CONCEPT OF INTRANET SYSTEM OF THE CENTRE FOR HUMAN RIGHTS OF THE REPUBLIC OF MOLDOVA

Project „Support in consolidating the National Mechanism for the Prevention of Torture according to the Optional Protocol to the Convention against Torture"

1. INTRODUCTION

The project aims at contributing to the prevention of the domination of torture and other acts of violence, inhuman treatment or punishment by consolidating the National Mechanism for the Prevention of Torture according to the requirements of the United Nations Convention against Torture (CAT) / Optional Protocol to the Convention against Torture and under the protection of the national system for protection and promotion of human rights.

Within this project, an analysis of the CfHRM's and the NMPT's tasks was carried out and a range of recommendations regarding the improvements of their institutional capacity for the exercise of the tasks of work were elaborated, these also comprising the support for the improvement and implementation of the legal framework in the domain of human rights protection. One of the main responsibilities of the CfHRM is the acceptance, analysis and processing of the petitions from different categories of natural and legal persons, which covers the most part of the center's occupation and that have registered a growth during the last for years. Under these conditions, the implementation of an automated system of documents' registration, management and processing is absolutely necessary.

The National Mechanism for the Prevention of the Torture (NMPT) was created as a consulting council under the CfHRM which is designated to give consultation and assistance in the exercise of the parliamentary lawyers' attributions in problems connected to the involvement of the civil society in the national torture eradication process, as well as the direct attributions wile monitoring the phenomenon of torture and other cruel or inhuman punishments or treatments.

The system to be implemented aims at the creation of an environment of collaboration and documents' exchange inside the CfHRM and NPM and also at uniting all subdivisions and their representatives into a unique informational system, regardless of their geographical situation. The implementation of such a system would lead to the improvement of the processes of work within the organization, would open the extended possibilities over the skills of information analysis and reference, the control over the documents' flows.

In order to assure the verity of the decisions and judgments taken by the persons with decisive positions, the Digital Signature will be applied to the Intranet System documents.

2. GENERAL PROVISIONS

Full name: The Intranet Management System of the Centre for Human Rights of Moldova and the National Mechanism for the Prevention of Torture

Short name: *Intranet System of the CfHRM and the NMPT*

The concept's aim is to contribute to the implementation of the Intranet System of the CfHRM and the NMPT, as a part of the infrastructure, drafted according to the legislation in force and the international practice in the domain of informational technologies.

3. AIM AND OBJECTIVES OF THE INTRANET SYSTEM

The aim of the IS consists in implementing a modern solution of collaboration and management of workflows and documents to offer a more qualitative public service and make the process of decision-making more transparent. The IS stimulates the use of information and communications technologies (ICT) for the exercise of a more efficient and transparent performance.

System's definition

The Intranet System represents a private informational system used within the organization, which has as definition the totality of information storage and organization procedures, definition and management of workflows, measures of storage and use of the information meant to contribute to the fulfillment of the CfHRM and NMPT objectives.

3.1. INTRANET SYSTEM'S DESCRIPTION

The Intranet System of the CfHRM will be an informational system that will assure a unique point of access to the informational resources, applications and services within the organization. It must offer equal possibilities and similar conditions of work for all branches of the Centre for Human Rights in the territory. It is important to mention that the National Mechanism for the Prevention of Torture is a subdivision of the CfHRM having its own office and this must be considered as a separate entity with similar status for the branches of the CfHRM in the territory. The Intranet system must become a unique environment for collaboration aiming at collecting, structuring and processing the information coming from external sources of the system as well as within it (as internal sources we may mention: internal guidebooks, informative handouts of internal circulation, minutes of internal sessions, etc). The access to all informational objects within the system must be a secured one with clear delimitation of the roles and access rights.

IS Objectives
- creation of a medium of collaboration and information within the CfHRM and NMPT
- clear and unique structuring of the information
- improvement of the work within the organization
- tasks management and their fulfilment
- reduction of the effective time to answer to interpellations
- formation of a data repository regarding the organization's activity
- homogenization of the information, messages and actions in the central office and the branches in the territory
- guaranteed rapid access to the data and information regardless of the location
- automation of the workflows within the organization

IS Principles

The fundamental principles according to which the Intranet System of the CfHRM and the NMPT will be implemented are as follow:
- **Legitimacy Principle** – the functions and operations in the system fulfilled by the its users are of legal character, according to the human rights and the national legislation,
- **Authenticity Principle**– the data stored and presented by the system are authentic. Their authenticity is certified by the existence of a record regarding their creation, as well as a digital signatures applied on these electronic

documents. The electronic documents' authenticity also assures the non-repudiation of the data,

- **Identification Principle**– the informational packages are given a classification code at a system level by which the univocal identification and their referencing is possible,
- **System audit principle** – the system registers the information about the changes taking place, to make the reconstruction of a document's history possible or its condition at a previous stage,
- **Software platform independence principle**– the system may be built based on the modules elaborated by command or based on the existing software products. The concept does not limit the approach of the system's development, as long as the identified needs are satisfied and a greater value for the offered price is granted.
- **Accessibility and integrability principle** – even if it offers multiple functionalities, the system is built as an integral element, used by the users through a unique interface. Moreover, the principle implies the fact that the system's expansion and development will be made by protocols and points of connection projected from the beginning.
- **User-oriented principle (usability**) - structure, content, means of access and navigation are focused towards the system's user.
- **Extensibility principle** – the system's components offer facilities of adjusting and extending existing functionalities for the conformation with CfHRM's needs in a continuous change.
- **Open standards' use principle** for the inter-operability with external systems and for the assurance of the informational according to the norms in force.
- **Security principle** – protection of the information integrity, accessibility and confidentiality.

4. TERMINOLOGY

Antivirus – a program package protecting the operational software from attacks.

Domain – a logic group of computers using the same central data director. This central database includes users' accounts and security information for the resources of this domain. Each person using computers that are part of a domain, receive accounts of unique user names. This account may be granted access rights to the resources in this domain.

E-mail – one of the most frequently used Internet services. It emulates the mail service, when the persons can send messages to the recipient's address.

Workflow - definition, execution and automation of business processes in the event when the tasks, information or documents are transmitted from a participant to the other for an action, according to a set of procedural norms. The organizations use workflows for the coordination of tasks between people and synchronization of data between the systems.

Internet – global network.

PKI - **Public Key Infrastructure** – offers to the users a public network without basic security means such as the Internet to assure the security and private exchange of data using private and public cryptographic key pairs, obtained and transmitted by a trustworthy authority. PKI offers digital certificates that can identify a person or organization and directory services that can storage, if necessary, and revoke certificates.

LAN - Local Area Network – part of the physical and technological infrastructure assuring the inter-connectivity of informatics systems in adjacent places (a building or storey). The defining characteristics of this type of networks include big rates of data transfer, smaller geographic locations and is based on the property upon the network infrastructure (in comparison to those rented from third parties).

Documents' management – a practice used to capture, manage, storage, maintain, deliver and destroy the "documents" within an enterprise. In this respect, the notion of "documents" may be used to describe a large amount of informational assets, including images, textual documents, graphics and drawings, as well as new electronic objects, such as web pages, e-mails, instant messages or video files.

Records' management – the practice to manage the records of an organization from the moment when these are created until their eventual destruction. These include the classification, storage, security, as well as the destruction or keeping of records in the archive.

Licences' management – correct and accounting registration of available software licenses and their use on the existing calculation systems.

Tasks' management – the process of a task management (or a task portfolio) during its whole life cycle, including its planning, testing, control and reporting. The efficient management of the tasks presupposes the management of all aspects connected to an activity, including its status, priority, time, necessary human and financial resources, recurrence, compulsory notifications etc.

Audit reports – records about the actions undertaken within the software system.

Secured network – a network that guarantees the confidentiality and security of communications.

Internet services- the totality of services available on the Internet.

SICDE – An Integrated System of Electronic Documents' Circulation

Single Sign On – a service offering to the internal and external users of the system access rights to the services, based on their credentials in the domain of origin, under the conditions when the domain of origin and the host domain are in relationships of trust.

Infrastructure security system – the security services conceived to assure the system's hardware and software integrity and availability. This includes the automated updating of the software, the distance management and setting up, antivirus, firewall, etc.

ICT – Information and Communications Technologies.

WAN - Wide Area Network – a network covering a big area (such as, the networks with connection exceeding the towns, regions, or countries' frontiers).

Web - **World Wide Web** – represents a big hypertext interconnected set of documents, accessed through the Internet. At present, this term is almost a synonym of the Internet, since the users find it very use to use and access.

5. LEGAL-NORMATIVE SPACE OF SYSTEM'S PERFORMANCE

The Centre for Human Rights of the Republic of Moldova was created based on the Parliament's Decision Nr. 57 of 20.03.2008 with a status of independent state institution with its office in the City of Chisinau.

The CfHRM and the NMPT acts according to the Constitution and laws of the Republic of Moldova, the Parliament's, Government's decisions, international agreements and treaties of which the Republic of Moldova is part, other normative acts and internal guidelines.

The Intranet System of the CfHRM and the NMPT is guided by the same legal-normative framework and conforms to the laws and regulations in the sphere of informatics systems' development and the software products lifecycle.

Especially, the process guiding the elaboration of concepts is defined by the technical regulations "Software Lifecycle Processes" RT 38370656 - 002:2006 elaborated by the Ministry of Informational Development.

The decisions and available space of solutions are modelled by the connective normative acts of the Republic of Moldova, as well as the international standards and practices in the domain.

5.1. LEGAL-NORMATIVE SPACE OF THE REPUBLIC OF MOLDOVA

The normative acts of the Republic of Moldova that are in direct relation with the processes within the CfHRM and well as regulating the organization of informational systems and technical documentation are specified.

- Constitution of the Republic of Moldova
- Law of Parliamentary Lawyers nr. 1349 of 17.10.1997
- Law "of Public Offices and Status of Public Officers " Nr. 158 of 04.07.2008,
- Law of Petitioning nr.190 of 19.07.1994
- Decision of approving the Regulations of the Centre for Human Rights, structure, status of the positions and the method of its financing Nr. 57 of 20.03.2008
- Law of access to information Nr. 982-XIV of 11.05.2000,
- Law of informatics Nr. 1069-XIV of 22.06.2000,
- Law of state informational support and informational resources Nr. 467-XV of 21.11.2003,
- Law of electronic document and digital signature Nr. 264-XV of 15.07.2004,
- Law of personal data protection Nr. 17-XVI of 15.02.2007,
- Government's Decision of special telecommunication systems of the Republic of Moldova Nr. 735 of 11.06.2002,
- Government's decision of certain measures for the creation of a telecommunication System of public administration authorities Nr. 256 of 09.03.2005,
- Government's decision of public keys certification centres Nr. 945 of 05.09.2005,
- Government's decisions for the approval of the Regulations regarding the order of applying digital signatures in electronic documents of public authorities Nr. 320 of 28.03.2006,
- Government's decision for the approval of the Regulations regarding the electronic mail system of the public administration authorities Nr. 969 of 23.08.2007,
- Government's decision for the approval of the Integrated System Concept of Electronic Documents' Circulation Nr. 844 of 26.07.2007,
- Government's decision on the measures for the creation of an automated informational system "State Register of Lawful Entities " Nr. 272 of 06.03.2002,

- Government's decision for the approval of the automated informational system concept "Population's State Register" and the Regulations of the Population's State Register Nr. 333 of 18.03.2002,

5.2. LEGAL-NORMATIVE SPACE AND INTERNATIONAL PRACTICES

Besides the local normative grounds, the concept is based on the international researches, practices, guides, inter-operability criteria, model solutions and requirements etc. The list below includes references used by the authors when elaborating the concept:

- *Legal Framework*
    - UNIVERSAL DECLARATION OF HUMAN RIGHTS of 10.12.1948
    - Optional Protocol to the Convention against Torture and other cruel, inhuman or degrading treatments or punishments, adopted on December 18, 2002 in New York

- *Electronic Information*:
    - Guide of successful practices in using electronic information, DLM Forum, http://dlmforum.typepad.com/gdlines.pdf
- *Documents'/Records' Management System*:
    - MoReq2 - Model Requirements Specification for the Management of Electronic Records, http://www.moreq2.eu/
    - DoD 5015.02-STD RMA Design Criteria Standard by US Department of Defence, http://jitc.fhu.disa.mil/recmgt/standards.html

6. SYSTEM FUNCTIONAL SPACE

6.1. BASIC FUNCTIONS OF THE CFHRM

According to the Parliament's Decision Nr.57 of 20.03.2008 the basic principles of the CfHRM and the NMPT are the following:

- The assurance of the activity of parliamentary lawyers, oriented towards guaranteeing the observance of the constitutional human rights and freedoms in the Republic of Moldova by the central and local public authorities, by the enterprises, institutions and organizations, regardless of the type of property and legal form of organization, by the public associations and persons with positions of responsibility at all levels;
- The improvement of the legislation in respect of the domain of protection of human rights;
- Legal training of the population.

When fulfilling its tasks, the Centre:

- Examines the intimations of the citizens the rights and freedoms of which were violated, as well as the cases of special social importance;
- Examines periodically the problems regarding the behaviour towards persons deprived of liberty, in the places of their detention, to increase , if necessary, their protection against torture and other cruel, inhuman or degrading treatment and punishments;
- Based on the analysis of the data regarding the violation of the constitutional human rights and freedoms, it prepares and remits to the central and local public authorities general objections and propositions regarding the assurance of the

citizens' constitutional rights and freedoms, the improvement of the activity of the managing administrative apparatus and the amelioration of the behaviour towards persons deprived of liberty, as well as the conditions of their detention;
- Spreads amongst the population informative materials about the human rights;
- Collaborates with means of mass information, with non-profit organizations acting aiming at protecting the human rights in the country and abroad.

It is important to mention that according to art. 232 of the „Law of Parliamentary Lawyers" the CfHRM creates a consulting council aiming to grant consultation and assistance in exercising the parliamentary lawyers' attributions as a National Mechanism for the Prevention of Torture (NMPT), that come to help the parliamentary lawyers in exercising its attributions on the segment referring to the persons deprived on liberty.

6.2. BASIC FUNCTIONS OF THE CFHRM AND NMPT INTRANET SYSTEM

Based on the CfHRM and NMPT functions and tasks laid on the Intranet System that must be elaborated, this must also fulfil, besides the functions determined by the objectives, aims and destination of this Concept, the basic functions of the type informational system, established in the Government's Decision Nr.844 of 26.07.2007" regarding the approval of the Integrated System Concept of Electronic Documents' Circulation", where basic are the following:

- Formation of a data repository necessary for the CfHRM and NMPT activity. These include the functions of data insertion, updating and radiation. These functions are fulfilled within the everyday activity of the employees of the centre and their branches in the territory, as well as during the exchange of information with other external systems.
- Organization of the informational assurance in the data repository;
- Assurance of the authenticity at all stages of collection, storage and presentation;
- Assurance of data protection and their security at all stages of collecting, preserving, processing and using the state informational resources;
- Assuring the competent public authorities and the people with relevant information;
- Assuring the Intranet System's interaction with other external informational systems;
- Assuring the workflows and mechanisms for the control of their fulfilment;
- Assuring a unique medium of information and communication, as well as unique culture of organization.

Besides the basic functions, the Intranet System of the CfHRM and the NMPT will assure the fulfilment of certain auxiliary functions referring to its good performance:
- maintaining, updating and developing the infrastructure
- support and assistance in operating the Intranet System components
- assuring the conformation with the software processing licensing conditions.
- Audit and activities' inspection
- Keeping the history of modifications and activities
- Collecting the statistics and reporting.
- Working in common on the documents' projects including their creation and management
- Strict evidence of the records (finished documents)
- Organizing the individual and group activities and agenda of work
- Assuring the access according to the individual and group permissions.

7. SYSTEM ORGANIZATIONAL STRUCTURE

Basic functions, referring to the maintenance of the exploitation and possession of the Intranet System are attributed to the CfHRM and the NMPT.

The current section makes a presentation of the basic functions connected to the creation, component, functionality, exploitation of the Intranet system that fall under the CfHRM and its subdivisions.

Role	In charge
Owner of the informational resources	**CfHRM** To assure the information integrity, the CfHRM will transfer the reserve copies of the databases and storages to preserve other organizations that have expertise and facilities guaranteeing the preserving of the optimal conditions of data supports.
System holder	**CfHRM**
Intranet System's hosting	**CfHRM** The elements of the Intranet System's informational infrastructure, such as the database servers, application servers as well as their support components are placed in the building of the companies offering specialized support services (Hosting Services). The connection with the Intranet System servers will be made by a broadband internet connection (optical fibre or ADSL connection).
Elevated access rights	**CfHRM's management** The CfHRM's management received from time to time from the Intranet System's Administrator the lists of the persons with elevated access rights and issues decisions regarding the including and excluding of persons form these lists.
System's registrars	**CfHRM's staff** The CfHRM's staff is authorized to register and modify information in the Intranet System.
System users	**CfHRM's staff, NMPT's staff** The Intranet System Administrator, based on the decisions of the persons in charge, assures the users' registration, radiation as well as granting the IS user rights
IS administration, monitoring and maintenance	**A third company specialized in maintenance services** The CfHRM will delegate the functions of the Intranet System's administration, monitoring and maintenance to a third company specialized in offering professional services of support and maintenance.

8. SYSTEM'S DOCUMENTS

8.1. INFORMATIONAL OBJECTS

The informational model of the automated system of the secretariat works must include the following informational objects:

- Electronic document – the information in electronic form, created, structured, processed kept and transmitted via computer, of other electronic kits or technical or program means ;
- Document on paper mount;
- Technological document – registration documents, classifiers, guidebooks, tasks, schemes, schedules, journals, service files etc.). In the Integrated System of Electronic Documents' Circulation (ISEDC), the technological documents may be electronic documents (signed with electronic signature) or may present a totality of system information and/or service-system information (without any digital signature);
- Electronic image of the document on paper mount–fulfilled by optical scanning, detection or collecting of the document's text in a documents' editor;
- Paper copy of the electronic document– the copy printed on paper and authorized in dull legal manner and that contains the remark that it is a copy of an electronic document;
- Classifiers and guides – these constitute the normative-informative information about the System, which is meant for the centralized use by the users, the exploitation staff and the information security staff when executing their functions;
- Cryptographic keys – The cryptographic keys constitute parameters of cryptographic algorithms, meant to protect the integrity and confidentiality of electronic documents, as well as for the signing and checking of the electronic document with the help of digital signature. The cryptographic keys represent a special type of informational objects needing protection against the unsanctioned access or certification.

8.2. INCOMING AND OUTGOING DOCUMENTS

At present, the CfHRM and the NMPT use a series of incoming-outgoing documents that are regulated by the Law of petitions and other internal normative acts regulating the working procedures within the organization.
According to the art.4 of the Law of petitions, the term of petitions means "any application, claim, proposition, intimation, addressed to the resort organs, including the prior application by which an administrative act is contested or the non-solving of an application in the term established by law".
According to the internal instructions regarding the examination of petitions and audiences as primary documents there may be:
- The application for the addressing to the Centre
- A form to submit petitions
- Electronic audience file
- Complete audience file on paper
- The file of recording telephone appeals (green line)
- Electronic file of submitting a petition or appeal to the CfHRM

As system's outgoing documents there may be considered:
- The Centre's decision upon the case
- The answer to the petitions sent to the applicant

- Informative note regarding the case and the legislative sphere to be examined
- A request for the sanctioning of persons with positions of responsibility that committed violations, that generated the considerable breaching of the human rights and freedoms
- Cover letter to remit cases for examination by competence according to the art. 20 clause 1 letter „c" in the Law of parliamentary lawyers
- Letters and appeals to other external organizations;
- Any type of information sent at request to other organizations outside the Intranet system.

The annexes to the primary documents may be considered technological documents, and namely:
- Documents confirming the violation of human rights
- Documents confirming the person's identity
- Experts' notice and conclusions
- The act of conciliation when the case is solved with the agreement of both parties, signed in the presence of the parliamentary lawyer

Internal informational objects:
- Informative notes regarding the results of the work with petitions on different periods of time
- Statistical reports
- Reports of the parliamentary lawyer in the plenum sessions of the Parliament
- The record card (journal) of the transmission of the petition for examination from a subdivision to another within the CfHRM.

8.3. DOCUMENTS' AND RECORDS' LIFECYCLE

The electronic documents' and records' lifecycle is guided by the Law Nr. 264-XV „of the electronic document and digital signature" of 15.07.2004 as well as the international standards of specialty ISO 9001.

According to the standards of specialty an electronic document has the following characteristics, which makes it different from a record:

- It is in a continuous cycle of work, which means that the document can be edited by several users;
- It has a history of versions, it is adapted as a result of the changes coming from outside, it is edited by persons participating in its development and revision;
- The difference between certain versions may be viewed;
- It is published in defined places, known to all user with dull access rights;
- It is authenticated correspondingly.

The record is the final condition of a document attesting a documented activity that has taken place, or which represents a condition in a certain moment of time and that cannot be changed (reports, informative notices, etc), or is a result of the definition of a document's version as „final".

All document and records undergo several conditions in their lifecycle:
- active document– when the document undergoes a range of modifications and editions by the authorized persons;
- record – the moment when the document becomes „final" and now activities of its editing are expected; These documents are accepted as final and authorized, thus becoming records,

- Archived documents – when the documents are no longer used in the everyday activity, these are archived according to the legislation in force.

These stages in a document's lifecycle make a distinction between active documents, records and archived documents. The following sections present the differences while managing the documents during different stages of their lifecycle.

Active Documents

The active documents are those document that are in process of work, such as electronic messages from the account of an employee, a newly-created report or analysis at someone's work position, a document form a library of documents or the company's web pages. The documents will be modified in time, will be copied and distributed throughout the organization in a regular process of work.

The active documents may be declared to be records from the moment when these serve as a proof of an activity or transaction. Some of the active documents will never become records.

At a certain stage in a document's lifecycle this stops to be active. If this document becomes a record, it must be saved and kept for a period of retention.

Records

The records may be documents or other physical or electronic entities within the organization that **serve as proof** of the activities or transactions carried out by the organization. These must be kept for a period of time to be consulted when necessary, for example, for regulating or legal reasons.

When an active document is declared to be a record, this can be moved or copied to a protected locations, such as a physical safe or a repository of electronic records, and a period of retention is assigned to it that specifies the period of keeping the record within the organization.

Archived Documents

These are inactive documents, which are not records (or because these need no period of retention or because these have never been classified as records). The archived documents will pe kept by the company for non-legal reasons such as keeping them for the history.

9. SYSTEM'S INFORMATIONAL SPACE

9.1. REVIEW

The Centre for Human Rights and the National Mechanism for the Prevention of Torture of the Republic of Moldova has been created as an independent public authority, which should assure the guaranteeing of the observance of fundamental human rights and freedoms. In it process of work, the organization interacts with a range of institutions of the public authorities of the Republic of Moldova, international bodies, natural and legal persons. The collecting and synthesis of the information, the registration of CfHRM's appeals, the execution of documents and communication is fulfilled by different means of information exchange, such as direct dialogues, public relations, press handouts, non-formal meetings, briefings, telephone discussions and other verbal and non-verbal means. Nevertheless, the main means of communication is the written one, which may have different forms such as notes, leaflets, strategies, policies, reports, analyses, legislative initiatives etc. This diapason of forms may be

presented on an amount from several written by hand to hundreds of pages of analyses.

Since a big amount of information is involved, it is inevitable to lay this processing power on the informational system, which in our case is the Intranet System of the CfHRM and the NMPT, which will offer support to the staff of all levels so that this can carry out their tasks, including the elaboration and creation of documents of different dimensions, the exchanges, monitoring, capturing and transformation of records, the extended control on the workflows' progress, the assessment and decision-making regarding the current priorities, the tasks management and reporting skills. This whole range of activities may be adjusted by automating the process of documents' management. The generic nature of documents, as well as records allows the incorporation into one system of a wide range of possibilities. Even so, there will be a lot of restrictions since this workflow is generally managed by the staff and it is possible that only a person can assess and fulfil correctly the steps to be done in the process of work.

The CfHRM and NMPT Intranet System Concept will identify a series of documents and records used most frequently to standardize and allow the implementation of automated workflows. Initially a limited number of workflows will be implemented, which cover the critical areas within the Centre's functionality and comes to help its workers in fulfilling the basic tasks and namely receiving appeals from the persons whose rights have been breached. The list of flows will further be filled in with other processes within the organization if the following increase of their efficiency will be managed.

9.2. INFORMATIONAL OBJECTS

The informational objects represent a totality of objects in the System, their attributes, the scripts according to which certain actions are fulfilled.

The informational objects have the following peculiarities:

- uniqueness (the uniqueness of the object consists in the existence of the unique identifier, which differentiates this object from other similar objects);
- condition (the object's condition is described by a set of attributes, describing the object's variable properties, take into consideration in the system);
- conduct (the object's conduct is described by the list of events the object undergoes and that are taken into consideration in the system),
- derivation (the object is *proper* if it is initially taken into consideration and identified in this system, and is *borrowed* if it has been taken together with the identifier from another system).

To assure the uniqueness of an informational object, a system of their codification will be established, which will have as parameters: the issuing body, type of document, version (if applicable), other classification identifiers. The objects borrowed from other informational systems will be registered in the Intranet System, maintaining the original codification of the issuing informational system (as an example of borrowed object there may be the Laws of the Republic of Moldova having their own codification). The borrowed objects that have no proper codification will be granted a separate (provisional) codification.

The Intranet System defines the following main objects:

- Person (inner user, natural person submitting an appeal)
- Institution (Court, Parliament, legal person)
- Basic document (incoming/outgoing/internal)
- Additional document

- Database recording

Person

This is an informational object holding information about the person's identity (last name, first name, year of birth, place of residence, contact details). The unique identifier of the Person is borrowed from the State Population's Register – IDNP.

Institution

The informational object holding information about the institution (name, address, contact details). The object will be registered into the Intranet System as proper object by assigning the corresponding identifier in the system.

Incoming Document

This represents the totality of defined forms to initiate an appeal to the CfHRM by different methods, in written, orally, by email, telephone or other sources. As incoming objects there may also be internal interpellations within the organization to initiate a process of work which will be finished by the production   at different artefacts. The object is proper for the system and the codification will be made depending on the type of appeal and the method of registration.

Additional Document

This represents the totality of auxiliary documents aiming at presenting a more detailed analysis of the case, that lead to certain clarifications, expertises, opinions, statistical data. The objects are identified as proper or borrowed depending on their origin.

Outgoing document

This represents the totality of forms and documents that are fulfilled or drawn up as a result of a final decision-making on several cases, system statistical reports, analyses and informative notes, other documents executed as a result of a process of work. The objects are identified as being proper to the system and the corresponding codification is applies depending on the type of the document and the issuing body.

Database Recording

In comparison with other objects, these are virtual objects attesting the process of electronic recording of the information in a format proper to the electronic system. The object's codification is fulfilled by the database of the Intranet System and will be performed according to the standards of capturing and recording the data.

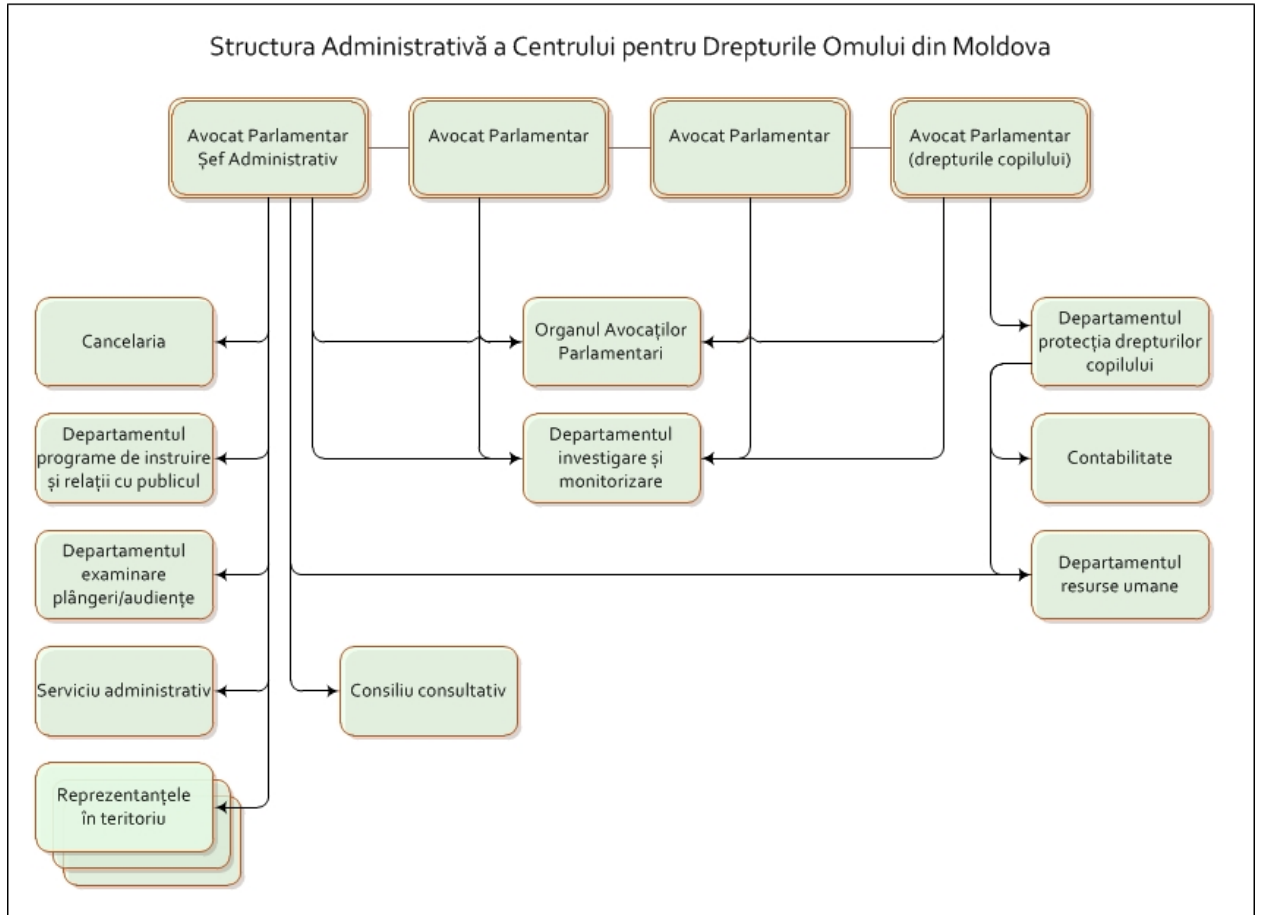## 9.3. ADMINISTRATIVE STRUCTURE OF THE CENTRE FOR HUMAN RIGHTS OF MOLDOVA

Fig 1. Administrative Structure of the Centre for Human Rights

9.4. WORKFLOWS MANAGEMENT

The Intranet system has a as its objective the organization of documents flow within the CfHRM and the NMPT. In this respect it is necessary that this mechanism will contain the whole set of tools necessary for a good performance and which include the facilities of management and definition of workflows and which would allow to the records and documents undergo all stages of elaboration and approval before reaching to the final stage. This module is necessary for the granting of assistance in managing a great amount of documents and to define the set of steps which this document or the set of documents must undergo but also the participants in the process and their role in taking decisions on the workflow documents. The components include a range of functionalities such as the search, editing, distribution of documents but also control mechanisms on the fulfilment of tasks within this flow and alert mechanisms in case of non-observance of the terms of taking decisions regarding the document. All actions are carried out through familiar, intuitive and easy to use interfaces, based on WEB technologies and that do not need the purchase an setting up of an additional program on the users' computer.

At this stage, the basic problem the CfHRM and MNPT is facing consists in the big flow of incoming documents that must be received, classified and further distributed for examination and processing to the corresponding persons. That is why one of the flows that must be implemented are based especially on the critical activities within the Centre and are described in the "Internal instructions regarding the examination

of petitions and hearings of citizens" fulfilled according to the Law of Parliamentary Lawyers, the Regulations of the Centre and the Laws of Petitioning.

It is important to mention that the flow may be launched when entering the documents' system from different sources (fig 2). The starting of the workflow will be made by the staff, which registers and distributes the applications (CfHRM's chancellery). The sources and methods by which the applications reach into the system are diverse, besides their origin-based classification: internal and external, the methods of entry will also be taken into consideration : personal submission, mail, e-mail, web forms, as a result of an audience, the parliamentary lawyer's referring the matter to himself.
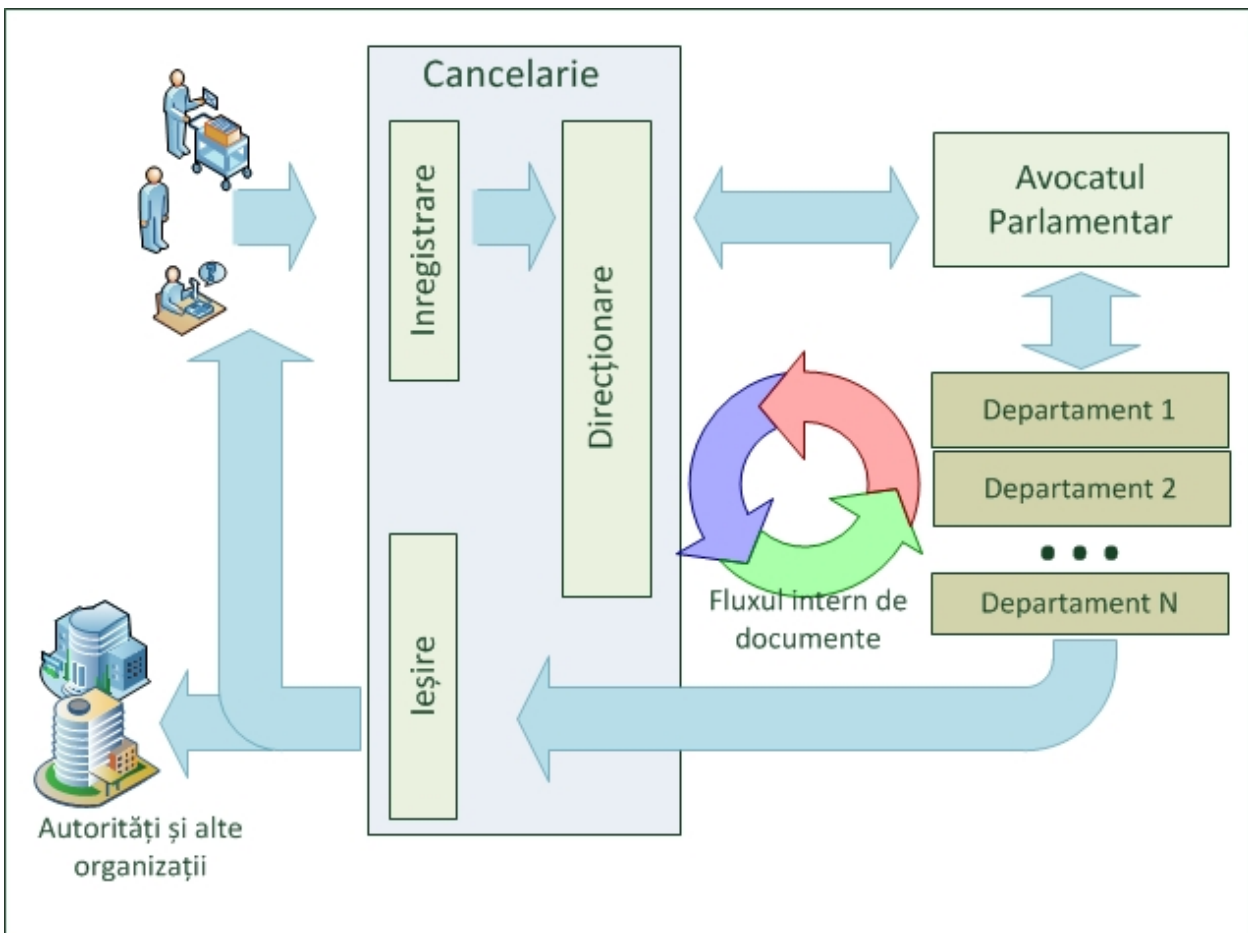

Fig 2. Generic document flows within the CfHRM

It is important that the applications entering the system shall have an increased degree of veracity so that these can be examined and put into work, that is why this sorting and decision can be taken by a competent person and that will start or later stop a workflow, a thing that cannot be granted to informational technologies to be launched automatically when entering the document into the system.

9.5. TASKS AND AGENDA MANAGEMENT

The definition of a workflow imposes the definition of the activities that must be applied on the informational object (document) by different actors in well-defined time spans. The activity allotted to a well-determined actor, which also has a well-defined time of execution, beginning time, is further called task. The tasks may be unitary and

complex. A complex task is a task including several activities. Each activity consumes and further produces artefacts, which serve later as entry to other activities.

Outside the informational systems the tasks are filled in a special table give to the staff, where the progress and use of this person during his/her activity within a defined period of time can be supervised. This type of register for each separate person bears the name of agenda.

The same is within the Intranet System of the CfHRM and the NMPT, where this type of recording must be invested into the informational technologies and it must benefit of their extended possibilities.

The tasks management system will allow:
- Viewing all tasks allotted to certain persons within different time spans;
- Setting the tasks priorities up;
- The existence of a system of automated notification to the changes applied on the task;
- The updating of the tasks' fulfilment status, setting up the degree of visibility on different task parameters visible to other users;
- Grouping the tasks according to the type, to offer sufficient information for reporting. There will exist no restrictions concerning the tasks types, since these will be set up dynamically by the administrator.
- The possibility to plan the events reported to a task. The system will offer viewing the events reported to tasks and will transmit email notifications that refer to the planned events.
- The possibility to annex links to the tasks-associated documents.

The definition of tasks may be fulfilled from the workflows management interface and the tasks management system's own interface.

The tasks' management system must be integrated with packages for the editing of documents and electronic mail systems by which the Intranet System will be integrated.

9.6. INTERACTION WITH EXTERNAL INFORMATIONAL RESOURCES

The Intranet System must have the possibility to interact with other external systems. Under the definition of external system, there may be understood not only the systems of other organizations but also the systems within the CfHRM that are not part of the Intranet System.

As a potential system with which an interaction would be desired there may be considered the "**Automated Informational System "State Population's Register"** which grants access to the data about natural persons, their domicile address and the documents that have been issued to them. According to the Government's Decision Nr.333 of 18.03.2002, for the approval of the Concept of Automated Informational System "State Population's Register" (S.P. R.) and the Regulations regarding the State Population's Register, the information in the S.P.R. will be provided based on contract. The contract will contain the aim for the information request and the method of its use, the data volume and structure, the document's form and language, the type of supports that the data is provided, as well as the method of offering the information (paid or unpaid). The details regarding the method and format of receiving the information will be established further in the development stage.

Another potential system under consideration may be the"**Database of the Ministry of Home Affairs"**, from which the CfHRM, in the person of parliamentary lawyers, who,

according to the law, are entitled to ask for confidential information about the persons involved in the cases under examination, will solicit for and receive information regarding the events/incidents with the participation of citizens. Each addressing to the database of the MHA must be secured, personalized and recorded into the internal electronic register, because strictly confidential information about the person under discussion is requested. Other potential systems with which an integration is desired are the following: the central databank of the Cadastre of Immovable Property of the State Enterprise "Cadastru"; the access to the database of the Department of Penitentiaries .

The possibility of integration with the external systems, conditions and methods of their execution must be analyzed further in the development stage of the Intranet System.

10. SYSTEM'S TECHNOLOGICAL SPACE

10.1. REVIEW

The system's technological space presupposes the definition of methods for the assurance of the system's integrability and support to assure a good performance according to the criteria of similar system's performance and use. The technological space also addresses the problem of information quality and security within the system.

10.2. IS NETWORK AND SERVICES OF THE CFHRM

To assure the accessibility to the Intranet System it is necessary to project an internal network of the CfHRM, which would connect several sub-networks from the Center's branches in the territory. The engine supporting the Intranet System, the database and infrastructure of assuring the communication and protection of the information will be situated in the central office of the CfHRM, or in centres of third companies assuring the system's support and maintenance. The connection with the Centre and its branches in the territory is necessary to be a broadband one that could maintain the indices of performance and accessibility at a high level. From the point of view of assuring a higher degree of security and control on the connections, each of the Centre's branches must have their personal sub-networks, which will be later controlled and monitored by the information's security service.

The access to the Intranet System's services will be fulfilled by an Internet connection and assured by the national providers of such services.

The system must have communication services that assure their good performance and which would integrate into the services of management and functionality of workflows, documents' and records' management, internal communication services based on identifiers defined within the system (personal accounts). The personal accounts must be unique and transparent in different functional modules of the integral system. So, all personal computers of the users will be connected into a domain and the authentication of each person will be fulfilled by this. The assurance of a single point of authentication will allow the integration of different subsystems that need authentication and that will be done in the moment of the user's authentication in one of them. As a whole, the authentication will be done when accessing the operational system by the user and further the domain server will identify the user at each trial to access the information from other systems and will provide information about its status as well as information about the rights of access for this system.
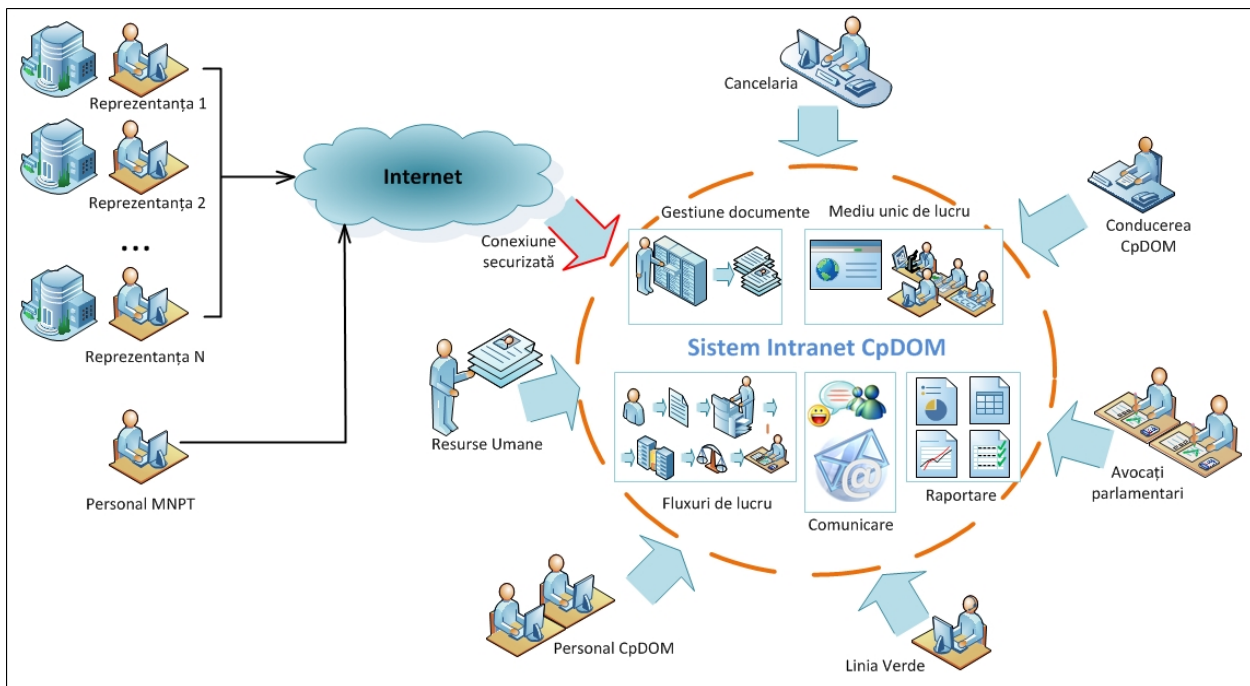
Fig.3 General Structure of the IS of the CfHRM

Electronic Mail

Together with the development of informational technologies, the electronic mail has become one of the main methods of communication, due to the rapidity and later accessibility of this service. The communication and exchange of files is the widest spread aria of email service use. The same thing with the Intranet System of the CfHRM and the NMPT, where a proper system that would offer electronic mail services should be implemented, which would later be integrated with the workflows' management systems to deliver the corresponding information regarding the tasks laid on the user, notifications about events, delivery of files or references to these, which must be examined or approved.

Web Resources

The web resources constitute a totality of information situated in the Internet space and that may be accessed with the help of some utilities of general use, which is available of the users' computers (web-browser, RSS, web-services, etc).

The CfHRM has its own web resource (centre's web page), which is initially not granted with the task to transfer its management within the Intranet System, the integration only being limited to capturing some information coming from the forms of requests towards the Centre on its web page, which will be later received and recorded into the system in the corresponding manner.

Files' Transfer

The transfer of files is a generic term for the act of files' transmission through computerized networks or internet. The CfHRM's staff will be able to transmit files by means of email, instant messages or common workspaces. At the same time, there must exist the possibility download files on the Intranet server, to publish them when necessary or send to the colleagues the file's address.

11. ASSURING THE SYSTEM'S INFORMATIONAL SECURITY

11.1. ASPECTS OF INFORMATIONAL SECURITY

By the notion of system's informational security a series of terms, such as: measures, policies, technologies, points of control, organisational structure, attributions and functions within the system may be reported. It is necessary to identify these means of control to address aspects of informational security and to implement them into the informational system of the CfHRM.

In order to reach an increased level of informational security it is necessary to consider two component parts of the security: the component of physical security and the component of security by applying informational technologies:

- The security by applying informational technologies addresses aspects to protect the information by applying certain measures of security at a logical level, by using the informational technologies. There we may consider antivirus, antispam, sub-networks logical delimitation, firewall and control programs when using piracy programs, recording and updating of software licenses;
- The physical security refers to the protection of the Centre's physical infrastructure and the application of security measures on all physical components within the Centre (access points in the centre's building, access to the computers, printers).

The informational security must conform to the requirements of the legislation of the Republic of Moldova in force and later with the international standards that do not contravene to the law and allow increasing the degree of security. The informational security will be assured by practical measures, and by the elaboration of policies of informational security within the CfHRM.

As aspects of informational security there may be:

- *Data integrity* – the protection of the data against disasters by creating reserve copies, with the possibility to recover it in shorter terms; creating a secure hardware and software, which has an increased stability for failures.
- *Data availability* – assures the rapid and integral access of the users to the data set taht is available according to the policy of rights and permissions.
- *Confidentiality* – assures the access to the data only for the authorized staff.
- *Authenticity* – guarantees the fact that the data have not been modified. Besides authenticity, it is important to assure the non-repudiation of the data, that is the authors will not be able to deny the document's origin.

11.2. AUDIT RECORDINGS

One of the aspects of informational security consists in the detailed control on the actions taking place in the system to detect at an earlier stage some of the trials to access confidential data or prejudice purposely or accidentally the information's integrity. These moments may be identified not only by the existence of a service aiming at monitoring all actions taking place in the system. The set of actions undergoing monitoring may be extended by the system's administrator. All entries about the users' activities in the system, as well as the actions coming from outside the system, may be subject to a detailed analysis in the case of detecting some irregularities or attempts of corruption or unauthorized access to the system data.

12. CONCLUSION

This concept comes to create a general idea about the informational system that will be implemented in the Centre for Human Rights of Moldova and the National Mechanism for the Prevention of Torture. This concept was grounded on a detailed analysis of the legal-normative framework regulating the Centre's activities, the existing informational systems of the CfHRM and the general principles of work, the existing component of infromational infrastructure, the mechanisms of access to information and teh aspects of informational security were also analysed.

The concept identified the arias needing an improvement and traced some directions to go to in order to benefit of the infromational technologies to optimize and make more efficient the process of work within the Centre. The implementation of such a system brings the process of work in the organization at a more qualitative level, but its implementation needs investments in the improvement of the informational culture of all employees. Some of the old methods of work will disappear and other new ones will take their places, some of the everyday staff's activities will undergo changes. The development of certain processes of classification and storage of the information in the system will be necessary, processes that would assure the information's security, these being able to affect the position's files of all employees of the Centre.

The key-decisions presented in the document offer benefits exceeding by far the potential negative involvements. The major benefits changing completely the course of things in the organization are the following:

- Automation of workflows within the organization – The control of tasks' fulfilment refers mostly to the informational technologies, the human factor having the role to monitor its running.
- Use of email services for the management of the mail, agenda, tasks, events.
- Collaboration between the users in the elaboration or examination of a document.
- Information's security
- Digital signature
- Connection of all branches in the territory in a unique system
- System's extensibility with modules and new functionalities, integrability with external systems

All these are things that are absolutely necessary for the increase of the efficiency of an organization and this system comes to bring such benefits.