**GENERAL ASPECTS**

The solution is web-based (front office and back office), accessible and functional at the highest standards of quality of use both on desktop devices and on any type of mobile device (fully mobile responsive), from the following internet browsing solutions: Google Chrome, Microsoft Edge, Mozilla Firefox, Safari. Access to the IT solution is made through URL, not being with access only based on IP addresses. The solution is hosted in one of the certified clouds in Romania.

The IT solution is based on "open source" solutions so that the beneficiary of the system and its users are not dependent on any proprietary technology that could induce hidden costs or additional costs.

The solution allows an integrated management of daily service tasks within the institution and in relation to other public or private entities, citizens or legal entities.

The solution integrates in a unitary way components of:

- Electronic identity management

- Digitized physical registry and automated online registry

- Automated electronic archive and back-digitized physical archive

- Management of workflows with documents / documents

- Qualified electronic signature in the browser

- Digital governance of signature rights across the institution

- Cloud-qualified electronic sealing, integration with trusted authorized service providers

- Email / Electronic Messaging and Chat integrated with the certified electronic identity component

- Notifications (system and push in the mobile app)

- Electronic forms both for the use of external users (natural and legal person citizens) and for the internal use of officials.

- External communication - Interconnectivity with an unlimited number of central and local public administration institutions, deconcentrated or of any other type as long as there is a form of legal constitution

- Integrations with institutional data providers ANAF, RECOM (directly or through existing service providers in the market), etc.

- Integration with the EU trusted list with trust service providers at European level

Browser-to-server communications are encrypted using cryptographic protocols (HTTPS) designed to ensure the security of internet communications (SSL/TLS).

The graphical interface of the solution complies with good practices in web design:

-Intuitive

- predictable

-Minimalist

- Charges quickly

- clearly present the work options

- easily communicates with the user

- Use custom styles based on user actions

-Attractive

-Customizable

- Handles errors in a friendly way

- uses terminology specific to each type of user

- presents an optimal number of choices that the user can make

- provides contextual explanations of functionalities

- has relevant validations for the forms to be filled in

It must be taken into account that the graphical interface must satisfy all types of users, regardless of their level of understanding, their digital skills and their degree of resistance to change, and the computer system complies with these requirements, having the following characteristics:

*Intuitiveness*

o The design elements are found on the page following an elementary and easy-to-use logic (titles, subtitles, menus, options, etc.) – the interface for officials follows the administrative logic, terminology and work tools specific to the public administration environment

o Button names are relevant and comply with industry-standard designs

o The existence of the Help button where it is real needs further explanation.

*Predictability*

o Graphic elements (buttons, icons, menus, checkboxes, radio buttons, etc.) behave according to industry standards – the user experience standards existing globally

*Caracter minimalist*

o Each window of the proposed solution contains the bare necessities of elements without generating a sense of visual burden for the user

*Clear functionality options*

o The options that the user has (droplist, menus, sub-menus) are clear, contextual and do not present residual information (which the user does not need in the context in which he is)

*Easy communication with the user*

o The Solution has a system of "real time" notifications that accompany the operations that are in progress or that have been carried out, e.g. the message is being sent, the message has been sent, the documents have been signed, the documents have been archived, an error has occurred, etc

o Communication is mainly done through images and icons – text should be avoided as much as possible

*Custom styling*

o Action buttons have standardized formatting (shape, color, size, etc.)

o Elements and symmetry of text inputs impose a sense of order and clarity when navigating the page

*Attractive character*

o Given the very wide range of audience followed, color shades are generalist

*Customization*

o Interface benefits from customization elements such as first name, first name, profile picture, etc.

*Handling navigation errors*

o allows the user to return to the previous page – the "back" function

o Accidental exit from the page is prevented by warning messages

*Terminology*

o Terminology for user interfaces for individuals and legal entities allows the user to easily understand the meaning of words and describe the functionalities – explanatory tool-types.

*Optimizing User Choices*

o The choice options (droplist, menus, submenus, etc.) made available to the user are contextually filtered according to the type of identity (natural or legal person), institution, professional identity, role held at the level of the institution, compartment, so that the number of options reflects the specifics of the activity and the particular context in which the user finds himself.

*Contextual explanations:*

o Existence of explanatory tool-types and their structure

o Contextual Help buttons to help the user understand the functionality used

*Input validations*

o At the level of all interfaces and web forms used for user interaction with the IT solution, there are content validations designed to ensure the correct and complete collection of data.

The IT solution has a single registration and authentication page for all types of users (individuals, legal entities, officials), justified by the need to ensure a single access gate for all users regardless of their type.

Authentication in the IT solution is secured using an additional layer of 2FA (2 factor authentication) security, ensuring not only the user's authentication, but also his certified identification (eID).

The homepage of the system includes the functionalities of:

- Identity validation

- Password validation

- Password Privacy

- Password view

- Username recovery

- Password recovery

- Validate 2FA

- Revalidate 2FA

The solution presents custom error notification messages for each error that the user can generate in the authentication process.

The homepage of the solution allows the initiation of the onboarding process (registration of individual and legal entity users) and transparently presents to potential users:

- Personal data processing agreement

- Terms and Conditions of use of the IT solution

- Privacy Policy.

**ELECTRONIC IDENTITY MANAGEMENT**

The IT solution includes a rigorous and auditable process for the management of electronic identities (individuals, legal entities, officials). To avoid any confusion, the term auditable means the ability of the IT solution to create and store in an aggregated manner (on a "root of trust" model) accurate records for each step described in the process of creating the electronic identity, records that cannot be deleted by any user. The electronic identities residing in the IT solution are created through the physical presence at the institution's counters of the applicant or directly through the online environment and are unique and interdependent. The identities of natural and legal persons can be created by all officials, while the identities of officials can only be created by system administrators.

The operations of creating/modifying identities are done on a transactional basis and will have fallback procedures for the cases in which they occur. The IT solution has protection mechanisms for simultaneous editing of recordings. The audit mechanisms shall comprise at least the following elements:

- Accurate and complete collection of identity attributes – all input validations must be accurate, pre-existing and comply with industry standards

- Capturing and saving your personal data processing consent

- Registration application signed by handwriting registered in the Electronic Registry of the institution (for cases of identification at the counter)

- Video identification (when online identification) saved in the cloud and associated with the work that established the auditable procedural framework for online identification – the video file will be associated with the identity of the person concerned

- The level of trust given to the identity

- Qualified electronic signature of the official

- Electronic seal of the institution

The electronic identity is to be previously verified/validated and subsequently initiated by the public official who made the identification (either at the counter or online). Electronic identities (personal or professional) are defined by attributes specific to each type of identity and are aggregated under a unique identifier (ID) that will include the identity created in its evolutionary form (including all changes made throughout its existence). All verified and validated attributes that were the basis of an electronic identity (regardless of whether personal or professional, natural or legal person) are personally assumed by the official who has validated the attributes by their qualified electronic signature, thus acquiring irrefutable character. Identities, including personal ones, will be able to have one or more roles associated with the IT solution governed by specific digital governance models. To avoid any doubt, the digital governance model is understood as a set of rules/procedures that define identity/role. These sets of rules/procedures must cover at least:

- The people responsible for configuring the respective identity/role

- The specific operations that the identity/role can do

- Legal consequences generated

Each identity (personal or professional) has a distinct set of credentials that uniquely identify a single identity. Roles associated with an identity, whether personal or professional, are accessed and used based on the credentials of that identity. Identities belonging to a single person are integrated via SSO (Single Sign On), who can switch between identities without any additional authentication. Professional electronic identities (those of legal persons and officials) cannot exist in the absence of the personal electronic identity that is of the "Master" type at the level of the IT solution. Deactivating/Deleting the Master (personal) identity also generates the deactivation/deletion of all other professional identities. A person can hold only one personal electronic identity and an unlimited number of professional electronic identities.

The management of the virtual space of legal entities is carried out collaboratively by the administrator of the legal entity / his/her proxy and officials, each of whom has the following responsibilities:

*Responsibilities of the official:*

- Verification of the correctness and integrity of the data about the legal entity

- Verification of the correctness and integrity of the data about the legal representative of the legal entity

- Activation of the professional identity of the legal representative of the legal entity

- Activation of the identity of the legal entity

The identity of the legal entity will not be able to exist in the absence of a legal representative (directly or through a proxy) with an electronic identity of a substantial/high level of trust at the level of the IT solution.

*Responsibilities of the legal representative of the legal entity / its representative:*

- Initiating / Activating / Deleting / Deactivating / Suspending the professional identities of other employees

- Establishing the public services to which they have access

- Maintaining data about the legal entity at a level of accuracy that reflects the current state of affairs

Each effective identity (personal or professional) has a unique set of credentials. The credentials will constitute an irrefutable proof of identification and based on them, the user will be granted access to the system. The roles associated with an identity, whether personal or professional, will be accessible and used based on the credentials of the identity to which they are associated, the user being able to navigate between them without additional authentications.

Each electronic identity is confirmed by the holder on an external channel (email, SMS, etc.) to the IT solution and it will become fully operational after the moment of confirmation. The external channel used must be outside the physical and logical control of the contracting authority.

In relation to the degree of operationalization of identities, they can be:

-Effective

- Non-effective

- Preliminary indicia of identity certified by officials

*EFFECTIVE identity* - Electronic identity, regardless of its type, in order to be effective, must cumulatively meet 4 conditions:

- Be identified by a unique identifier

- Possess the full set of attributes specific to their identity type

- To be consciously assumed by its holder -

- To be actively exercised in the virtual space

*NON-EFFECTIVE IDENTITY* - All identities that must include CNP or CUI/CIF, but which do not cumulatively meet the conditions of effective electronic identity will be considered non-effective. Until the moment of its confirmation by the holder, the electronic identity will be ineffective. Non-effective identities will be able to become effective only after they are complete, explicitly assumed and exercised at the level of the IT solution.

*Identity clues* – Data regarding an applicant (e.g. email address, phone number, etc.) that have not associated a CNP/CI/CIF and that are stored at the level of the IT solution are considered preliminary clues in establishing a future identity. The preliminary indications of identity will be assumed by the official who entered them into the system and subject to audit. The IT solution has the ability to capture, save and partially operationalize preliminary identity clues. They generate limited legal consequences depending on the context in which they are used. Whether the electronic identity is effective, non-effective or only in the form of preliminary identity clues, the IT solution is able to implement contextual digital governance models for them.

The identities (including the supporting documentation) can be exported if necessary to other systems, thus ensuring the full independence of the beneficiary in the relationship with the institution.

Identity management is carried out at the platform level so that full compliance with the provisions of the European GDPR and eIDAS regulations is ensured.

The IT solution has the ability to store and operationalize through specific digital governance models electronic identities in the following logical states:

 For individuals and legal entities in at least the following states:

- Period of inactivity

- The period between the moment of initialization and the moment of confirmation of the electronic identity

- Period of activity

- Suspension period – e.g. suspicions of fraud, secondment, temporary unavailability, etc.

- The period after deactivation

 For officials:

- Period of inactivity

- The period between the moment of initialization and the moment of confirmation of the electronic identity

- Period of activity

- Period of leave

- Suspension period

- The period after deactivation

The information regarding the user's electronic identity is available and accessible to each user in a "My account" section.

From the perspective of the individual user, the graphical interface displays at least:

- Personal data of the holder of the personal electronic identity

- Profile picture

- Updated identity documents of the holder

- Data on the official who created the electronic identity

- The user's handwritten signature

- Qualified electronic signature of the identity holder accompanied by all its details (supplier, validity period, etc.)

- Changing the password to access the system

From the perspective of the legal entity user, the graphical interface displays at least:

- Personal data of the holder of the professional electronic identity

- Data specific to professional identity

- Profile picture

- The user's handwritten signature

- Qualified electronic signature of the identity holder

- Changing the password to access the system

From the perspective of the operating user, the graphical interface displays at least:

- Personal data of the holder of the professional electronic identity

- Data specific to professional identity

- Profile picture

- The user's handwritten signature

- Qualified electronic signature of the identity holder

- Changing the password to access the system

The requirements regarding the graphical interface apply accordingly. Electronic identity attributes that are not considered to have a high degree of sensitivity (such as documents and personal data), respectively those that in everyday life are within the reach of the user and can be modified/edited/updated without explicit validation by the officials (email, phone number, profile picture, handwritten signature). For the rest of the information, validation by the official is required and, where possible, its qualified electronic signature by the holder of the electronic identity.

Information on all users, natural persons, legal persons, or officials shall be available and accessible to all officials on a need-to-know basis. The information will be accessible only individually and subject to the existence of a valid reason. The reason for access will be captured in the system to ensure compliance with GDPR provisions. For the avoidance of doubt, the solution offered will not allow any type of user to view all personal identities in the system in the form of a list and without a valid reason captured at the time of access.

Officials have tools for managing user data, such as:

- initiating the process of resetting the access password

- viewing the history/previous versions of the user's personal data.

- editing users' personal data.

**ELECTRONIC REGISTRY**

TYPES OF REGISTRY OFFICE

Taking into account the specific needs of the public administration, the information system ensures, in a standardized and integrated manner, the following components specific to the registry activity:

- Digitized physical registry activity – respectively the entry of requests and the exit of correspondence through the institution's counters

- Automated online registry activity – entries and exits made directly through the virtual environment

In order to remove any doubt about the meaning of the terms used, we mention that the terminological meaning of the two types of registries is as follows:

*Digitized physical registry* – the capabilities offered by the IT solution to take over the documents received on paper and to introduce them on the digitized workflows

*Automated online registry* – the capabilities offered by the IT solution to take over the documents received on the online channel and to enter them on the preconfigured or configurable workflows.

The IT solution complies with the following fundamental working principles:

The institution's registry is organized taking into account the material competence of this institutional function, namely:

(1) Reception and distribution of documents entered into the institution

(2) sending documents to entities external to the institution

(3) the circulation of documents for internal use.

The registry will be structured taking into account the classic administrative relational tools, namely [PAPER - ACT - FILE]

Thus:

- an ACT will be able to be part of one or more electronic works/files at the same time, the differentiation being made contextually based on the unique registration number received at each association – an act will not be able to exist on its own, but only in the structure of a work

- a PAPER will include one or more documents related to the same request as well as all the contextual elements that define the respective work, namely communications, participants (each with its own role, connections, references, etc.)

- a DOSSIER will always include several associated works around a common topic.

**CONCEPTUAL CONSIDERATIONS ABOUT ELECTRONIC DOCUMENTS**

In order to ensure a correct understanding of the terms, an electronic document is understood to be an electronic document that has at least the following characteristics:

- Has an author (with a certain identity or not)

- Has content that reflects something that has been said, done, or agreed upon

- It is signed and assumed in the name of a person or another person

- Has or has not been subject to a registration process (has a registration number)

- It has been created in an electronic system or represents a qualified electronically signed copy of a paper document.

Electronic documents can be issued by individuals, legal entities or institutions. Acts issued by natural persons and legal persons (other than institutions) in order to be relevant in an institutional context must be subject to a registration/registration process.

Documents issued by institutions can constitute electronic documents only to the extent that they meet the following conditions:

- Presents clear clues of the author of the document

- Bears the visual identity of the issuing institution

- Has gone through a process of signing, endorsement and approval formally agreed at the level of the issuing institution

- Has been registered with a unique registration number in the records of the issuing institution

**SPECIFIC CONSIDERATIONS REGARDING ELECTRONIC DOCUMENTS**

The IT solution provides the following capabilities regarding the electronic documents / acts that will be managed at the level of the institution:

- ensures the upload of files in the system individually or in batches, both through upload buttons, as well as through "drag and drop" and "copy-paste" operations – the upload can be done from the electronic archive of the system to which it has access and/or from the computer

- ensures the deletion of electronic files from the system except for those that have been electronically archived whose deletion is not allowed.

- ensures the conversion (automatically and manually) into PDF format of files from sources external to the system uploaded to the system and those redacted in the system (the following electronic file formats jpg, jpeg, bmp, png, doc, docx). Conversion to PDF format can be done both individually and in batches.

- has an integrated electronic procedure for compliance with the original by means of the electronic signature qualified by the official. Compliance with the original by qualified electronic signature can be done both individually and in batches.

- ensures the versioning of electronic documents in the process of becoming documents (on the approval, approval, registration flows)

- ensures the easy collection of all relevant metadata according to the context in which the user is located (personal, institutional archive)

- allows the renaming of electronic files without the need to download them from the system

- allows a rigorous record of the main acts and their annexes – the "main act-annex" relationship being stored at the system level

- ensures the visualization of electronic documents / acts in the system without the need to download them

- allows electronic signature both by sending the electronic document/act on an electronic and static flow.

- Qualified electronic signature can be done both individually and in batches.

- allows the user to place the qualified electronic signature so that it does not overlap with the text. If the document uploaded to the system has a rotation factor, the placement of the electronic signature takes this element into account.

- has legal electronic archiving facilities, as well as storage facilities

- has file size control policies in place

- it has capabilities to separate the pages of a document and save them as different documents, to order / reorder pages within the same document, to concatenate several files

- has the status of trust service provider according to the eIDAS regulation for the validation of qualified electronic signatures and qualified electronic seals in a document / document and certifies the validity of electronic signatures and seals in a document

- ensures that electronic documents will be unique at the system level

- ensures the ability to make electronic references to electronic documents to an unlimited number of electronic files.

- electronic documents can be saved by groups specific to the activity of each structure in the organizational chart

- allows the configuration of access rights at group and document level,

- provides capabilities to configure access rights to groups for both writing and reading. The configuration can be done individually or as a predefined group of users in the system.

- electronic documents can be moved between archival groups associated with the same register. Moving to groups associated with a register other than the one in which it was registered is prohibited.

- in their relation to electronic files, electronic documents may be subject to the following operations:

Save to folder

Delete from folder

Move to another folder

Create Reference in Another Folder

File Comparison

- allows the grouping of acts into groups that can be subject to the following types of operations:

Create and edit the group

Delete the group

Establishment of access rights to groups

Association of specific process types

**CONCEPTUAL CONSIDERATIONS REGARDING ELECTRONIC WORKS**

The IT solution treats the Works as logical structures characterized by at least the following attributes:

- Type of work

- Registration number of the work (for registered ones)

- Name of the work

- Date and time of creation

- Date and time of registration

- Completion date

- Method of completion

- Chronology of the work - the sequence of actions and events recorded in the content of the temporally marked work

- Data about the participants in the work, the roles they have in the work and their status

- The content of the paper – it can include messages, ideas, suggestions, arguments, points of view, etc.

- Documents/Papers of the work

- Information about possible connections

- Work governance – the particular set of rules and actions that govern the work according to its type

- The status of the work (e.g. statuses – not exhaustive – not registered, in progress, completed, etc.)

- Any other event or object recorded at the level of the work and that can contribute to creating the context for the creation and development of the work (e.g. reading reports, notifications, announcements, message counter, duration, etc.)

**SPECIFIC CONSIDERATIONS REGARDING ELECTRONIC WORKS**

The IT solution provides the following capabilities regarding the electronic works that will be managed at the level of the institution:

- has a section for the record of the works in which the official participates

- allows viewing all the works in which the user participates in a list / table format

- allows filtering/sorting/searching of works according to the attributes mentioned in the section "Conceptual considerations about works"

- allows the user to create/edit/sign/configure and dispatch jobs on workflows based on their type

- allows multiple job signing and automated sending on pre-established workflows – job packages (with all files attached)

- The shipment is made as a transaction and has fallback procedures implemented in case errors occur in the processing and shipping process. The solution allows automatic sending of electronic jobs to recipients in batches (tens, hundreds, thousands, tens of thousands, hundreds of thousands of jobs at once)

– the consignment transits the qualified electronic sealing operation and allows the recipients to return with a response to the institution.

- Shipping can be done both inside and outside the system.

- The system provides shipment progress reports and, if errors have occurred in the shipment process, they are captured to allow officials to analyze them.

- has a section of Drafts intended for saving works that are in the process of being edited and for various reasons could not be finalized and shipped. The user is allowed to resume editing from where they left off.

- has a section for archiving completed works

- allows a view of the detailed history of each work in which the user has participated

- has a job counter that updates according to the filters applied in the job list

- has defined at the system level a Procedure for Handing Over - Receiving the works

- the section for the record of the works is integrated with the Electronic Registry of the institution, the Electronic Archive of the institution, the Qualified Electronic Signature and Sealing Component

- allows uploading files from the computer and from the electronic archives available to the user

- integrates the electronic archival nomenclature to allow the user to save files on groups and electronic folders

- has in the process of editing a paper all the capabilities of the system presented in the electronic documents

- has online file/text message editors that include standardized text formatting elements at the level of web platforms

- is integrated with the identity management component so that it can easily import the information/attributes provided by it: e.g. Professional electronic identities, the specific status at the time of writing the work of the other participants (active, on leave, suspended, etc.)

- has a process nomenclature with predefined governance that allows filtering on the user's page only those types of processes that comply with their duties

- implements in the activity of the officials the concept of "account manager" – sole holder for solving the work.

- allows the configuration of the work through operations such as creating the content of the work, establishing the roles and responsibilities of each participant, modeling/reshaping the signing flow of the work documents, etc

- implements automation capabilities for the execution of the course of the works – once the work is configured, the execution of the operations follows one another without an explicit intervention of the user

**CONCEPTUAL CONSIDERATIONS REGARDING ELECTRONIC FILES**

In order to ensure an accurate understanding of the needs of the institutions, we mention that 2 types of files have been identified at the level of the institution:

* Electronic work files – this type of file brings together several works around a common topic – they arise as a result of joining several works
* Electronic document files – this type of file aggregates in the same place the documents that concern a specific process in the institution's activity (e.g. personnel files, public procurement files, project files, etc.)

**SPECIFIC CONSIDERATIONS REGARDING ELECTRONIC WORK FILES**

The IT solution provides a procedure for configuring the digital governance of the electronic work file that includes information on the following aspects:

* Creating and Deleting the Folder
* Edit folder attributes
* Add and delete electronic works in the folder
* Establishing the rights of access to the electronic work file

**SPECIFIC CONSIDERATIONS REGARDING ELECTRONIC DOCUMENT FILES**

The IT solution provides the following capabilities regarding the electronic document files that will be managed at the level of the institution:

* has a mechanism for creating/editing electronic document files to establish which officials and under what conditions will be able to use the functionality
* Enables a "tree" architecture with folders and subfolders where subordination relationships between folders at the solution level can be modified

**REGISTER OF WORKS AND REGISTERS OF DEEDS**

The IT solution allows the creation and configuration of the institution's registers. It also allows the possibility for several structures in the institution with similar competences to use the same register.

The institution's registry allows a centralized record at the level of the Single Register so that all the works carried out in the current activity can be found in a single interface.

The institution's registry includes a single register of works at the level of the institution, called the Single Register, and an unlimited number of registers of documents intended for each structure in the institution's organizational chart (service, office, compartment, etc.). The Single Register provides unique registration numbers for the works, while the Registers of Deeds will provide unique registration numbers for the documents. The Single Register includes both entry and exit works as well as internal works. The registers are integrated with the Current Electronic Archive (not the back-digitized one).

The registry allows for multiannual management of registers, automatic generation of registers at the beginning of the year, automatic archiving of registers from the year ended and linking registers from successive years. The operation is commonly referred to as "year-end automation".

**REGISTRATION OF WORKS AND DOCUMENTS - TERMS AND CONDITIONS**

The registration number represents the particular context in which the work/act originated (at the internal and output works) or was taken into account by the institution (at the entrance works). For this reason, the way of assigning numbers must be rigorously controlled and reflect reality exactly. The granting of registration numbers must take into account the following essential terms and conditions in order to have a legal, fair and transparent record of the electronic works and documents in the institution:

* The registration numbers given to the works are automatically granted by the system respecting the chronological order of the creation of the works. The solution allows the granting of registration numbers manually under the procedural conditions agreed at the level of the institution.
* The granting of registration numbers is done incrementally (one after the other).
* For entry works, registration numbers are granted at the time of their registration, i.e. at the time of entry
* For internal and outgoing works, the registration numbers are granted when the work has gone through the approval and approval flow, respectively it has been signed electronically qualified by all signatories and electronically sealed with the electronic seal of the institution
* The granting of registration numbers is secure, auditable
* The IT solution can assign numbers to jobs both in individual format and in large series of jobs called "batches" (tens of thousands of jobs consecutively).
* The registration numbers granted to works and documents are unique
* The registration numbers are inserted into the document structure in PDF format together with all the metadata of the author, signatories and institution.
* Registration numbers are visible both on the document and in the document signature panel along with all other metadata.
* The IT solution allows the official to determine the location of the registration number within the document if necessary – the place where it will be visible on the document being important in order to avoid overlapping the registration number over the content of the document.
* The solution allows the registration number to be printed if necessary for the works received and recorded at the counter.
* The IT solution allows the registration numbers granted to the work and all the documents it includes to be cancelled in cases agreed at institutional level (e.g. the filing of a paper).
* The IT solution does not allow the deletion of registration numbers.

**CONSIDERATIONS REGARDING THE DIGITIZED PHYSICAL REGISTRY**

Digitized physical registry:

* allows the reception of requests from other entities, whether natural or legal persons, with the collection of all relevant metadata for the respective work.
* It allows the retrieval of requests in email/electronic messaging format or on standard forms. All the standard forms existing and used within the institution will be available for the reception of requests by the registry officials.
* ensures the reception of requests in all 3 identity hypotheses in which the applicant may be:
	+ Applicant with effective identity
	+ Applicant with non-effective identity
	+ Applicant who presents only preliminary indications of identity (e.g. petitions sent by email)
* allows the distribution of the works on the resolution flows and subsequently to the persons responsible for solving them, fully capturing the entire institutional flow of the work
* has a section of Drafts intended for saving works that are in the process of being edited and for various reasons could not be sent
* allows the communication of exit documents when the holder of the request / his representative presents himself at the counter. In the case of communication to processors, the system must condition the communication to the loading of the power of attorney into the system
* allows searching for the works and viewing their content in the Single Register at the request of the beneficiary (natural person, legal entity or official), accessing them in compliance with the conditions imposed by the GDPR, printing and sending the documents from the work to the citizen presented at the counter.
* allows viewing all assigned requests and filtering by the following criteria:
	+ Applicant Name
	+ Job Number
	+ Recipient Name
	+ Subject
	+ Content
	+ CNP / CUI
	+ Date of receipt
	+ Date of Registration
* The search can be done through simple filters or conjugate filters so that the search time is limited to the maximum.
* Archiving assigned work after it has been completed. The archiving of works can be individual (job by job) or in "batch" (several works archived by a single operation).

**AUTOMATED ONLINE REGISTRY CONSIDERATIONS**

Automated online registry:

* allows the automated receipt (both in ticket format and on standard forms) online of requests from other entities, whether individuals or legal entities, with the collection of all relevant metadata for the respective work. The automated distribution of the works received through the online environment is configurable according to the following criteria:
	+ Workload of the official
	+ hierarchical criterion (automatic assignment to the head of structure)
	+ territorial jurisdiction of the official
	+ Substantive competence of the official
* Allows you to view your request history in order to avoid duplicating identical requests
* Allows viewing all requests that have been assigned to an official for processing, with the option to filter by the following criteria:
	+ Applicant Name
	+ Job Number
	+ Subject
	+ Content
	+ CNP / CUI
	+ Date of receipt
	+ Date of Registration
	+ Status of the work

The system allows:

* The possibility of assigning a work either to another official within the institution or to another institution, where appropriate. The distribution must be able to be individual (job by job) or batch (several jobs sent by a single operation to the responsible official.
* Organising consultations with other officials to respond to citizens' requests
* Joining several works in a file – joining must be possible both with a work already existing in the institution, and with a work that is to be born in the institution (e.g. a new work is connected to the existing work that is about to be born)
* Online communication with applicants to request further details on the submitted application
* Finalization / resolution of the requests received through one of the methods of completion available in the system. Completion can be individual (job-by-job) or "batch" (multiple jobs completed through a single operation).
* Archiving of completed works. The archiving of the works must be individual (job by job) or in "batch" (several works archived by a single operation).

**ELECTRONIC ARCHIVE**

**CONCEPTUAL CONSIDERATIONS REGARDING THE ELECTRONIC ARCHIVE**

The IT solution makes available to each type of user (natural person, legal person or official:

* an electronic archive of documents / documents – intended to allow the user quick access directly from the cloud to all his documents (both personal documents and documents issued by an institution)
* an electronic archive of works – intended for archiving requests sent to the institution and which have already been completed.

SPECIFIC CONSIDERATIONS REGARDING THE ELECTRONIC ARCHIVE OF NATURAL AND LEGAL PERSONS

The IT solution has the following technical capabilities:

* It is integrated with the electronic identity management component and allows access to documents according to the level of trust (low / substantial or high)
* It is integrated with the electronic forms component and with the email solution of the system so that the user can upload documents individually or in batches directly from his electronic archive
* allows authorized users to view, download and print documents/documents
* allows viewing all metadata stored at the system level for each document / act
* It has filtering, sorting, and searching capabilities based on relevant metadata (e.g., file name, registration number, date, etc.)
* allows the user to delete personal documents/documents from the archive
* It does not allow the user to delete the documents sent to him by the institutions
* allows the user to view the work of which the document issued and transmitted to him by the institution was part
* has mechanisms for the native and implicit collection (without the user making an additional effort in this regard) of metadata through controlled, validated and parameterized inputs in order to ensure a higher level of accuracy of this information
* has a policy for the management of documents uploaded to the system at least from the perspective of:
	+ Supported file formats
	+ File naming parameters
	+ File size
	+ Document scanning
	+ File access (for legal entities that have more than one representative, the solution establishes the access rights of each one to the files)

**SPECIFIC CONSIDERATIONS REGARDING THE INSTITUTION'S ARCHIVE OF ELECTRONIC DOCUMENTS**

The IT solution has institutional electronic archiving capabilities that meet the following conditions:

* The cloud provider is certified by the relevant ministry/authorities for electronic archiving services
* Allows the creation of the electronic archival nomenclature (according to the legal provisions) and the management of the institutional electronic archive
* It is integrated into all relevant means of communication (which produce legal consequences) at the level of the IT solution
* It is integrated with the identity management component to collect the user's identity documents directly from the onboarding procedure
* It has explicit auditable mechanisms (logs) regarding any change, access or operation that has an impact on the electronic archive
* It is syncrized with the institution's registers to ensure good traceability and transparency in the management of documents
* Saves all relevant metadata of documents in their PDF structure
* It can export at the request of the beneficiary, in a structured format and at no cost to the beneficiary, all the documents existing in the system and the data collected as a legal obligation of the institution. The data that exists in the system in order to personalize the user experience is not subject to this obligation.
* Upon request, at no additional cost, an exact mechanism for extracting metadata from exported files can be requested.

**CONTEXTUAL MODELING OF ELECTRONIC WORKFLOWS**

The IT solution has flow modeling capabilities with the following functional requirements:

* Modelling is available to all officials
* Once modeled, the flow is executed automatically, without the intervention of the official
* A rollback mechanism is implemented that can be called motivated by any of the participants in the flow
* Flow modeling includes the following features:
	+ Name of the created flow
	+ Structured content creation capabilities (text, inputs, validations, etc.)
	+ Process to which it relates (substantive jurisdiction)
	+ Originator data
	+ Signatory data
	+ Recipient data
	+ Monitoring flow execution
	+ Possible specific conditions determined by institutional governance (e.g. territorial competence)
* Conditions regarding qualified electronic signature and qualified electronic sealing of documents, such as: designation of signatories, establishment of the order of signing, establishment of the reason for signing for each signatory, positioning of signatures, positioning of the seal, versioning of documents in the signing process, cancellation of signature, revision of signature.

**QUALIFIED ELECTRONIC SIGNATURE**

The IT solution can use without any restriction qualified certificates issued in accordance with the provisions of the eIDAS regulation by any authorized provider on the territory of Europe. The documents uploaded to the system can be electronically signed with any type of accredited cryptographic instrument (electronic signature with qualified certificate stored on the token or electronic signature with qualified certificate stored in the cloud at one of the authorized providers at European level).

Qualified certificates with cryptographic keys stored in the cloud can be synchronized with the system, offering the possibility of rigorous management of it: e.g. import, deletion, certificate details view, etc.

The IT solution has integration with 3 trusted service providers authorized for this purpose at European level.

From the perspective of qualified electronic signature, the system has the following functional requirements:

* allows the synchronization/desynchronization of the qualified electronic signature certificate with the system
* allows the integration of the handwritten signature into the qualified electronic signature
* has the Integration of the qualified electronic signature on all communication flows implemented at the system level
* allows simple signing (1 document) and batch signing (multiple documents) to all users in the system
* allows contextual management of signing reasons
* allows signing within or independent of the existence of a signature flow
* allows the verification and validation of qualified electronic signatures applied on documents / acts, respectively:
	+ Validate the signature type
	+ Certificate chain of trust verification
	+ Date and time of signing
	+ Identity of the signer
	+ Whether or not the document has been modified after signing
	+ Data on the validity of the qualified certificate
	+ Issuer of the certificate
	+ Reason for signing
* allows the positioning of the qualified electronic signature visible on the document at the user's free choice – if the supporting document will have a rotation factor inserted, the application will take it into account.
* allows operations such as unsigning, re-signing, re-signing,
* allows viewing the list of signing requests and managing signing requests/invitations
* allows multiple signatures (several Papers at once) with the possibility of selecting the papers that will be the subject of signature
* allows you to preview the documents to be signed without the need to download them
* allows simultaneous qualified electronic signing of multiple documents and queue signing

**QUALIFIED ELECTRONIC SEALING**

The IT solution can use without any restriction qualified electronic seals hosted in the cloud issued in accordance with the provisions of the eIDAS regulation by any authorized provider on the territory of Europe. The access of the IT solution to the electronic seal hosted in the cloud is made secure and auditable.

The IT solution has integration with 2 trusted service providers authorized for this purpose at European level.

From the perspective of qualified electronic sealing, the system has the following functional requirements:

* allows qualified electronic sealing in both automatic and applied

Manual

* allows simultaneous qualified electronic sealing of multiple documents and queue sealing
* allows the management of multiple sealing queues to ensure increased application speed when the system performs qualified electronic sealing of a very large number of documents
* It is integrated with the mechanism for granting registration numbers to all documents originated or registered in the system.
* allows the electronic seal to be visibly positioned anywhere on the document – if the supporting document will have a rotation factor inserted, the application will take it into account
* It has fallback mechanisms for cases where documents released for qualified electronic sealing have structural errors and cannot be sealed, requiring the intervention of an operator in this regard.

**EMAIL AND CHAT WITH CERTIFIED ELECTRONIC IDENTITY**

The email solution has the following functional requirements specific to all "email client" solutions, namely:

* has the classic communication structure specific to all email clients  Received  Sent  Drafts  Archived
* allows two-way message exchange between officials and all types of users
* It allows the two-way exchange of messages via email with individuals and representatives of legal entities, regardless of whether or not they have an electronic identity at the system level, whether or not they are users in the system.
* allows you to build a message with the classic elements of email messages, namely:  Recipient  Subject  Message content  Attachments
* It is integrated with the automated online registry to allow the transformation of a message/email into a paper when it meets the conditions required by the institution. This is to avoid the manual transfer of the content of requests between different email solutions.
* has built-in automatic and manual PDF conversion capabilities for attachments
* allows the conversion of files to PDF format to be done individually or in batches
* has qualified electronic signature capabilities for attachments

**FEATURES SPECIFIC TO THE INTEGRATED CHAT SOLUTION**

The chat solution integrated into the system is available to all users, individuals, legal entities and officials. It has the functionalities specific to chat solutions, namely:

* Two-way message exchange
* File attachments
* Individual or group communication
* Audio conferencing
* Video Conference
* Screen sharing
* Collaborative documents

Officials may enable/disable the chat functionality of individuals and legal entities on their own initiative.