB	Microsof t Windows Server 2016 or later (64- bit)	4 GB	8	1
MG MT- PRD 1	Powe red On	Nor mal		58.08 GB	11.7 3 GB	0 Hz	2.3 4 GB	1	81 MB	Oracle Linux 8 (64-bit)	8 GB	4	1