Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

ANNEX

TECHNICAL SPECIFICATION FOR PROCUREMENT OF A CASE MANAGEMENT SYSTEM FOR DPMLTF

1.1 Current situation

Montenegro is located on the so-called "Balkan Route" - the crossroads of various smuggling channels that go from the Middle East to the European Union. One part of the so-called The Balkan Routes passes through Montenegro. Drug trafficking is predominantly recognized as one of the main elements of cross-border crime, while trafficking in human beings and smuggling of migrants, as well as smuggling of excise goods, are significant criminal activities that generate material gain.

The SOCTA 2017 has identified the risks of the following occurring forms of crime:

1. Drug trafficking,
2. Serious crimes against life and body,
3. High-level corruption,
4. Usury
5. Illegal migration and human trafficking
6. Money laundering

All these forms of crime, regardless of whether they are committed in Montenegro or abroad, predominantly generate property gain, which through legal crime of money laundering is introduced into legal flows, both in Montenegro and abroad. To prevent these crimes being committed, strong financial intelligence unit (FIU) is imperative.

Former Administration and now the Department for the Prevention of Money Laundering and Terrorist Financing receives between 220 and 270 suspicious transactions annually, which also represented the same number of open analytical cases, and about 30.000 cash transactions. It is quite difficult to process all this information properly without proper application support for receiving the case and for using analytical tools to automatically process and select potential candidates for further-analytical work.

The processing of the inspection case consists in a lot of manual work from the management, police officer/inspectors and the supporting staff. The information is collected from the reporting agencies mainly from the existing portal in different formats (xml, docs, spreadsheets, etc.), are managed and distributed in collaboration in the existing system and to case inspectors.

High-level Case processing consists of analysing of the existing data and gathering additional information from different other sources as police databases, other state agencies, foreign partner agencies, in different channels of communications and forms, but mainly in paper documents, emails. The information is consolidated and is processed by the inspectors and head of departments and it leads to the decision. In this process the managers, inspectors and supporting staff are supported poorly by the existing system. Figure 1 below explains in high level the process in DPMLTF:

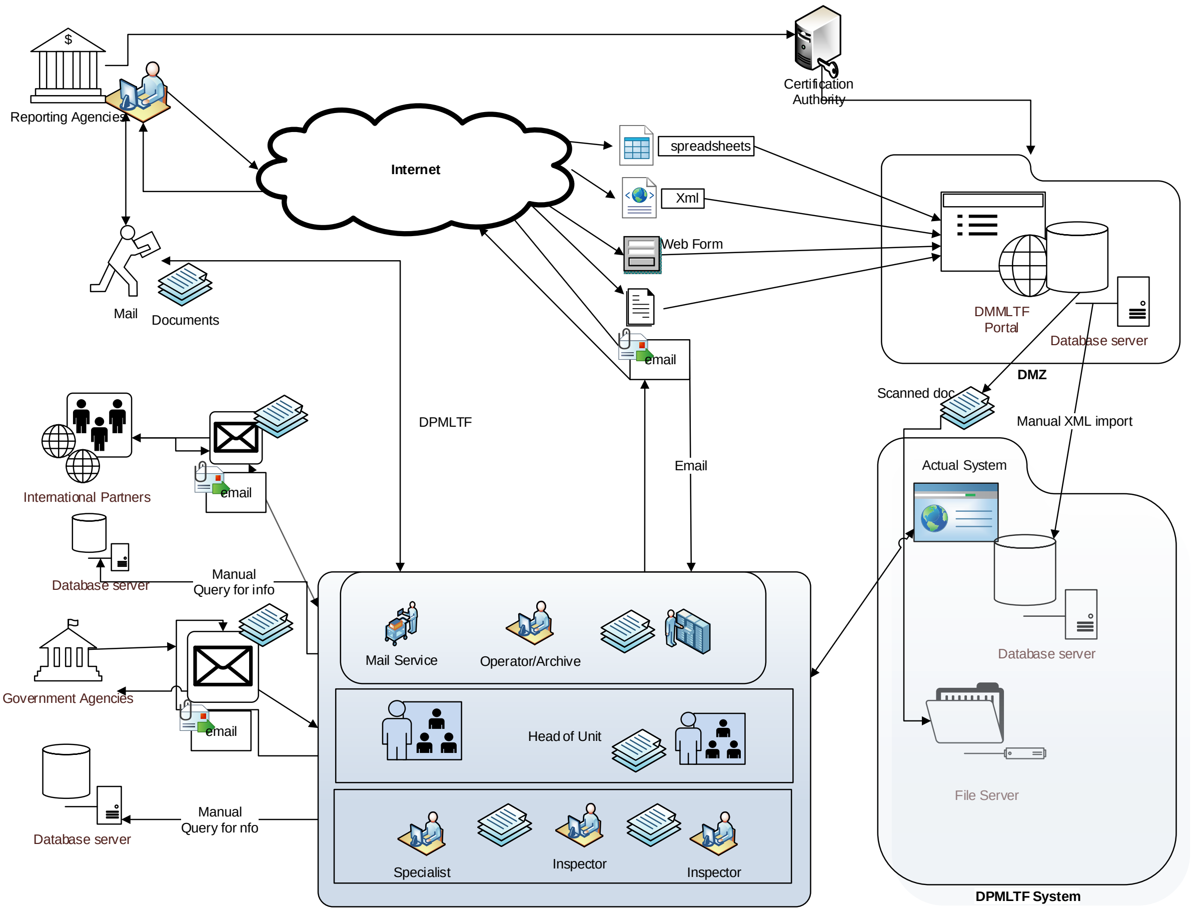


Figure 1: DPMLTF process description

For the moment the Department for the Prevention of Money Laundering and Terrorist Financing doesn't use a proper Case Management System that would aggregate data around entities (persons, legal or natural) that are potential perpetrators of criminal offences. Lack of such system designed to support the workflow and the working processes of the DPMLTF leads to the following difficulties and problems:

- Lack of coordination among different cases and organizational units within the Department that manage those cases,
- Inconsistent monitoring of cases in order to prevent overlapping of cases involving the same persons,
- Inability to link different items based on key parameters (entities), which will initiate adequate analysis and complete targeted checks
- Absence of an indexed (structured) database made of data from previous cases that would provide a good basis for the use of analytical tools.
- Lack of capacity to store data in an appropriate form in the financial intelligence database, and then structured distribution to other organizational units or other authorities for further competence
- Lack of ability to monitor the fulfilment of deadlines for handling cases, and to put appropriate notes on the implementation of cases (so-called flagging)
- Lack of ability to meet standards for data secrecy and data protection (deadlines for data storing that would automatically signal the need to extend the deadlines beyond their expiration date)
- Lack of electronic communication between organizational units within the Sector
- Lack of automatic connection to available databases
- Lack of logs on access and data processing
- Lack of appropriate data protection measures in databases.

As the result the Department for the Prevention of Money Laundering and Terrorist Financing has difficulties to effectively perform the tasks within its jurisdiction without an adequate software application to overcome the mentioned shortcomings.

In order to improve the performance of the DPMLTF to increase the effectivity it is necessary to provide appropriate IT systems and tools for processing received information, and also all banking data (suspicious transactions and cash transactions), there must be an appropriate information platform that will automatically electronically collect this information, automatically check it through the available databases, deliver potential hints, and in accordance with indicators, direct work of officers towards those data that indicate suspicion of money laundering or terrorist financing offenses.

1.2 General description

This Project aims to create the preconditions for strengthening analytical capacities of the Department through systematic collection of information to be used for analysis of financial intelligence data received from the reporting entities based on the Law for the Prevention of Money Laundering and Terrorist Financing and automatic verification of this information through available police databases as well as databases of other state authorities, and preparing that data for easy export to appropriate analytical programs for the purpose of producing analytical reports and information to the competent authorities for processing criminal offences of money laundering and terrorist financing as well as predicate criminal offences.

Reception, processing and forwarding of information will be aimed to be electronically, in accordance with:

1. standards governing confidentiality of information and personal data protection,
2. in accordance with European Union standards in the area of preventing the use of the financial sector for the purpose of money laundering and terrorist financing,
3. in accordance with the FATF Recommendations and the best practice defined at the EGMONT Group level.

The result of the Project will be more effective and efficient handling of collected intelligence and other data, and ultimately a larger number of analytical reports on suspicious transactions that will directly lead to larger number of investigations and criminal proceedings for criminal offenses of money laundering and terrorist financing as well as predicate criminal offences.

Furthermore, the creation of this application will influence a more comprehensive and systematic analysis and comparison of obtained data and intelligence with existing databases, as well as better international cooperation with foreign partner financial intelligence units.

Future DPMFTF systems environment will consist in different modules that will work as one, where all the modules and applications will aim a different business scope, serving to the final goal for assisting DPMLTF inspectors and staff in their daily job and maximizing the automation of processing the information.

The system in the future will have the following Modules

1. Module for - Case Management, - subject of this procurement
    a. Business Process management
    b. Document Workflow Management
2. Module – Portal – the portal is functional and need to be improved –**Subject of this Procurement**
3. Module - Data Integration Gateway - **Subject of this Procurement** which will include at least:
    a. Integration with Portal (Communication with Reporting agencies)
    b. Integration with Police Databases
    c. Integration with other State Agencies
    d. Integration Foreign Partner Agencies
4. Reporting –Subject of this procurement
5. Module – Expansion of System Integration Gateway – Not subject of this Procurement which will include:
    a. Integration with other State Agencies system expansion

   b. Integration Foreign Partner Agencies system expansion

6. Business Intelligence – Not subject of this Procurement

The Case Management System with its two sub modules and initial reporting. All these will be described in more details in this document.

Description of the Portal System Integration Gateway.

Control and verification of the data and information on purpose of Money laundering a terrorist financing submitted is the core part of the DPMLTF system. The entire system shall be designed in a way, that allows the DPMLTF staff to effectively check subjects, data and information received from other institutions. All inspection job relies almost entirely in information received by other public or not public registries of data, such as reporting agencies as Banks, CDA Stocks, Securities, Custom, insurance, registry of immovable property, register of vehicles, fiscal service databases shall also be connected to the different internal and external law enforcement agencies. For the moment DPMLTF realizes partly this through the existing portal where mainly the reporting agencies submit their information in a structured form (XML and data forms). In the future DPMLTF system should communicate via APIs to enable cross data checking in other systems that have the possibility to expose their data for consumption via web services.

For the moment DPMLTF receives structured reporting data from different agencies summarized in the table below.

Type of reporting entity	reporting options:
Banks	xml electronic forms
CDA and stocks	xml
Turnover of the securities	electronic forms
Custom administration	electronic forms
Life insurances	electronic forms
Other reporting entities (Notaries, lawyers, merchants, car dealers, real estate dealers, accountants….)	electronic forms

The data are received through the DPMLTF existing portal and reporting are digitally signed by the reporting agencies. The new system should support the Digital Signature infrastructure in use by DPMLFT.

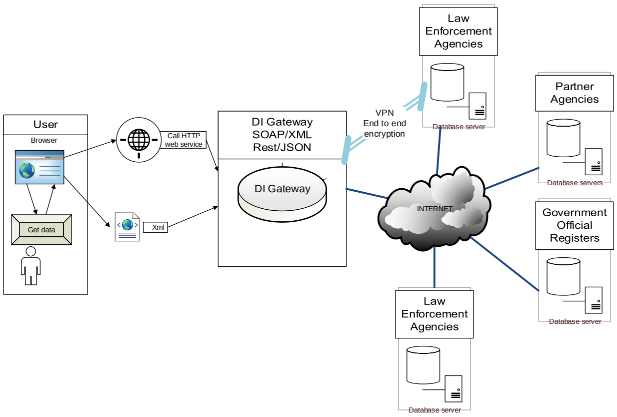
Meanwhile the business needs for the case processing within the department requests to have information from different other data sources. The difficulty is the different development status of the data sources (registers), diversity of the technologies and standards in use and to interconnect with these registers will be done a specific analyse specifics of each of them.

At present, DPMLTF exchange information with related agencies and institutions in different forms and partly in paper-documents based communication that cause a lot of workload and difficulties in coordination. The communication with other institutions and partner agencies is summarized in the table below:

Government Institutions	Existing Communication	Description of the information
Ministry of interior	Data exchange in hard copy	Information for: - Civil Status, - Residence - permanent /temporary - ID documents - Registered vehicles
Police directorate	Data exchange in hard copy between departments and electronical access to police databases CRA	Information for: - Wanted, - Border, On-call service, - External data, - Criminal offenses,
Tax Administration	Data exchange in hard copy and free access to public web site (CRPS) Tax portal	Tax and financial statements and data of business subjects, ownerships, activities, and tax identification number
Real estate administration	Data exchange in hard copy and access to web application with digital certification	Cadastral data and ownership
Ministry of justice	Data exchange in hard copy and access to web application.	Information about penalties, offence and prison sentences
Court council	Data exchange in hard copy	Information about court decisions and criminal proceedings
State Prosecutor's Office	Data exchange in hard copy	Sending notification about money laundering and financing terrorism
Agency for national security	Information exchange in hard copy	Exchange Information about financing terrorism and money laundering
Central bank	data exchange in hard copy and access to web application with digital certification	Information about target control of reporting entities/ Data of accounts of residences (available throw web application).

Government Institutions	Existing Communication	Description of the information
Capital market commission	Data exchange in hard copy	Information about: 1. Brokers, 2. stocks, 3. funds 4. Central Depository Commission
Anticorruption agency	Data exchange in hard copy and access to public web site	Information mostly about politically exposed persons

The new Case Management System consider making possible the processing of the information as it is and to give to DPMLTF staff tools to search and filter the information about inspection subjects in different databases by any parameters (including personal data of subjects).



The system should be able to get the requested information about investigated subjects from at least (but not limited to) the following:

Civil Status, Residence - permanent /temporary, ID documents, Registered vehicles, Wanted, Border, On-call service, Criminal offenses, Central Business registry, Information about penalties, Offence and prison sentences, Interpol and SIENA[1].

1.3 Users Roles

The Application needs to have a developed flexible administrative management, in the context of defining the authorization of certain officers, as well as defining the level of users. The system should have different user roles including but not limited to the following:

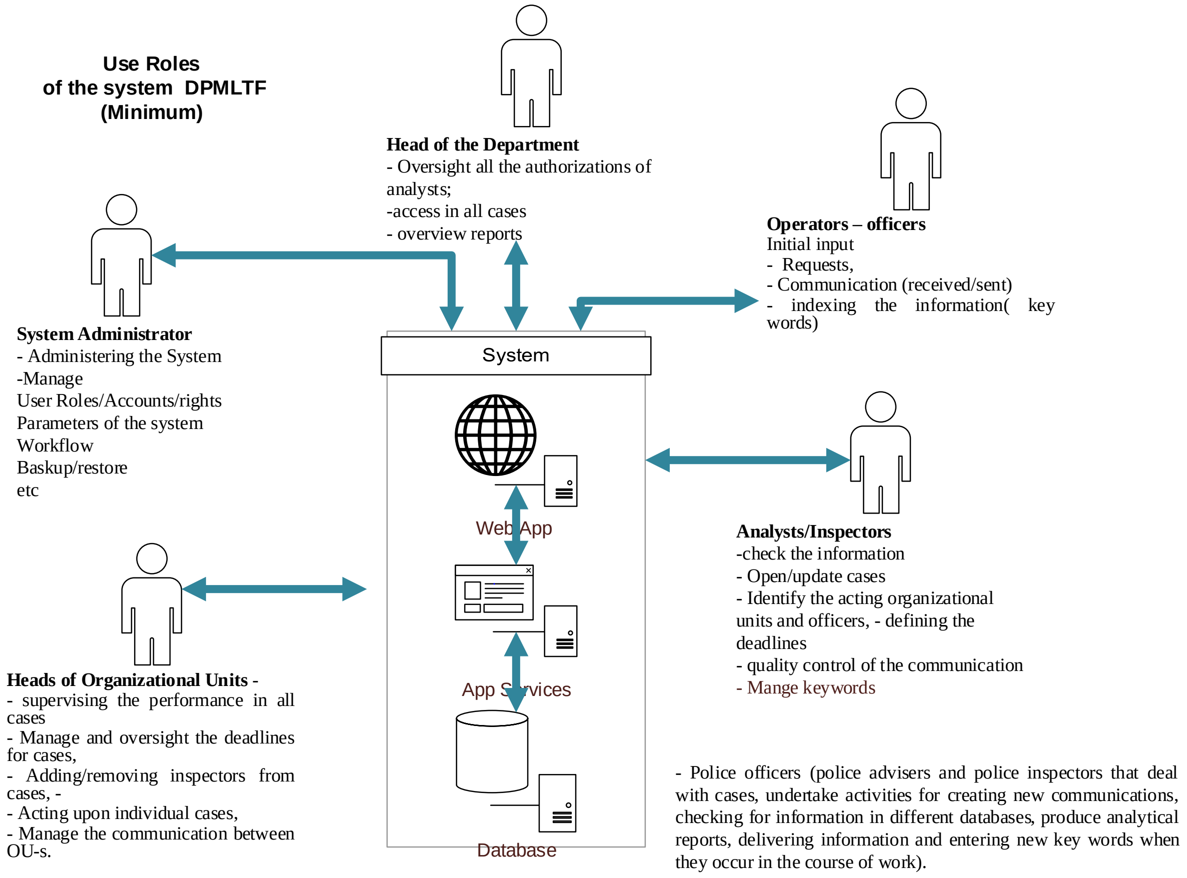
a. Operators (officers performing the initial input of all the requests (received/sent) in the application and indexing the key words)
b. Analysts/inspectors (officers who check the overlapping of new cases with the existing ones (upon the entered key words) and decide on opening new cases/attaching requests to the existing cases, identifying the acting organizational units and officers, defining the deadlines for action and quality control of the sent messages of Police officers (police advisers and police inspectors that deal with cases, undertake activities for creating new communications, checking the existing databases, creating analytical reports, delivering information and entering new key words when

[1] The Secure Information Exchange Network Application (SIENA) is a platform that meets the communication needs of EU law enforcement

they occur in the course of work). The inspectors can act as case owners but as well they can be assigned as case contributors in other cases with different level of access.

c. Heads of organizational units (organizational units within the DPMLTF, that are responsible for supervising the performance in all cases that are being processed with that organizational unit, through: following the deadlines of completing cases, adding/removing staff from cases, changing deadlines for completing cases, acting upon individual cases, communicating with other organizational units within the Department).
d. Head of the Department (who has all the authorizations of analysts and possibility to make all the changes to cases, from the entry, changes, to deletion, as well as the possibility of overviewing all the reports upon any criteria).
e. Administrator (who has the role of administering users, opening new users accounts, changing passwords, removing users, changing rights, adding characteristics to categories of users, adding or removing the organizational units within the Department etc.)

In case the circumstances require other assignments of roles and levels of users, passivating of certain levels of users should be enabled at the administrative level, as well as adding characteristics of those levels to some other levels of users (for simplifying the work process), so the application has to be flexible in the context of levels of users and characteristics they have.


Use Roles
of the system DPMLTF
(Minimum)
Head of the Department
- Oversight all the authorizations of analysts;
-access in all cases
- overview reports
Operators – officers
Initial input
- Requests,
- Communication (received/sent)
- indexing the information(key words)
System Administrator
- Administering the System
-Manage
User Roles/Accounts/rights
Parameters of the system
Workflow
Baskup/restore
etc
System
Web App
App Services
Database
Analysts/Inspectors
-check the information
- Open/update cases
- Identify the acting organizational units and officers, - defining the deadlines
- quality control of the communication
- Mange keywords
Heads of Organizational Units -
- supervising the performance in all cases
- Manage and oversight the deadlines for cases,
- Adding/removing inspectors from cases, -
- Acting upon individual cases,
- Manage the communication between OU-s.
- Police officers (police advisers and police inspectors that deal with cases, undertake activities for creating new communications, checking for information in different databases, produce analytical reports, delivering information and entering new key words when they occur in the course of work).

1.4 Process Execution and Business Process

The DPMLTF system should allow the design of business processes to manage all the steps from the receiving of data/information up to the finalization of the business processes. It should also allow address other operations of DPMLTF such as data entry provided with advanced search capabilities and very with good data validation in order to avoid human mistakes, communication with external agencies in different communication channels, document handling, work flow engine, semi-automatic data indexing (key words) which are reliant on good subject data in order to be effective.

The following requirements describe the sub-processes as defined in DPMLTF operation framework figure.

Digitalisation of communications:

By digitalization all the data are entered into the system (electronic communication, e-mail messages, attachments, message texts, etc...) A structured information, whose structural elements are key words or entities, is created out of the message in the form of text, The message is attached to the case in case the communication with the same reference number or key words match is found in the system, or a new case is opened. The process of digitalisation of messages is the process of transforming unstructured incoming messages (most usually in the form of electronic communication or e-mail messages or scanned or PDF files) into structured digitalised messages. The incoming unstructured messages must be kept in the original format (e-mail messages as msg file) and attached to the created digitalised message.

The information from the text of incoming messages are structured in such a way that the parts from the text should be captured and those parts become the key words of the message such as but not limited to:

- name, surname, UMCN, IMEI phone number, account number, registration plates of the vehicle, name of the legal person, name of the bank etc.

Creating cases and attaching communication messages to the case

The user of the system should be assisted by the system to identify if the incoming data or information belongs to any existing communication. In case when those do not belong to any existing case, the system must assist the user to create a new case where the information must be attached to it. The system should assist the users to assign case number based on well-defined criteria's, taking in consideration that case number will be the key of any further communication for the case.

Case Processing

Case will be processed by Users (Police advisors / inspectors). The system must support them in analysing the information, communication internally and externally, updating the information. In mostly of the cases the case is managed by the case owner (user role- police officer- inspector), but in several cases the System should allow the case owner to assign to the case other users as Case Contributors. The Case Contributor will be allowed to have controlled access over the case information and the system must create the possibility for the case owner to assign different level of access in different level of objects for the case contributor. The system should allow the users to update the case data/information, to attach to the case all type formats of communication that they have about the case (messages, documents, data, etc), to link different cases that can be related, cases and as well to keep all time parameters of the case processing, Time alerts – arbitrary alerts with chosen date/time when the system is going to send an e-mail with text note to the user who created that note.

Each case has a deadline for being completed, the deadline is defined when creating the case and cannot be changed by the acting officer after being initially recorded in the base. Before the expiration of that period the acting officer is automatically sent a notification that the deadline for completing the case is close. If the case is not completed, and the deadline has expired, a notification is automatically sent to the acting officer, head of the Division, analyst and head of the Department. The system must allow to managers to overview the cases processing situation and as well to provide a workflow instrument for their collaboration with case owners. At the end the system should allow to finalise the case, store the case data respecting requirements of data protection legislation and as well making data available in UML format if they will be needed in the future for the Law enforcement Partner Agencies.

Case related Communication

During their daily work, DPMLTF staff communicate internally and with external agencies and institutions. Mostly the initiation of the communications is triggered by two main reasons:

- On Receiving of Data/information through communication channels (message that contain requests, data, information,). That represents the beginning of communication.
- Starting the communication upon the initiative of a Division within the DPMLTF for different reasons that they can have during their daily investigations.

The system should assist the users to manage the communication flow, regardless of the fact how the case was initiated. The communication should continue during time, and System should accommodate and facilitate this process. The system must create the possibility for the users to have an intuitive visualisation of the communication, accurate relation between the case and data/information, very careful categorisation and indexing for further processing. It must allow the users to have the communication translated in different languages as well.

Sending messages

It should be noted that the term "Message" is used here for a complex entity which, in addition to the text, attachments and destination where it should be sent, also contains a set of structured information (metadata taken from the existing case parameters). Some of them are as follows:

1. Communication reference
2. Urgency mark
3. Secrecy mark
4. Reply time
5. Time of sending
6. Use of information mark
7. Period of keeping the information
8. Accuracy information mark / source reliability
9. Disclaimer

The final text and message format should be created by the acting officer by simple selection of communication pattern. The communication patterns are created by the application user. These are arbitrarily formatted texts with tags (each tag for one structured information) that will be, in the moment of creating the message, filled with values of appropriate message elements. The pattern format can contain tables, pictures, caption and other, in addition to standard options for selecting font and size of text parts.

The acting officer should have options for sending:

1. Original message text
    1. Translated message text

Depending on the selected option the generated message will be either in the original language or translated.

The activity sending message transforms the message into the appropriate electronic format (ex. e-mail message) which is automatically sent from the application. When sending the message, the attached xml format can be sent (depending on whether it has been created by the officer) together with the structured entities which already exist in the text of the message.

Overview of communications (Messages) and Cases

- Messages that are not attached to the case should be highlighted in red in the table of all communications.
- All messages should have visible marks of urgency, general status (digitalised, sent, draft message created, forwarded for sending, returned for improvement etc.).
- The messages should be highlighted (ex. in bold font) to the users who didn't read them.
- The messages can be grouped per status, time of creation and other parameters.
- The cases containing changes must be highlighted (ex. in bold font).
- Both messages and cases should have the option of preview window.

Alarms

The alarms should be automatically generated in the following cases:

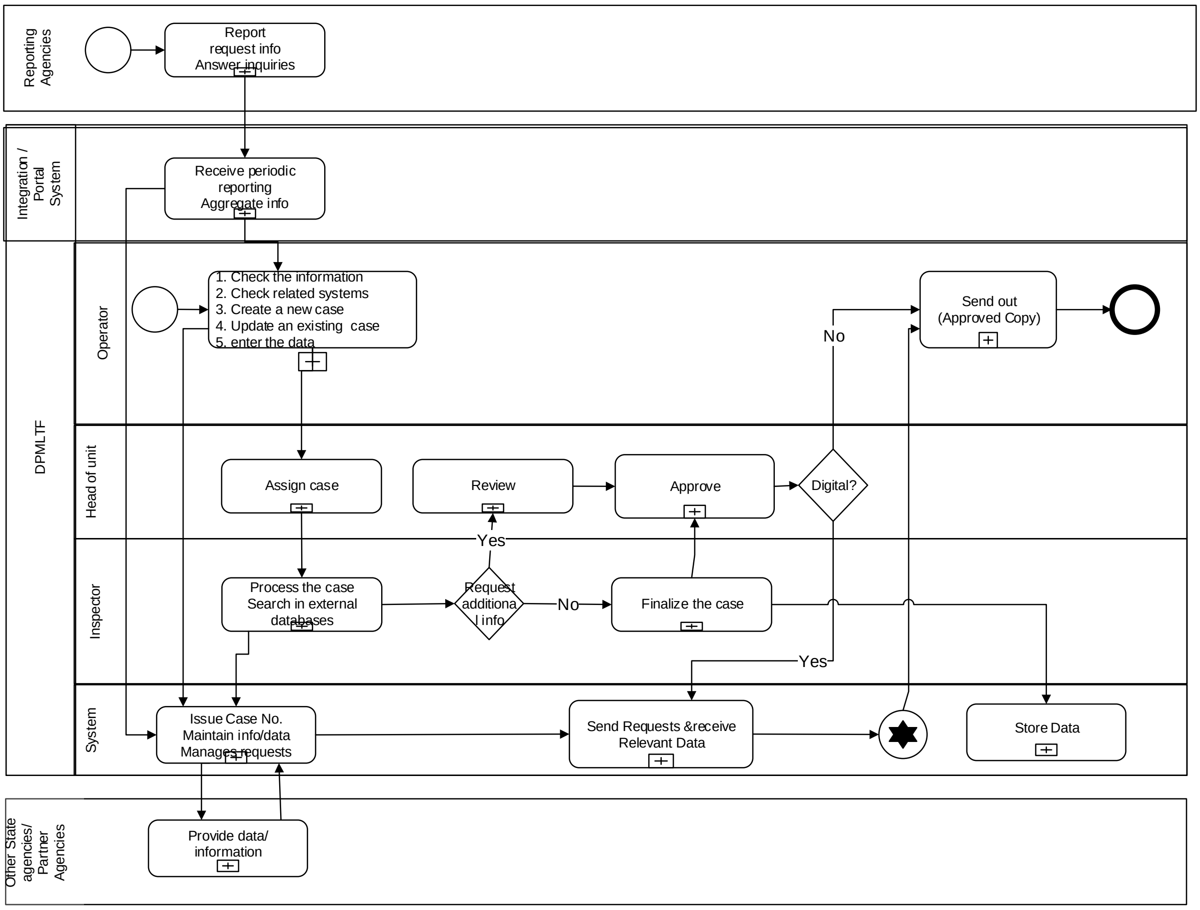
- Urgent messages with short reply deadline
- Unread messages
- Warnings on the absence of the officer when assigning him the case
- Notifying the tasked officers on the access of other system users to their cases
- Notifying the tasked officers on new messages in the case, changes in the case
- Notifying the officers on the forthcoming secrecy data expiration or personal data protection
- Notifying the tasked officers on deleting messages / cases due to the expiration of personal data protection period

Searches per cases and communications.

Communications (Messages) and cases are searched by key words contained in the messages. Given the set of key words the system must return the messages that contain those parameters in their set of key words. The same types of key words are being matched. For example, in case a vehicle with registration number "AA1122" is searched, the messages containing in their set of key words that parameter shall be returned as a reply to the search. The Application first conducts the search of messages and over that set of messages it finds the cases to which they belong, and which are also returned as the result of the search. The user can see only the basic data and only in case he is authorised for those messages and cases. The searches should be done only per English alphabet, and the application should also return the matches for combination of our letters (č, ć, š, ś, ž, ź, dž). The searches can be made per free text as well.

The user can be authorised for a case and its messages even in cases when he is not assigned (joined) with that case. This can be done in cases when the case has no confidentiality degree. Logs (search criteria) are kept in the base together with the data on user and time of conducting the search. If the user is not tasked with the case which the message belongs to a notification is automatically sent when the user opens the message. It is similar when opening cases. If the user is not joined to the case a notification is sent to the acting inspector in the case that is opened for review. So, the user can, as search result, get cases and messages even then when he is not tasked with them if they are with no confidentiality degree (or not designated as restricted), but the access to their details is announced by notification to the officer acting in those cases.

DPMLTF - Basic Process (BPMN)


Reporting Agencies
Report request info Answer inquiries
Integration / Portal System
Receive periodic reporting Aggregate info
DPMLTF
Operator
1. Check the information
2. Check related systems
3. Create a new case
4. Update an existing case
5. enter the data
No
Send out (Approved Copy)
Head of unit
Assign case
Review
Approve
Digital?
Yes
Inspector
Process the case Search in external databases
Request additional info
No
Finalize the case
Yes
System
Issue Case No. Maintain info/data Manages requests
Send Requests &receive Relevant Data
Store Data
Other State agencies/ Partner Agencies
Provide data/ information

1.5 Legal framework

For the implementation of the Project, the following COE, EU and FATF the standards should be considered and must be met:

- COE Convention on Laundering, Search, Seizure and Confiscation of Crime and Financing of Terrorism (Warsaw Convention, 2005)

  - Article 12 - establishment of FIU
  - Article 13 - Implementation of the FATF Recommendations
  - Article 15 - Principles of international cooperation
  - Article 43 - confidentiality of information exchanged
  - Article 46 - cooperation between FIU

- EU Directive 2018/843 of 30.05.2018 on the prevention of the use of the financial sector for the purpose of money laundering or terrorist financing (amendment of Directive 2015/849)
- FATF-a
  - FATF Recommendation No. 2 - Effective co-operation at national level
  - Recommendation No. 24 - Timely access to data
  - Recommendation No. 29 - FIU Standards and Authorisations
  - Recommendation No. 33 - keeping appropriate statistics
  - Recommendation No. 40 - Establishing the widest international cooperation in the fight against ML / FT
- Principles of international cooperation in the part of spontaneous and upon request providing basic and additional information
- Principles of access to data through the access to all available administrative and police databases
- The principle of direct querying into accessible databases
- The principle of personal data protection of Data confidentiality principle

2 Requirements,

2.1 Functional Requirements

Functional requirements have been grouped into the following. The tables show the general functional requirements for the **CM System** (hereinafter **System**), and the specific or special system requirements.

The Bidder shall commit to every function/requirement in the given tables of this document and enclose the completed tables in their Bid. The required functions/requirements marked with the letter "R"must be met. The requirements/functions that are optional, but desirable, are marked with the letter "O". Depending on whether the required or optional functions/requirements are met, the Bidder shall circle the appropriate mark "R" or "O". In addition, in the column "Bidder response", the Bidder must state how the function/requirement will be met, by using the following marking system:

Table 1.

Bidder response	Description of how the requirements shall be met
A	Exists as a function and is already implemented with at least one client – may be presented on the client's premises
B	Exists as a function, but not implemented with any client – may be presented on the Bidder's premises
C	Function requires little modification /programming and may be realised in a set time limit
D	Function cannot be met

All the functions marked by the Bidder with A, B and C are the subjects of delivery and the Bidder must deliver these within the bid-price.

The Bidder must enclose a functional specification in their Bid, i.e. a description of the bid software solution, and other relevant accompanying documentation that describes the bid solution.

The number of key requirements is ***113*** all of which are all required. In addition to listed requirements, the software solution must be designed also in accordance with the requirements given in Annex 1 of this document.

Table 2.

	Function	Description	Type	
FR001	Case Management	This is the main component of the system that is subject of the procurement and provides capabilities for executing, tracking and monitoring the business processes of DPMLTF staff.		
FR002	Entering Information (or opening a case)	It must be compulsory to enter data concerning the implementation of the Law FIU (article 84) When opening the case or when sending a communication, it chooses on what basis the data is received or sent, according to which the set of data prescribed for the selected register entered.		
FR003	Linked with International Police Collaboration and Criminal Intelligence Analytics	The Application must be compatible and linked with the existing Case Management Applications in the Criminal Police Sector (International Police Collaboration and Criminal Intelligence Analytics) for the electronic exchange of data between these Sectors and mutual (automatically) checks of databases both when entering keywords and when searching for databases.		

	Function	Description	Type	
FR004	System Integration Gateway	The Application must have a portal through which all available national (DPMLTF's database, Police Department, MIA and other authorities, as well as operational databases of the International Police Collaboration and Criminal Intelligence Analytics) and international (Interpol, Europol) databases can be checked in the background with one entry. If checks are done through the case, the application must visually signal in which databases the keyword match occurred. Also, that available databases can be checked from the case, using keywords already entered.		
FR005	Integration with existing Portal	The Application must integrate and enhance the existing Institutions and reporting entities Portal existing in the Department. The Case Management Application would improve and upgrade existing modules (for reporting entities)		
FR006	Integration with external systems	The Application must be linked to the ESW communication link, Europol Siena web services, Interpol I-link web services and I-24/7 communication link, police application web services (searches, on duty, border), MIA web application of civil status (persons, documents, weapons), web application of the Ministry of Justice (criminal records), web applications of other authorities (Central Bank, Real Estate Administration, Tax Administration, Central Registry of Commercial Entities, etc…)		
FR007	Create Case	The System must allow human workflow definition for creating a case. This human workflow should be supported by a high-level business process executing instance independent of the service business process flow instance		
FR008	Create Case	The System must allow creating a case during the service execution business process flow. This business process flow is loaded dynamically upon the operator starts a case		
FR009	Resume Case Processing	The System must allow processing of opened cases by a high-level business process flow that resumes processing of cases that are in the status "In Processing". These are cases that have been opened and that needs some days or months to be completed depending on the business processing logic of the business process types that they represent		
FR010	Case numbering	The System must allow the creation of cases (case number, process types and other general data regarding this processing request) upon the selection of the type requested by the operator the system component should supply the case management components with the active list of parameters.		

	Function	Description	Type	
FR011	Case numbering	The System must support creation of case numbering templates to allow generation of unique numbers per case. These numbers are important numbers to track the cases and the complete business process flow as well regarding the future communication for the case.		
FR012	Case numbering	The System must support case numbering templates definition based on service types so cases regarding each service type can be tracked and properly reported by the Reporting and performance component		
FR013	Case status	The System must support definition of case statuses like (opened, "In process <user>", Incomplete, suspended, Rejected, Closed etc.). The definition will be based on definition by DPMLTF that will define the business process flow of the service being developed.		
FR014	Contacts	The System must possess a manageable detailed contact list of the contacts in external agencies. This component will assist future communication regarding a case based on type of request or communication selected.		
FR015	Calendar	The System must possess a calendar for the contact list of the users in DPMLTF. This component will allow future coordination regarding assignment of new case based on the availability of the resources.		
FR016	Interoperability	The System must provide an API module which should be capable with an ability to serve as a gateway for connecting system to third party interfaces.		
FR017	Interoperability with the Portal	The System module must be provided with functionality to execute data transactions by the means of electronic data input/output using standard web service protocols with the DPMLTF Portal.		
FR018	Interoperability	The Interoperability component should have the ability to be quickly configured to integrate with specific application programming interfaces (API) of the configuration of the DPMLTF portal.		
FR019	Case Monitoring	The System must contain a Performance dashboard which should be provided with the ability to measure and to assemble primary records		
FR020	Case monitoring	The Performance dashboard should include corresponding features in order to facilitate above mentioned process including derivation of analytical data based on pre-defined calculation rules and presentation of results in a tabular form or graphical chart, including options of drill-down capabilities.		
FR021	Case task Management	The System must contain a Task Management module that must encompass, administer and deliver a wide range of functions pertaining to tasks life cycle.		

	Function	Description	Type	
FR022	Case task Management	The Task Management module must allow creation, assignment, and review, routing and tracking tasks in a hierarchical or peer-to-peer organisational environment. Task management system's underlying objective is to help users to achieve goals, and groups of users to collaborate and share knowledge for the accomplishment of collective goals.		
FR023	Case Messaging	The System must provide an integrated instant messaging module that must enable internal users' communication.		
FR024	Case Communications	The Module should allow provision of all-in-one web interface to all messaging services, such as internal system messages (personalised records), web message boards, instant messages, MS Outlook email, SMS, etc.		
FR025	Incident tracking	The System must contain an Incident tracking component serving as a "virtual help desk" which must allow administration of functions pertaining to system incidents.		
FR026	Incident tracking	The Incident tracking component must include ability to control and manage incidents and errors efficiently including the possibility to update incident settings, browse incidents, browse errors, manage incidents type, review, route, assign and respond to them.		
FR027	Incident tracking	The Incident tracking component must possess the feature to generate summary reports on a weekly, monthly, quarterly and annual basis.		
FR028	Case data visualisation	The System must provide ability to show case data in the table/grid format		
FR029	Case data sort and search	The System must provide ability to search, sort and page thru the case data		
FR030	Case Data Search t	The System must provide ability to perform advanced search on case data by one or more fields, including simple text or number fields, as well as date ranges, values selected from dropdowns, etc.		
FR031	Case management	The System must allow for exact, non-exact and phonetic searches by keyword, as well as by user-defined attributes. The System must support all characters in the Montenegrin alphabet and create premises for supporting characters of other languages in official use (Bosnian, Croatian, Serbian and Albanian languages are in official use.)		
FR032	Case management	The System must provide ability to input data into customisable web form interface using various field to capture various data types (personal data, numbers, date and time, email and phone, bank records, property records, etc., in dropdowns and text areas, etc.)		
FR033	Case files	The System must allow input forms to have ability to upload files and images and to assign to a case.		

	Function	Description	Type	
FR034	Data Validation	The System must allow input forms to have validation checks upon business rules provided by the beneficiary in order to avoid human errors.		
FR035	Case data analyse	The System must provide ability to collect, analyse data and apply predefined business rules using logic constructs (IF-THENELSE), internal and external APIs (database stored procedures and web-services), data retrievals and calculations.		
FR036	Case workflow	The System must provide a Workflow Engine as backend application with functionalities to administer semi-automated workflows that appear to the users as a sequence of data entry forms and other activities.		
FR037	Case workflow	The Workflow Engine must allow building such sequences dynamically, in real time, depending on user data entered at every step.		
FR038	Case fields	The Platform must allow ability to add all required fields to the data table from the gallery of available types which must include text, text area, date, date-time, integer, decimal, money, dropdowns, related fields, master-slave relations, etc.		
FR039	Visualisation	The Platform must allow system administrators and developers to customise visual tools such as Forms, Grids, Profiles and user interface of the system using online capabilities of the platform.		
FR040	Business Rules	The Platform must provide ability to define business rules using visual flow-chart like designers		
FR041	Validation	The Platform must provide ability to extend validation logic of entered data using JavaScript scripting languages		
FR042	Case forms	The System should provide a HTML5 container to contain and load predeveloped electronic forms.		
FR043	Business Process	The System should allow case management capabilities through a business process flow and human workflows		
FR044	Business Process	The System should offer the possibilities to create and administer high level business processes and sub-processes to support different execution paths of the service logic flow.		
FR045	Business Process	The System should support high level flows that call sub flows (exp. Selected request data from external agencies, trigger different processes to be executed)		
FR046	Business Process	The System should provide a designer integrated within the system that allows the appropriate users to design a process flow regarding any service or any case management process flow		
FR047	Business Process	The System should provide a Decision point (event based gateway) within the process flow to define different processing paths within the process flow.		

	Function	Description	Type	
FR048	Business Process	The System must provide ability to execute long-running Business processes, persist running processes to survive server reboots		
FR049	Document Management capabilities	The System must provide ability for authorised users to create, delete, rename folders and add, edit, delete, move documents and set access permissions to files and folders.		
FR050	Document Generation	The System must provide ability to generate documents in multiple formats, such as MS Word (.doc), Adobe (.pdf), etc. by populating templates with "live" data from the database		
FR051	Document Templates	The System must provide functionality for creating and updating templates for generating documents		
FR052	Multiple-Language Support	The System must provide translation of all text elements, labels and messages shown on the interface		
FR053	Multiple-Language Support	The System must provide online capabilities for managing translation dictionaries, adding new terms with translation and updating existing to facilitate localization of the application		
FR054	Multiple-Language Support	The System must provide the capabilities to maintain document templates in original language and their translation in Montenegrin language		
FR055	System Administration and Configuration	The System must provide user management capabilities for creating and updating user profiles		
FR056	Role Management	The System must allow the assignment of one or more specific roles to user account		
FR057	User Password	The System must allow for updating user password and it should require a Strong Password according the following principle: A strong password consists of at least eight characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) case-sensitive(contains letters in both uppercase and lowercase).		
FR058	User Account Management	The System must allow for approving, locking and unlocking of a specific user account		
FR059	User Audit	The System must provide history of user activities		
FR060	User Audit and Monitor	The System must provide information of users currently online		
FR061	User Account Management	The System must support 2-tier User Approval Process		
FR062	User Authentication	The System must support Two-Factor User Authentications		
FR063	Role based authorisation	The System must support Role-based Access and Authorisation		

	Function	Description	Type	
FR064	Password Administration	The System must support Password Encryption		
FR065	Audit trail	The System must support Audit trail by capturing all changes of data		
FR066	Audit trail	The System must provide details of User Activity Trail to system administrators		
FR067	Act as developing platform	The System should support a 4- phased approach to software testing and deployment: Development, Testing, Acceptance and Production (DTAP)		
FR068	Secure communication	The System must support HTTPS/SSL		
FR069	User logins/logouts	The System must track all Login/Logout History		
FR070	Identity Providers	The System should be able to relay on multiple identity providers by supporting claim-based authentication and authorisation. Supported protocols should include SAML2.0, WS-Federation, OAuth 2.0 (Open Authorization Framework)		
FR071	Active Directory	The System should support Active Directory for authenticating its internal employees		
FR072	Authentication Provider and PKI	The System should be able to authenticate the users based on digital certificates issued by official PKI infrastructure of Montenegro		
FR073	Digital Signing	The System should be able to sign digitally the messages and documents, based on digital certificates issued by official PKI infrastructure of Montenegro		

2.2 Non-Functional Requirements.

No.	Function	Requirement		
NFR001	Data Migration	The System should c migrate data from existing system in DPMLTF		
NFR002	Component of Subjects	The System should create the component of investigated subjects.		
NFR003	Web Base	The System must be web-based and accessible via intranet.		
NFR004	Single sign on	The System must support single sign on for the users of DPMLTF		
NFR005	User Groups	The System must allow definition of different user groups with different access privileges to different modules or functionalities of the system.		
NFR006	Object Rights	Users with the right access privileges in the system must be able to assign rights to objects at any time. Objects include different: modules/functionalities/folders/subfolders/ documents/messages/processes.		

No.	Function	Requirement		
NFR007	Rights assignment	Users with the right access privileges must be able to assign rights to individual users or groups of users.		
NFR008	Data Access	The System must allow access to functionalities and data to the users as per the privileges defined and assigned to them in the system. The System must prevent the access of data and functionalities of the system to the users if their privileges in the system do not allow it.		
NFR009	Session lifetime	The System must provide session expiration setting. If a user is not active for a specified period, he must be automatically logged off. The period must be configurable via system parameters by the system administrator.		
NFR010	Logging	The System must support logging and traces of each action done across each of the modules. Each action must be logged with at least the following data: 2. User; 3. Date and time; 4. Module; 5. Action; 6. Reference module		
NFR011	Data Validation rules	The System must implement data validation rules so that it prevents the user against making errors.		
NFR012	Data Custody	The whole set of documents generated during the process of declaring and inspecting must be stored as per Data Protection Law requirements.		
NFR013	System Availability	The System availability must be at least 98%.		
NFR014	Training	Training of the users of the system. A train the trainer program should be created within the project effort. The supplier must train the users and the trainers chosen by the beneficiary. Every system role must be covered.		
NFR015	Languages of training material	User manuals must be provided and be delivered electronically must be in Montenegrin language and must be accessible for on-demand requests. They should be available for end users internally (e.g. via existing intranet).		
NFR016	Source Code	Source code developed in the scope of the project must be delivered in electronic format. The Source Code ownership will be passed to the DPMLTF free from copyright. Installation of development and testing environment on the equipment of DPMLTF		

Reporting component for the Case Management System should be a web application with responsive interfaces, which is supported by desktop, mobile and tablets. The functionality requirements include:

ID	Function	Description	Type	
RFR001	Authentication & Authorisation	The System should allow access only to authenticated users, based in their roles will view the appropriate reports and graphics to them	R	
RFR002	Data Access	Must allow access to the data, reports or analyses based on the user profile. Data could be accessed by User interfaces or by Web Services.	R	
RFR003	Reports and Graphics	Must present numeric reports or graphics and diagrams, which can be general or detailed ones.	R	
RFR004	Reports and Graphics	Must ensure precision in the report presentation.	R	
RFR005	Reports and Graphics	Reports/graphic printing and exporting functionality	R	
RFR006	Reports and Graphics	Dynamic reports which view information based on personal user requests.	R	
RFR007	Filters	The dashboards with reports and graphics should allow filtering with advanced and professional methods	R	
RFR008	Filters	Should give possibility to the users to easily use filters to build and personalise reports fast and professionally	R	
RFR009	Analyse	The System should transform and view data in a statistical format easily accessed by users	R	
RFR010	Analyse	The System should implement analyses with advanced techniques, to help managing and monitoring the performance of the system.	R	
RFR011	Alerting	The System should send mail alerts to the administration and clerks about the status of the case from the backend (in case of asynchronous services).	R	
RFR012	Alerting	The System should send mail alerts to the clerks to remind about processing the case, if the limit time of the case is running out.	R	
RFR013	Logging and Tracking	The System should track the access of the reports	R	
RFR014	Case management Reports	These reports will be viewed and used by governmental administration. to know and control the functionality of the system and the work of clerks (for example): • The number of opened cases in a day, month… • The number of closed cases with success • Time the cases were processed • Which services are most requested? • The period a case stays not processed. There must be send email alerts to the clerks and other specialists when the case is not processed for more than an allowed time limit.	R	

ID	Function	Description	Type	
RF015		The reporting component should produce statistical reports for the Categories of data according to Schengen catalogue, based in at least these parameters: • persons, • documents, • objects (vehicles, vessels, aircraft, telephones, other items…) • etc.		
RF016		The reporting component should produce statistical reports, for Categories of data according to Egmont: • Suspicious transactions (STR) • Cash transactions (CTR) • Reporting entities (banks, Insurance Sector – insurance companies, Securities sector– brokers (CDA and KHOV), Investment companies, Legal persons dealing in currency exchange, Leasing companies, Casinos, Real Estate agents, Dealers in precious metals and precious stones, Lawyers, Notaries, Accountants, Auditors, Trusts and companies providing services of founding legal persons, Investment funds, etc.)		
RFR017	Performance management Reports	These types of reports will be viewed by the DPMLTF. For example, some useful reports: • The system servers' utilisation • The load of processed data • The response time from backend for services • The failed requests because of communications • The average number of concurrent requests flowing in the system	R	
RFR018	Combined Analyses	It should be possible to combine data that are project related with available data about citizens/business entities and produce analysis across regions, municipalities, industries, etc.	R	
RFR019	Process Execution Monitoring	Analysts should be able to perform business activity monitoring: identify process' bottlenecks, identify process instances that last longer than the average, compare process duration over different time periods, etc.	R	
RFR020	Data Visualisation	Analysts should be able to use different types of data visualisations to spot trends, hidden patterns or show data in the form that is easy to understand.	R	
RFR021	System reports	System administrators should be able to monitor systems and analyse: • Application usage at different levels • System outages; • System performance; • Service performance; • System or service peak/off-peak performance.	R	

ID	Function	Description	Type	
RFR022	Analyses Environment	Analysis should be done with intuitive, easy to use interface that requires minimal user training and encourages self-service. Results should be easy to share in the form of reports or dashboards The solution shall support: • Multi-tier architecture • Web-based access • Offline reporting capability • Ease of use • Ability to connect to various data sources and to report on joined data • Export data in various formats, Excel, PDF and HTML as a minimum • Seamless Integration with MS Office tools	R	

2.3 Other Non-Functional Requirements

Expandability.
The system is expected to cover a wider scope in the future, and to offer to its users extended access to new features and new data. Therefore, the architecture of the system shall support distributed solutions. Additionally, the system should permit technical ways to extend its provided functionality, robust SDK and enable integration with other systems providing APIs.

Network Topology.
The system should be able to work in intranet topology in a WAN, while end users will access it through secure connectivity.

Number of Documents and Records.
The software should put no limits to the number of documents and records that can be archived and indexed, which should be limited only by hardware and storage size.

Software licenses
All software licenses for databases, applications development and other third-party licenses that are needed for the System development/implementation and work should be provided by the contractor as part of system development, whenever those are not provided by DPMLTF.

2.4 Architecture Requirements

General Requirements

The system architecture shall be split into layers to decouple user interface, business layer and data layer.

The proposed Infrastructure Architecture must be designed in a way to be capable for future enhancements.

This architecture should support three requested main components:

a. The intranet facing system that allows the officials of the reporting agencies to report electronically;
b. The Data Integration Gateway that will assist the system to get data from external systems. DI Gateway (DIG) will be a supporting architecture making possible the integration of available external electronic systems. This architecture is based on a messaging mechanism (publish/subscribe) will make possible to connect and communicate with external systems (WEB services). Through this architecture can be enabled interoperability with diverse electronic systems in service of government agencies, reporting agencies and foreign partner agencies. Also,

though this component will be possible to expose for the external partners DMLTF functionalities (e.g. data fields) through the Portal.

c. The internal CMs system will be accessible only to DPMTF and designated to fulfil user requests in the institution, those are responsible to administer the data, information and the cases.

It is recommended that the first component should keep a shadow register of online reporting that will be able to synchronise with the internal subsystem database (back office system).

A high-level view of the required architecture is presented in the Figure below

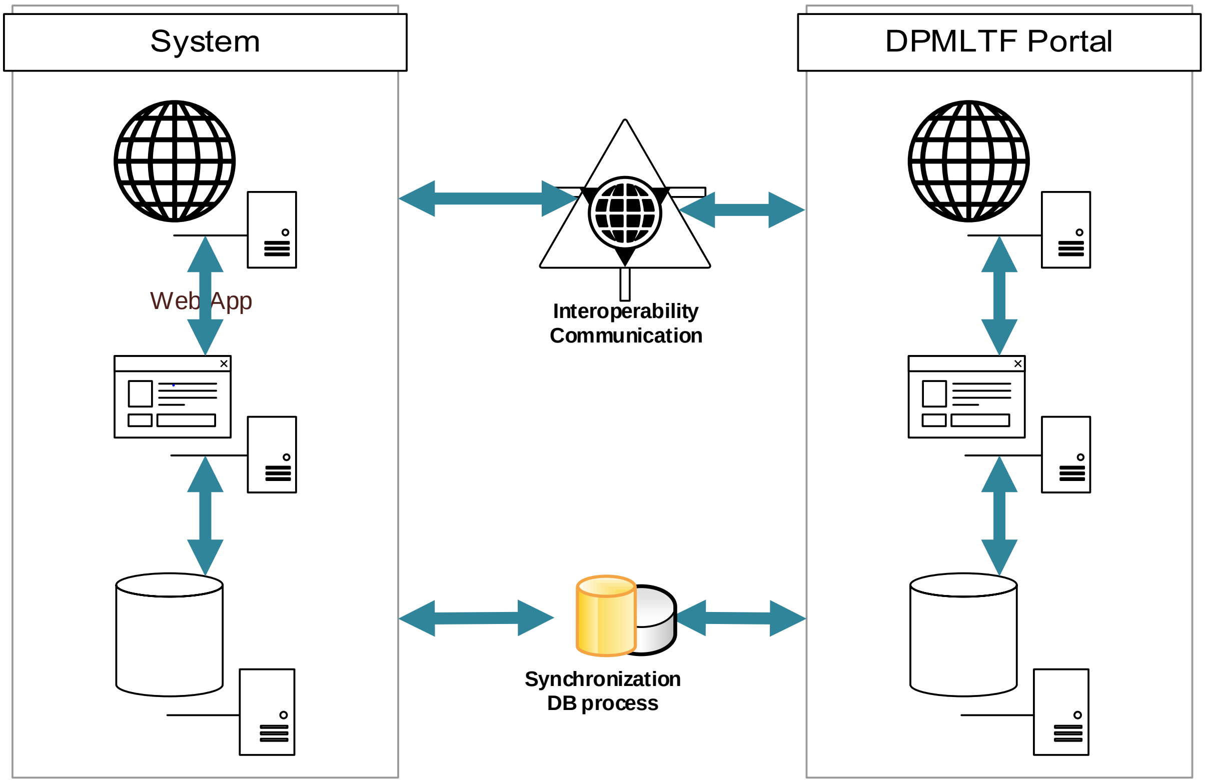


Figure 2 High Level Architecture.

This figure is intended to be a high-level overview of various components, focusing on the entire system. As such, it is not complete and even for components listed in the documentation it may not represent the current real network and service architecture of DPMLTF.

The above architecture will be supported by the respective hardware with the technical requirements as described in the paragraph below.

It should keep in mind that this infrastructure will have to process quite many applications as per the figures below:

- It is estimated that there are approximately 40-80 staff members in different roles;
- For each of them is needed information from several sources of the different types;
- The frequency of reporting from the agencies depend on the type of the agency: daily, periodic as weekly/annual, upon event, etc.
- There are more than 30 institutions from which DPMLTF requests information to verify what the subjects have declared, including state institutions, banks and financial institutions.

The development of the DPMLTF should be carried out according to the Montenegro IT government requirements and relevant security standards.

The development of the system shall be guided by the modular principle preferably using open ICT standards.

The system shall allow for further expansion and additions of new functions or improvements.

The system shall be simple and user-friendly, and its functionalities shall be ergonomic and shall have a logical concept.

The language of the system is Montenegrin.

Use of Continuous Delivery approach is recommended.

When possible, the System can be developed using off-the-shelf solutions allowing for further customisation.

Scheduler Requirements

As required, there will be a continuous need for notifications. The system should have configured Internal scheduler that runs various tasks like full re-index of the database, bulk verification of data, notification of users about deadlines and problems with their information, etc.

The system should perform a timeline control for the DPMLTF workflow process.

System Management, Administration, and Security Specifications

General Requirements

In addition to the management, administration, and security requirements specified in each section covering the various hardware and software components of the System must also provide for the following management, administration, and security features at the overall system level.

Security & Data Integrity

A Complex System of Information Protection will eventually be created and certified for the DPMLTF project.

The contractor will assist with preparation of the project documentation for Complex System of Information Protection (provide necessary documents and advise). Contractor should consider that the project is going to deal with information with limited access and plan and project Complex System of Information Protection with respect to that fact. The Contractor can be required to obtain certification of the Complex System of Information Protection under this contract.

The system shall guarantee data integrity, accountability and accessibility and prevent any altering, damages and unauthorised access to the system data.

Access to the system shall be realised by using the latest version of TLS protocol.

The system shall guarantee full data storage and integrity by using back-up mechanisms for database and the following mechanisms: The data entered into the system may not been edited, damaged or deleted without authorisation;

Any unauthorised attempt to edit data shall be logged with further possibility to be subjected to audit.

The system should log each activity related to a unique subject (e.g. personal ID number), so that there would be a central insight of who did what and when from the first opening the case to the last entered into the system.

A specific system auditor role should be implemented to prevent data alteration and manipulations. The detailed log file should be prevented from deletion and accessible only where a privileged DPMLTF official and the Auditor person role enter both their passcode.

This should prevent the log files from being manipulated by a single person.

2.5 Operating environment

In order to implement the System, DPMLTF will provide the necessary hardware and networking infrastructure which will be hosted at DPMLTF premises in Podgorica.

The following server infrastructure will be provided by DPMLTF for installing the System

Role	Quantity	RAM	CPU	HDD
Web	2	Minimum: 32 GB Preferred: 64 GB	Minimum: 4 core @ 2.2 GHz Preferred: 8 core @ 2.2 GHz	Minimum: 2x300GB Preferred: 2x600GB
DB	2	Minimum: 32 GB Preferred: 64 GB	Minimum: 4 core @ 2.2 GHz Preferred: 8 core @ 2.2 GHz	Minimum:2x300GB for OS Preferred: 2x300GB for OS + 2x600GB for the content

3 TRAINING OF SYSTEM USERS TO WORK WITH THE APPLICATION SOLUTION

A train the trainer program should be implemented within the project effort. The Supplier must train the trainers chosen by the beneficiary. Every system role must be covered.

The Supplier must supply within their offer a training plan showing the planned dynamics and content. Training must cover all modules of the systems, in practical and theoretical level.

All training will take place at the central location of DPMLTF in Podgorica, on the premises and with the equipment of the DPMLTF

The Supplier must deliver user documentation on the use of the CM SYSTEM, which will be used for training. Therefore, during training each participant/user shall have a manual about the training. It must be delivered electronically, in Montenegrin language and must be available for end users internally.

It is projected that the Supplier shall organise the testing of the participants after the completed training on the premises of the DPMLTF, with tests prepared by the Supplier and authorised by DPMLTF. The test results will be sent to the Project Coordinator of DPMLTF, who will decide on any potential additional trainings for individual users.

4 SOFTWARE REQUIREMENTS FOR HARDWARE AND SYSTEM SOFTWARE

If the proposed solution is based on the Microsoft products, DPMLTF's users are licensed to access Microsoft environments as part of global agreement of the Government of Montenegro with Microsoft, under the Microsoft Enterprise agreement framework (OS Microsoft Windows 10 , Microsoft Office 2016, Microsoft SQL Server 2017 , Windows Server 2016)If the proposed solution is not based on Microsoft technologies, the bidder must provide the relevant licenses for each user that will access the CM SYSTEM.

User workstations at DPMLTF have the following characteristics:

- Operating system Microsoft Windows 10;
- Web browser Internet Explorer 8 or newer (for Microsoft Windows operating systems 64 bits), Mozilla Firefox 3.6 or newer, Google Chrome 10.0 or newer, Opera 10.0 or newer, Safari 4.0 or newer.

The Supplier must list in their offer all the specific hardware and software requirements that are appropriate for the given solution, and which vary from the mentioned resources provided.

All the potential additional costs stemming from the need to order additional hardware and software components must be included in the bidding price.

The Bidder must adjust their application solution to the abovementioned resources provided by DPMLTF, in order to ensure the **normal** functioning of the application and database.

Normal functioning, i.e. acceptable performances is defined as response time of application complying with the following:

Response time should be measured on a workstation connected to the production system and attained at least 95% of the time under maximum workload conditions when the maximum number of designated users (40-80 users)are logged in to the system

5 PROJECT IMPLEMENTATION AND REALISATION

The period of project implementation and realisation must not be longer than 180 calendar days.

The Bidder shall give details of their suggested methodology of implementation, as well as the most detailed plan of project realisation possible with all its relevant activities, performers of activities, deadlines, and potential bottlenecks and key points. It is expected that the Supplier offers a plan of the implementation realisation of the software solution in phases:

- Inception report;
- Analysis;
- Design;
- Software solution development;
- Implementation of testing environment;
- Testing of software solution;
- Producing the as-built documentation, project documentation and user instructions;
- Completed training of administrators and system users;
- Establishment of production environment;
- Production.

The Bidder shall also compile a list of potential risks that can jeopardise the project realisation, as well as suggestions for their minimisation/elimination.

Upon signing the contract, the Ordering Party will send the Supplier the following set of documents:

- System architecture
- Description of workflows (including the existing documentation and forms that are currently being used in DPMLTF),
- Printed glossary of data – containing exact data sets regarding the equipment from the subject of the bid to be conducted in the new system.

It is expected that this set of documents will contribute to a faster and more effective phase of Software Solution Development Analysis.

In accordance with the characteristics, available functionalities and options for expanding the chosen software solution, and all this in agreement and collaboration with the Supplier, the Ordering party will also define in detail the new processes that will be the basis for the complete realisation of the software solution.

In establishing the system environment and necessary infrastructure, DPMLTF's appropriate technical service will play a significant role.

6 VERIFICATION/ACCEPTANCE

Verifying the success of the completed phases of implementation and testing of the software solution shall be carried out by a professional commission consisting of a Supplier's consultant, and a person to be appointed by DPMLTF.

The exact list of team members that will monitor the implementation of the CM SYSTEM, manner of testing and reporting will be defined in the inception report.

The elements of delivery which the Bidder must complete are:

- A Software solution which meets all the agreed functional requirements on the required technological CM SYSTEM
- Training of internal users
- Launching the new solution into production work
- Deployment of the new solution with good, acceptable performances

- Project and user documentation and instructions

The software solution that fulfils all the agreed functional requirements on the required technological CM SYSTEM will be verified as follows: the Supplier will carry out a presentation in a testing environment to the relevant representatives of the Ordering party, their advisors (the supplier of the study) and representatives of CoE where they will directly see and confirm that all agreed (functionality and content), has been executed and completed by the Supplier. A written protocol shall be made serving as proof of the completion of the contractual obligations by the Supplier, in accordance with Article 9 of the Legal Conditions (Section C. of the Act of Engagement). Performance and Load testing tools shall be proposed by the supplier and used during the presentation in the testing environment, to reproduce a real-life workload scenario which is expected when the system goes live.

6.1 Training verification

For the training verification it is necessary that the Bidder:

- Develops the training program based on the requirements listed in this Technical specification,
- Completes the training of all the course trainees,
- Devises tests for the trainees which all the trainees must pass,
- Performs the testing of staff (in the conditions which the Ordering Party must establish), supervised by the Department.

Training is verified when all the requested trainings are completed and the testing of all the staff is carried out. The obligatory condition is that all the staff pass the test with a minimum of 85% of completed tasks predefined by the minimum percentage of solved tasks. The minimal percentage of solved tasks is defined by the project coordinator from DPMLTF, in collaboration with CoE. A written protocol will be made, serving as proof of the completion of contractual obligations by the Supplier.

6.2 Verification of launching the solution into production wor

Verification of launching the new solution into production work is ascertained by performing Functional Testing and User Acceptance Testing (UAT). A written protocol will be made thereof, and it will be used as proof of the completion of contractual obligations by the Supplier.

The verification of the production work of the new solution with good, i.e. acceptable performances is ascertained by measuring the response of the application solution on an application sample chosen by the Ordering Party (Performance and Stress Testing). The measuring of the response will be performed in production conditions and in the period chosen by the Ordering party and in the presence of the Supplier and CoE representative. The measuring of the application solution response will also be performed in the intranet, at a minimal throughput of 20 Mbps, at a given workstation. A written protocol shall be made thereof, serving as proof of the completion of the Supplier's contractual obligations.

The Contractor's must submit a proposal for Functional acceptance tests for each phase.

The format of the Functional acceptance tests should be as follows:

Number of the test:	
Name of the test:	
Relation to the Functional requests for the phase:	
Steps in conducting the test:	
Expected results:	

6.3 Project documentation

All the project and user documentation must be in **the Montenegrin language**

The Project documentation must include:

- Logic data model;
- Physical data model, i.e. a complete database scheme (which includes all the objects in the database);
- Functional model of the system, with a description of each function;
- Model of roles, as a method of controlling data access;
- As-built design, which includes:
    - A description of the requested system environment and its establishment,
    - A description of the application system installation,
    - A description and detailed specification of all the necessary and performed system settings for the system to function efficiently in the production regime, which includes but is not limited to:
        - all the settings on the "client" application side,
        - all the settings of the client operating system
        - all the settings of the server operating systems,
        - all the settings of the web environment,
        - all the settings of the ancillary system software,
        - all the settings within the application system,
        - all the settings in the database.

6.4 User documentation

User documentation must include:

- General instructions for using the application, i.e. user interface;
- User instructions (manual) for each of the installed and used modules, i.e. functions;
- *"Online help "*, which is accessed directly when working with the application by pressing the F1 key.

Verification of project and user documentation and instructions is ascertained by the delivery/availability of their electronic versions (*Word, HTML and*/or *pdf* files), as well as by the accessibility/availability of *on-line help* with the appropriate content during application use. A written protocol will be made thereof, which will serve as proof of the completion of the Supplier's contractual obligations.

6.5 Contractor obligations

The contractor is obliged to:

- Generate the executed versions of the Software, on the equipment which is the property of the DPMLTF in the premises of DPMLTF.
- Thoroughly test Software, including, but not limited to, all its subsequent releases/editions, subsequent upgrades, enhancements and subsequent versions. This must be documented in written form and it should include detailed description of tests, the manner of conducting tests, test results and List of program errors and important issues. Plans for testing must be reviewed by DPMLTF in order to ensure that quality standards are maintained. transfer its entire right, title, and interest in anything created or developed under this Contract including all patents, copyrights, trade secrets, and other proprietary rights.
- execute and aid in the preparation of any papers necessary or helpful to obtain or maintain any patents, copyrights, trade secrets, and other proprietary rights under this Contract.
- handover the source code for an unlimited use without copyright restriction and Installation of development and testing environment to DPMLTF on optical medium. The Source Code is ownership of DPMLTF.
- The Contractor's obligation is to submit a proposal for Functional acceptance tests for each phase.
- The format of the Functional acceptance tests should be as follows:

The obligation of the Contractor is to guarantee that no part of the Software or documentation, covered by this Contract, shall contain the protection feature designed to prevent the use of the Software. This includes, but not limited to, any computer virus, worm, software lock, drop dead device, Trojan-horse program, trap door, time bomb or any other code or instruction that can be used for assessing, modifying, deleting, damaging or disabling the User Software or computer system. The Contractor is obliged to transfer ownership of the Source Code for the Application as well as physically deliver the source code to the Police Department

The Contractor shall compensate and enable integrity to the DPMLTF from complaints or activities of any or all third parties, including losses, expenses, responsibilities, real compensations for a lawyer and other expenses that may occur form such complaints and activities, where the reason is that the Software infringes or violates the copyright, brand, patent or business secret of a third party, on the condition that:

- DPMLTF immediately informs the Contractor in written on any complaints;
- The Contractor has a sole role of defending from any such complaint and all to carry out all the negotiations for reaching an agreement or compromise;
- DPMLTF shall ensure reasonable cooperation with the Contractor.

In any activity based on the complaint for violation, the Contractor has, at his own expense, (i) obtain for the DPMLTF the right to continue using the Software, or (ii) replace or modify the Software with the Software that does not cause violations but it ensures the same functionality.

7 WARRANTY AND SYSTEM MAINTENANCE

The Bidder must include in the price the maintenance of the Application with a warranty period of at least 12 months, which will secure the normal operation of the application and database. The warranty period begins with the date of acquisition (delivery and acceptance) of the information system.

Note: Bids with a warranty period shorter than 12 months will not be accepted.

As security for enabling the normal functioning of the information system within the warranty period, the preferred Bidder must secure a single promissory note registered with their parent bank and a letter of authorisation for 50% of the total amount of the contract.

If the Bidder fails to meet their obligations and deadlines stipulated in the technical specification, the Ordering Party has the right to activate the promissory note submitted as a guarantee of the completion of their obligations within the guaranteed period.

The Bidder must specify the price for the annual maintenance of the offered solution for every year following the offered warranty period for 5 years.

Upon the completion of the project, the Bidder is expected to continue to perform the following:

1. After receiving a written notification from the Client regarding the irregular functioning of the software solution, they must come to the premises and identify the problem, fix the problem/make an intervention so the programs can function correctly, or recommend how the problems can be overcome.
    7. All the irregularities in the functioning of the software that impact DPMLTF's capacity to use the system productively must be eradicated within 2 calendar days; more serious irregularities must be eradicated within 3 working days.
    8. The Bidder must expand or enhance their smaller solutions, as requested by the Client and which are the subject of this procurement, which includes alterations of the existing and the creation of new reports, minor changes in the data entry application, modifications and viewing, and change in the data access policy. "Minor changes" are defined as engaging the supplier up to 2 days per month, with no additional charge.
    9. To expand and enhance their solution at the Client's request (major intervention) which are the subject of this public procurement, and to create/modify the user documentation and to offer training to all the relevant users, with additional payment.

To perform additional training of users (whether new or current) regarding issues and areas which are specified and particularly requested by the Ordering Party, with additional payment.

ANNEX 1

Case Management Application – Requirements

1. The Application (CMA) is used for opening, registering and managing cases which are in the jurisdiction of the DPMLTF. The process of authentication and authorisation of the user, the application implements in integration with the correspondent user authorisation. The Application is used to keep records of DPMLTF's cases. Through this system both review and processing as well as "document management" of the related documents must be given. Documents can be electronic (free and structured text) scanned, fax documents, mails, pdf attachment, photos, photocopies of the documents, etc.

2. The Application has to have the possibility to independently process all cases which are grouped in few main groups and related subgroups (depending on internal division of work in the APMLTF and number of Divisions – line of work, which is determined by internal systematisation of the Department) and which is flexible and adjustable on administrative level after the application is created.

3. Security within the application must be ensured so that each employee in charge of the case can see only his or her cases, but with the possibility of alerting if there is an overlap of cases with another employee, regardless of the group of cases. In case of overlapping or connection of cases, the possibility of communication between the employees in charge of the cases should be given, through internal electronic communication and a formal request for access going to several addresses within the DPMLTF. The time limit of the case and an independent automatic alert should be provided when the deadline for completion of the case expires. Control of case access and act upon the case must also exist.

4. When entering information (or opening a case), it must be compulsory to enter data concerning the implementation of the Law on protection of personal data (records of personal data, date until data is stored, when they are deleted automatically…), the Data Secrecy Law (confidentiality level, expiration of the confidentiality…), use of information (codes for limiting the use of information - handling code), reliability of sources / accuracy of information (4x4).

5. The Application must provide the possibility of processing incoming standardised documents from multiple sources ranging from paper to electronic and minimising manual entry and mistakes made by employees. If it exists, the application in incoming communications must have the possibility to download and read, and structured storage of all keywords (entities) from XML attachment and UMF communication format.

6. It must be possible to quickly search cases in all key fields, in order to reduce the search and memory of numbers or keywords in cases. Key fields are key words, fields of work, groups and subgroups of cases, which organisational unit initiated the case (the sender), case reference number, communication reference numbers, start dates, expire dates, personal data records within which data is stored, deadline for storing data, confidentiality level with evaluation deadline, tag for information restrictions, keywords (categories of persons, documents, cases), as well as the ability to combine these fields and adding new ones in the future without major improvements on the application itself. The Application must have the possibility to create internal bases which will also me checked when entering entities (e.g. databases of persons who are under international sanctions or databases of persons registered as persons of interest in police records and similar). The Application must have the option for Free Text to input the reasons for extending the period of storing data or period for data secrecy. Free text search must also be enabled.

7. The Application must have the possibility of communication between the employees on the principle of chat in the case they are acting upon the application must have the possibility to show in one place, all notifications and messages sent through the application.

8. The Application must be compatible and linked with the existing Case Management Applications in the Criminal Police Sector (International Police Collaboration and Criminal Intelligence Analytics) for the electronic exchange of data between these Sectors and mutual (automatically) checks of databases both when entering keywords and when searching for databases.

9. The Application must have a portal through which all available national (DPMLTF's database, Police Department, MIA and other authorities, as well as operational databases of the International Police Collaboration and Criminal Intelligence Analytics) and international (Interpol, Europol) databases can be checked in the background with one entry. If checks are done through the case, the application must visually

signal in which databases the keyword match occurred. Also, that available databases can be checked from the case, using keywords already entered.

10. The Application must have the ability to index the keywords, semi-automatically (as offered candidate for entry) or automatically, if the information structure is already recognised (e.g. UMF information format or other xml format), from all files and display their content through the preview option. From this content the user must be able to select the desired keywords and their further processing (entering into the application, i.e. storing them in the database and automatically checking with the data already in the database as well as with other databases), such as filling in forms for cases data inputs as well as other processing.
11. As a reaction of the system to important events (defined by the administrator) in the user's work with the application, the application must be able to send appropriate electronic notifications to the defined addresses with the corresponding predefined content. Notifications – alarms are concerned: expiration of deadline for the completion of the case, time notification for any activity within the case, expiration deadline for storing personal data, expiration of the data confidentiality deadline, entering new data in the case, insight into the case by other employees, deleting the case, adding new employees on the case, consolidating and separating the cases, etc. This process of sending notifications is automatic and does not depend on the user. One example of an important event in this regard is the attempt by an unauthorised user to access the contents of a case, or the entry of new communication / information into an existing case, thus eliminating the need for the acting inspector to continually check all his or her cases in order to check if there is anything new in them.
12. The Application must have the possibility for the user, when sending standardise messages to the collaborating institutions, to do so with minimal data entry. Through the admin part, it must be possible to write content that meets defined message standards (predefined communication forms, containing all the essential details, which will be updated and added by the user).Case-specific information supplemented by these predefined content are communications sent by the DPMLTF as well as Departments within the DPMLTF. In this way, all communications are standardised and allow for the responsibility of the user to be reduced only to the correctness of the data in the act, while the set of metadata is predefined, mandatory and generated by the application. To this end, the application must not allow the transition to the sending point if all predefined fields are not filled in (required fields will be administered by a local administrator as needed). Predefined communication formats must always have the possibility to automatically enter in the corner of the act, the reference number of the case when printing.
13. The Application should also have the option to mark some cases, whether existing or new, as cases with increased importance, for certain employees, a group of employees, administrator or Head. Thus, beside the employee in charge of the case, the users for which the case is marked as significant are also notified about all changes and new development in the case of such importance. It must also have the option to formally delete data from the working part when data storing period expires i.e. placed in an archive that is not searchable except for the administrator.
14. The Application must monitor statuses of all letters/acts. If the sent acts were not answered in the specified period, the user will be alerted in this regard and the statuses of the case will be updated. Warnings are also related to notifications to the heads of untimely responses or delays in case management.
15. For the purpose of proper and timely handling of cases, the Application must be linked to the calendar of absences, whereby all employees who are absent from the office are obliged to enter their leave in the calendar. Such entry allows the Application to notify the employee who entered the request / opened the case that the said employee is not at work, thereby allowing the case to be rescheduled to another employee in an emergency, or to add a new employee to act upon the urgent request by the return of the employee in charge of the case. Also, depending on the deadline for completion of the case, the application automatically sends warnings (hierarchically, to the direct Heads and to the person who entered data in the case) that the inspector in charge has not read the new message / request, unless the message / request is viewed after the expiration of 10% of the deadline which is given for completion of the case (if the deadline for completion of the case is 10 days, the alarm will arrive after one day, and if the deadline for completion is 4 hours, the alarm will arrive after 1 hour). All warnings arrive via electronic notification to predefined user addresses.
16. The Application must have the capability of the so-called "internal locking of cases", which implies limiting access to the so-called "sensitive cases" only to employees working on it, and in cases where the case does not have a confidentiality level.

17. The Application must have the possibility to extract the highest level of confidentiality from the communications / messages in the case and accordingly change the level of confidentiality of the case where the communications are located (the case carries the level of confidentiality of the communication which has the highest level, and the communications within the case may have different levels of confidentiality).
18. The Application must provide the possibility to check the work and promptness of the case in DPMLTF and individual Divisions. This is accomplished by creating predefined reports within the application according to the specifications of the report requester.
19. The Application must have a module for upgrading to the existing system of communication with reporting entities and electronic receipt / sending of information to / from them, by electronic signature.
20. The Application must be flexible so that administrators can easily create new organisational units within DPMLTF so that internal communication and sending of requests can take place between them, even when the organisational scheme changes. The Application must thus enable the creation of internal cases at the Division level, according to communications - requests sent between Divisions.
21. The Application should also have the option of keeping all logs related to work on the application, in order to preserve their integrity and avoid the possibility of modification by the users of the application.
22. The Application should also have adequate security systems regarding securely logging of authorised users and digital signing of all communications.
23. The Application should be linked to the ESW communication link, Europol Siena web services, Interpol I-link web services and I-24/7 communication link, police application web services (searches, on duty, border), MIA web application of civil status (persons, documents, weapons), web application of the Ministry of Justice (criminal records), web applications of other authorities (Central Bank, Real Estate Administration, Tax Administration, Central Registry of Commercial Entities, etc…)
24. The Case Management Application should keep records of the documents and cases used by users of the Department for Prevention of Money Laundering and Terrorist Financing. Document and case data would be entered by filling out an electronic form or uploading an XML file by system users along with manual input by system users if the cases were submitted in paper form.
25. The Application should integrate and enhance the existing Institutions and reporting entities Portal existing in the Department. The Case Management Application would improve and upgrade existing modules (for reporting entities) by upgrading the portal module with data visualisation entered by the portal users while enhancing the overall system used by the Department users to overcome the existing need for administrator intervention in the event of an error in the data entry by portal users, inability to view data entered through the portal on the same day except through the database (necessary knowledge of databases), unstable integration of portal and system databases, through:

- Enabling a tabular view of the data contained in the portal database which, facilitates the said view for the system administrator to check or intervene if incorrect data is entered.
- Enabling increased validation of data entered by the portal user that also reduces system dependency on administrators.
- Improvement of integration between system databases and portals, advanced algorithms for data transmission and notification system in case of error.
- Improvement of the portal would reduce the time the administrator spends validating the data entered and assisting the portal users. Advanced validation of forms and XML files uploaded by portal users would allow faster and more efficient data entry. Improving the mechanism for transferring data from a portal database to a system database would increase system stability and reduce the number of interventions and validation by system administrator.

26. The Application should enable coordination of different cases and communications, consistent monitoring of cases in order to prevent overlapping of cases and communications, linking different cases, based on key parameters (keywords), for comprehensive use of available databases.
27. The Application should allow full text search and introduction of smart indexing modules based on previous entries in the database.

28. The Application should perform adequate and fast analysis and checks of existing national and international databases, as well as extract background checks based on the entered keywords (entities), for their postponed checking through national and international databases (so that working processes would not stop in case of background checks last too long, but these background checks could be postponed, e.g. overnight and etc.) and flagging (marking) for the acting inspector if there are matches with national databases.

29. The Application must have indexing (structuring) of databases made from data from previous cases, which would provide a good basis for the use of analytical tools (such as I2), as well as enabling the establishment of a logical connection and characteristics between the entities entered, with the option to export that data in a format acceptable for analytical tools for analytical processing. Introducing entity characteristics (e.g. suspect, accessory, witness, injured party…) and enabling connection – relations between entered entities for export in I-2.

30. The Application must be able to monitor the fulfilment of the set deadlines for completion of the case and monitor course of action upon request.

31. The Application must allow adequate compliance with the standards of personal data protection and secret data (deadlines for keeping in records of personal data, according to legal restrictions, automatic warning of expiry of dates, deleting of personal data, etc.)

32. The Application must enable the production of statistical reports, which must contain the following categories of data by which reporting (as parameters) can be performed:

    a. Categories of data according to Schengen catalogue

       i. persons,
       ii. documents,
       iii. objects (vehicles, vessels, aircraft, telephones, other items…)

    b. Categories of data according to Egmont

       i. Suspicious transactions (STR)
       ii. Cash transactions (CTR)
       iii. Reporting entities (banks, Insurance Sector –insurance companies, Securities sector– brokers (CDA and KHOV), Investment companies, Legal persons dealing in currency exchange, Leasing companies, Casinos, Real Estate agents, Dealers in precious metals and precious stones, Lawyers, Notaries, Accountants, Auditors, Trusts and companies providing services of founding legal persons, Investment funds, etc.)

33. The Application must provide a unique and centralised electronic storage of all data in the cases.

34. Communication within and outside the Department must be enabled directly from the application (generating certain message formats directly from the Application)

35. Indexing (structuring - tagging) all data from received information and automatic checking of existing data(crosscheck),in relation to whether this information already appears in previous cases (if they appear, obtaining case information), it must be made possible in order to prevent overlapping and duplication of police work.

36. Time limits for the execution of requests must be enabled, with adequate alarms in the event of deadlines being exceeded.

37. Forming internal databases (so called passive bases) on cash transactions, in all situations when there is no match and therefore no opening of the analytic cases (as a base to be checked with all new entries, and supplemented with new cash transaction entries)

38. It must be possible to form an internal database of persons of interest and persons subject to international sanctions (as passive databases) through which all data entered will be checked.

39. It must be possible to store data in the database and to check the database with the help of adequate alarms, whenever a hit is detected in the database

40. It must be possible to monitor case/communication by:

- the employee in charge of the case

- area (line) of work
- deadlines for the completion of cases
- sender
- recipient
- Etc…

41. The Application must enable:

    a. Checking the actions taken regarding the case
    b. Storing all information in electronic folder specified for the cases related to information
    c. Possibility to merge cases where the subject of investigation is the same person
    d. Compliance with EU standards in the field of data protection and data confidentiality
    e. Applying principle “need to know" through the introduction of handling codes (Handling codes: H0, H1, H2, H3)
    f. Application of rules of intelligence work in the area of evaluating data/source (4 x 4 model)
    g. Providing statistical data and reports related to cases/communications

42. The Application must provide the connection to the internal secure mailing system for direct exchange of data via a secure electronic communications network (Egmont Secure Web, FIU. Net, Interpol, Europol…)

43. The Application must have data processing logging (according to the EU Directive on the processing of personal data Article 25) (enable recording of all records (logs) for the following processing operations: collection, modification, insight, detection, including transfers, combining and deletion. Records on performing insight and disclosure allow to establish explanation, date and time of such actions and, if possible, identity of the person that performed insight or disclosed personal data and identity of the recipients of such personal data)

44. The Application must ensure that data processing security is introduced according to the EU Directive for processing personal data Article 29) - enable appropriate technical and organisational measures to ensure an adequate level of security with respect to risk, in particular with regard to the processing of specific categories of personal data, with particular reference to prevention:

    a. prohibit unauthorised persons from accessing processing equipment used for processing (monitor access to equipment);
    b. prevent the unauthorised reading, copying, modification or removal of data carrier (monitor data carrier);
    c. prevent the unauthorized entry of personal data and the unauthorized viewing, modification or deletion of stored personal data (monitor storing);
    d. prevent the use of the automated processing systems by unauthorized persons using data transmission equipment (user monitoring);
    e. ensure that persons authorized to use the automated processing system have access only to personal data provided for by their access authorization (data access monitoring);
    f. provide an opportunity to verify and determine to which authorities, personal data have been transferred or could be transferred or made available using data transmission equipment (communication monitoring);
    g. provide an opportunity to subsequently check and determine which personal data have been entered into automated processing systems and who and when they were entered (monitoring entries)
    h. prevent the unauthorized reading, copying, alteration or deletion of personal data during the transfer of personal data or the transfer of data carrier (monitoring transmission);
    i. provide the possibility of reinstatement of installed systems in the event of interruption (reinstatement);
    j. ensure that the system is functioning well, that system malfunctions are reported (reliability) and that personal data stored cannot be compromised due to the system malfunctions (integrity)

45. The Application must ensure connecting with criminal intelligence databases and international police cooperation databases for checks of existing operational data. Introducing the new level of access (of the user) to the data (under the principle urgent in connecting with criminal intelligence databases and the databases of other state authorities.

46. The Application must enable entering of batch formats (huge set of data for compiled checks). This is particularly important for cash transaction reports.

47. The Application must enable the monitoring of physical movement and filing of documents. The filing would mean placing documents at a certain physical location for permanently being kept where the location is uniquely designated (row, shelf, floor), as well as the barcode or some other method of designating documents. Detailed records on filing documents would eliminate the possibility of losing documents

48. The Application must enable the system users to assign the case to other users within the Department and set the deadlines for completing it while the system would generate notifications and warnings in case of missing deadlines. The records on meeting deadlines and conducting the undertaken activities regarding the case would enable the Department management to more precisely identify the "bottlenecks" in the organization. The monitoring of cases would be carried out upon the following criteria:

    a. The officer responsible for the case
    b. Area of work
    c. Deadlines set for completing the case
    d. Sender or receiver
    e. Category and confidentiality degree of cases

49. The system has to offer the option of categorizing cases both according to types and confidentiality degree so that such categorization together with the function of the system users would define the rights of access to and review of the cases in the system. During the review of the cases the system would record all the activities of the user related to a certain case and it would create a detailed auditing trace (audit).

50. The communication of users in the application would be made through "Chat" module which is the integral part of the system and which would keep all the messages exchanged among the users and thus keep the history of cases and documents.

51. The Application must enable the visualisation of data through charts and generating reports that would play a great role in improving the functioning of the Department for the Prevention of Money Laundering and Terrorist Financing. The graphical representation of data would enable the management of the Department to have clearer overview of all cases and documents that entered into the system under several criteria.

52. The system must function on the principle of automatic data processing which would include:

- Harmonizing upon the structure of XML received data and forms
- Input and searches of existing databases
- Storage of data in entities to which cases and key words are related
- Creating logical and analytical links between them
- Generating notifications and warnings in case of missed deadlines
- Validating all columns and fields in XML file loaded which would be prevent the attempt of irregular loading