Preservation Manual

Habacus S.r.l.

Habacus

SUMMARY

1. PURPOSE AND SCOPE OF THE DOCUMENT

This document is the Preservation Manual of **Habacus S.r.l.**, pursuant to the **AgID Guidelines on the formation, management and preservation of electronic documents**, in accordance with the Italian Legislative Decree n. 82/2005 so called "**Codice dell'Amministrazione Digitale**" (Articles 20, paragraphs 3 and 5-bis, 23-ter, paragraph 4, 43, paragraphs 1 and 3, 44 , 44-bis and 71, paragraph 1) and **AgID** (Agenzia per l'Italia Digitale) **Guidelines**.

The Preservation Manual details the organization, the subjects involved and the roles played by them, the operating model, description of process, architectures and infrastructures used, the security measures adopted and any other information useful for preservation system management and verification.

In detail, it describes:

a) the details of the persons who formally have assumed responsibility for the preservation system over time, describing in detail, in case of delegation, the subjects, their functions and areas covered by the delegation;
b) the organizational structure including the functions, responsibilities and obligations of every subjects involved in the preservation process;
c) the description of the types of digital objects subject to preservation, including the formats managed, the metadata to be associated with each type of objects, and any exceptions;
d) a description of the method of taking charge of one or more Submission Information Packages, including the preparation of the submission report;
e) the description of the preservation process and the processing of Archival Information Packages;
f) the manner of carrying out the exhibition process and export from the preservation system with the production of the Dissemination Information Package;
g) the description of the preservation system, including all the technological, physical and logical components and the procedures for their management and evolution;
h) a description of the procedures for monitoring the functionality of the preservation system and checks on the integrity of the archives with evidence of the solutions adopted in case of anomalies;
i) a description of the procedures for the production of duplicates or copies;
j) the timeframes for transferring the different types of digital objects to preservation

and, if necessary, for discarding them (as long as, in case of Public Administrations, they are not already described in the preservation plan attached to the records management manual;

k) the conditions requiring the presence of a public official;

l) the regulations in force, which are where digital objects are stored.

In case of inspection by the Supervisory Authorities in charge, the Preservation Manual allows easier control activities.

N° version	Date	Amendments made
01	February 2022	First version

2. DEFINITIONS

TERM	DEFINITION
ACCESS	Operation that allows the viewing of electronic documents.
RELIABILITY	A characteristic that, with reference to a document management or preservation system, describes its level of trust, while with reference to the electronic document, it describes the trustworthiness and accuracy in representing acts and facts contained therein.
COMPUTER DOCUMENT AGGREGATION	Set of electronic documents or set of computer files gathered by homogeneous characteristics (nature and form of the documents, or subject or functions of the entity).
ARCHIVE	The set of records produced or acquired by a public or private entity while performing its activities.
ELECTRONIC ARCHIVE	Archive consisting of electronic documents, organized into computerized document aggregations.
ATTESTATION OF CONFORMITY OF IMAGE COPIES ON AN ELECTRONIC MEDIUM OF AN ANALOG DOCUMENT	Statement issued by a notary public or other public official duly authorized, attached or connected to the computer document.
AUTHENTICITY	A characteristic under which an object is considered as matching to its original state at the time of its production. A characteristic under which an object is considered as matching to its original state at the time of its production. Thus, an object is authentic if it is both intact and complete, having not been subjected to any unauthorised modifications over time or space. Authenticity is assessed on the basis of precise evidences.
CERTIFICATION	Third-party attestation regarding conformity to specific requirements of products, processes, personnel and systems.
CLASSIFICATION	Activity of organizing all documents according to a scheme consisting of a set of hierarchically articulated items that identify the functions, competencies, activities, and/or actors of the producing entity.
PA CLOUD	Virtual environment that enables public administrations to deliver digital services to citizens and businesses in compliance with minimum security and reliability requirements.
CODEC	Encoding and decoding algorithm that allows binary streams to be generated, eventually bagged into a file or wrapper (encoding), as well as extracted from it (decoding).
PRESERVER	Public or private entity that performs electronic document preservation activities.
PRESERVATION	Set of activities aimed at defining and implementing the overall policies of the preservation system and governing its management in relation to the organizational model adopted, guaranteeing over time the characteristics of authenticity, integrity, readability, availability of

TERM	DEFINITION
	the documents
FILE NAMING CONVENTIONS	Set of syntactic rules that define the name of files within a filesystem or package.
DOCUMENT MANAGEMENT COORDINATOR	Person responsible for establishing uniform classification and filing criteria as well as internal communication between organization areas ("AOOs"), in accordance with the provisions of Article 50 paragraph 4 of Presidential Decree 445/2000 in cases of administrations that have established more than one AOO.
RECIPIENT	Entity or system which the computer document is addressed to.
DIGEST	See Cryptographic Footprint.
ELECTRONIC ADMINISTRATIVE DOCUMENT	Any representation, graphic, photocinematic, electromagnetic or of any other kind, of the content of acts, including internal ones, generated by public administrations, or, in any case, used by them for the purposes of administrative activities.
ELECTRONIC DOCUMENT	Any content preserved in electronic form, especially text or sound, visual or audiovisual recording.
COMPUTER DOCUMENT	Electronic document containing the computer representation of legally relevant acts, facts or data.
ELECTRONIC DUPLICATE	See Article 1(1) lett) i quinquies of CAD.
ESEAL	See Electronic seal
EXHIBITION	Operation that enables a preserved document to be viewed
ESIGNATURE	See electronic signature
ELECTRONIC DOCUMENT EXTRACT	Part of the document taken from the original document
EXTRACT BY SUMMARY OF AN ELECTRONIC DOCUMENT	Document in which facts, states or qualities inferred from electronic documents are concisely attested.
STATIC DATA EXTRACTION	Extraction of useful information from large amounts of data (e.g., databases, data warehouses, etc...), by means of automatic or semi-automatic methods
COMPUTER EVIDENCE	Sequence of bits that can be processed by a computer procedure.
ELECTRONIC DOSSIER	Structured and uniquely identified electronic document aggregation containing electronic acts, documents or data produced and functional for performing of an activity or carrying out a specific procedure.
FILE	Set of logically related information, data, or commands, named and recorded, by means of a processing or writing program, in the memory of a computer.
FILE CONTAINER	See Container format.
FILE WRAPPER	See Container format.
***SIDECAR* (FILE)**	File that contains metadata referring to a file or package of files.

TERM	DEFINITION
FILESYSTEM	File management system, structured by one or more tree hierarchies, that determines how files are named, stored, and organized within a storage facility.
ELECTRONIC SIGNATURE	See Article 3 of the eIDAS Regulation.
ADVANCED ELECTRONIC SIGNATURE	See Article 3 and 26 of the eIDAS Regulation.
QUALIFIED ELECTRONIC SIGNATURE	See Article 3 of the eIDAS Regulation.
FLOW (BINARY)	Sequence of bits produced in a finite, continuous time interval, with a definite origin but whose moment of termination may not be predetermined.
CONTAINER FORMAT	File format designed to allow the inclusion (enveloping or wrapping), in the same file, of one or more pieces of computer evidence subject to different types of encoding and which specific metadata may be associated with.
COMPUTER DOCUMENT FORMAT	Mode of representing the sequence of bits composing the electronic document; commonly identified with the file extension.
"DEPRECATED" FORMAT	Format formerly considered official whose use is currently discouraged in favor of a newer version.
ADDITIONAL FUNCTIONS OF COMPUTER PROTOCOL	In the computer protocol system, additional components to the minimum ones, necessary for document flow management, document preservation as well as accessibility of information.
MINIMUM FUNCTIONS OF COMPUTER PROTOCOL	Components of the computer protocol system that meet the minimum operations and information requirements of Article 56 of Presidential Decree No. 445 of December 28, 2000.
CRYPTOGRAPHIC HASH FUNCTION	Mathematical function that generates, from computer evidence, a cryptographic fingerprint or digest (see) in such a way that it is computationally difficult (in fact impossible), from it, to reconstruct the original computer evidence and to generate equal fingerprints from different computer evidence.
DOCUMENT MANAGEMENT	Process aimed at the efficient and systematic control of the production, receipt, holding, use, selection and storage of documents.
HASH	English term used, improperly, as a usage synonym for "cryptographic fingerprint" or "digest" (see).
UNIQUE IDENTIFIER	Sequence of numbers or alphanumeric characters uniquely and persistently associated with an entity within a specific scope.
CRYPTOGRAPHIC FINGERPRINT	Sequence of bits of predefined length, which is the result of applying a cryptographic hash function to computer evidence.
INTEGRITY	Characteristic of a computer document or document aggregation by virtue of which it appears that they have not been subject to any unauthorized alteration in time and space. The characteristic of integrity, together with that of completeness, contributes to determining the characteristic of authenticity.

TERM	DEFINITION
INTEROPERABILITY	Characteristic of an information system whose interfaces are public and open, and capable of automatic interaction with other information systems for information exchange and service delivery.
READABILITY	A characteristic of an electronic document that guarantees the quality of being able to be decoded and interpreted by a computer application.
PRESERVATION MANUAL	Electronic document describing the preservation system and detailing the organization, actors involved and the roles played by them, the operating model, and description of process, architectures and infrastructure.
MANAGEMENT MANUAL	Document describing the management system, also for the purpose of preservation, of electronic documents and providing instructions for the correct performance of the IT protocol service, document flow management and archives.
METADATA	Data associated with an electronic document, computer file, or document aggregation to identify it, describing its context, content, and structure, to enable its time management.
OBJECT OF PRESERVATION	Digital object submitted to a preservation system.
DIGITAL OBJECT	Digital information object, which can take various forms including those of computer document, computer file, computer document aggregation or computer archive.
Archival Information Package	Information package generated by the transformation of one or more Submission Information Packages consistent with the methods outlined in the preservation manual.
Dissemination Information Package	Information packet sent by the preservation system to the user in response to the user's request for access to preservation objects.
FILE PACKAGE	Finite set of multiple files (possibly organized in a subtree structure within a filesystem) that constitute, collectively as well as individually, a unitary, self-consistent information content.
Submission Information Package	Information package sent by the producer to the preservation system according to the format described in the preservation manual.
INFORMATION PACKAGE	Logical container enclosing one or more preservation objects with related metadata, or even just the metadata referring to the preservation objects.
PATHNAME	Ordered sequence of a file path and its name.
Path	Information on the virtual location of the file within the filesystem expressed as an ordered sequence of the name of the path nodes.
PRESERVATION SYSTEM SECURITY PLAN	A document that, in the context of the overall security plan, describes and plans activities aimed at protecting the computer document preservation system from possible risks.
SECURITY PLAN OF THE COMPUTER DOCUMENT MANAGEMENT SYSTEM	A document that, in the context of the overall security plan, describes and plans activities aimed at protecting the computer document

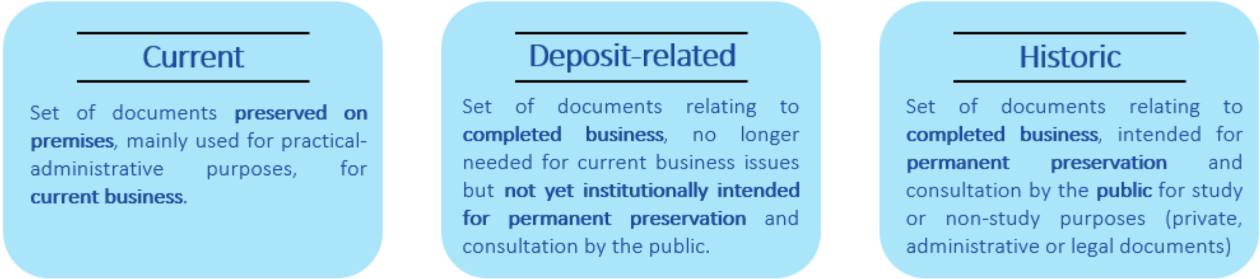
TERM	DEFINITION
	management system from possible risks.
CLASSIFICATION PLAN	Logical structure for organizing documents and digital objects according to a pattern inferred from the functions and activities of the organization concerned.
PRESERVATION PLAN	Document, attached to the management manual and integrated with the classification system, wheree criteria for the organization of the archive, periodic selection and preservation are defined in accordance with Article 68 of Presidential Decree No. 445 of December 28, 2000.
DOCUMENT AGGREGATION ORGANIZATION PLAN	A tool integrated with the classification system from the lower hierarchical levels and aimed at identifying the types of document aggregations (types of series and types of files) that need to be produced and managed in relation to the processes and activities whose functions performed by the entity are defined.
GENERAL SAFETY PLAN	Document that plans the activities aimed at the implementation of the protection system and all possible actions indicated by the risk management.
INTAKE	Acceptance by the preservation system of a Submission Information Package as it complies with the procedures set forth in the preservation manual and, in the case of outsourcing the service, in the agreements entered into between the owner of the object of preservation and the preservation service manager.
PROCESS	Set of linked or interacting activities that transform input elements into output elements.
Producer of the Submission Information Package	Natural person, usually different from the person who created the document, who produces the Submission Information Package and is responsible for transferring its contents to the preservation system. In public administrations, this figure is identified with the person responsible for document management.
QSEAL	Qualified electronic seal, as per Article 35 of the eIDAS Regulation.
QSIGNATURE	Qualified electronic signature, as per Article 25 of the eIDAS Regulation.
DEPOSIT REPORT	Computer document certifying that the preservation system has taken charge of the Submission Information Packages sent by the Producer.
PROTOCOL REGISTER	Electronic registry where the information prescribed by the regulations is stored for all documents received and sent by an entity and for all computerized documents of the entity.
EIDAS REGULATION	electronic IDentification Authentication and Signature, Regulation (EU) № 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

TERM	DEFINITION
REPERTOIRE	Register containing a sequential numbering of the files in the chronological order of their creation within the subdivisions of the classification plan.
PRESERVATION INFORMATION SYSTEMS MANAGER	Person who coordinates the information systems within the Preserver, with the professional requirements identified by AGID.
HEAD OF PRESERVATION SERVICE	person who coordinates the preservation process within the Preserver, with the professional requirements identified by AGID
PRESERVATION OFFICER	Person who defines and implements the overall policies of the preservation system and governs its management with full responsibility and autonomy.
HEAD OF THE ARCHIVAL PRESERVATION FUNCTION	Individual who coordinates the preservation process from the archival point of view within the Preserver, with the professional requirements identified by AGID
HEAD OF DOCUMENT MANAGEMENT	Person responsible for managing the document system or responsible for maintaining the computer protocol, document flow management and archives, pursuant to Article 61 of Presidential Decree No. 445 of December 28, 2000.
DATA PROTECTION OFFICER	Person with specialized knowledge of data protection legislation and practices, complying with the requirements set forth in Article 39 of Regulation (EU) 2016/679.
PRESERVATION SYSTEMS SECURITY MANAGER	Entity that ensures compliance with security requirements within the Preserver, complying with the professional requirements identified by AGID.
RESPONSIBLE FOR THE DEVELOPMENT AND MAINTENANCE OF THE PRESERVATION SYSTEM	Entity that ensures the development and maintenance of the system within the Preserver, complying with the professional requirements identified by AGID.
TIME REFERENCE	Data set representing a date and time with reference to Universal Time Coordinated (UTC).
DATA DUMP	A procedure by which one or more electronic documents are converted from one file format (i.e., envelope format, or file package format) to another, leaving the content unchanged to the extent possible allowed by the technical characteristics of the target file format(s) and encodings.
DISPOSAL	Removal of documents deemed no longer relevant for legal-administrative and historical-cultural purposes, in accordance with current legislation.
SERIEs	Aggregation of documents with homogeneous characteristics.
ELECTRONIC SEAL	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity.
PRESERVATION SYSTEM	Set of rules, procedures and technologies that ensure the preservation of electronic documents pursuant to Article 44(1) of the CAD.

TERM	DEFINITION
COMPUTERIZED DOCUMENT MANAGEMENT SYSTEM	Set of computing resources, equipment, communication networks, and computer procedures used by organizations for document management.
TIMELINE	Virtual timeline on which events relating to an information system or computer document are set. Very different examples of timelines constitute a system log file, a multimedia stream containing synchronized audio\video essences.
OWNER OF THE OBJECT OF PRESERVATION	Producer of the preservation object.
TRANSFER	Transfer of custody of documents from one person or entity to another person or entity.
TUDA	Consolidated Text of Administrative Documentation (Testo Unico della Documentazione Amministrativa), Presidential Decree No. 445 of December 28, 2000, as amended and supplemented.
OFFICE	Referred to a homogeneous organizational area, an office in that area that uses the services made available by the IT protocol system.
AUTHORIZED USER	A person, entity, or system that interacts with the services of an electronic document management system and/or a electronic document preservation system in order to use the information contained therein.
SUBMISSION	Transfer of custody, ownership and/or responsibility of records. In the case of a judicial and administrative body of the state, this is the operation of the person in charge of preservation that transfers to the State Archives or the Central State Archives records to be preserved there under the current legislation.

3. LEGISLATION FRAMEWORK

The Archive is the body of documents (both analogue and digital) produced or otherwise acquired by a corporate body during the course of its activities. The documents that make up the archive are therefore connected by a logical and necessary link known as the 'archival bond' and can be subdivided into three 'life stages':



Current

Set of documents **preserved on premises**, mainly used for practical-administrative purposes, for **current business.**

Deposit-related

Set of documents relating to **completed business**, no longer needed for current business issues but **not yet institutionally intended for permanent preservation** and consultation by the public.

Historic

Set of documents relating to **completed business**, intended for **permanent preservation** and consultation by the **public** for study or non-study purposes (private, administrative or legal documents)

FIGURE 1 ARCHIVE STAGES

The current phase is today partly replaced by digital archiving, i.e. the storage of a document on a Document System, Computer Protocol, CD, server, Repository. It is by nature a 'static' process, not regulated and subject to obsolescence over time.

The filing phase is now partly replaced by digital preservation, a regulated and accredited service in which the document retains its legal value and the characteristics of integrity, immodifiability, readability and authenticity, which a judge assesses in litigation.

Below is a list of the main Italian normative references on the subject, ordered according to the criterion of the hierarchy of sources:

- Civil Code [Book Five Of Labor, Title II Of Labor in the Enterprise, Chapter III Of Commercial Enterprises and Other Enterprises Subject to Registration, Section III Special Provisions for Commercial Enterprises, Paragraph 2 Of Accounting Records], Article 2215-bis - Computer Records;

- Law No. 241, August 7, 1990, and subsequent amendments. - New rules on administrative procedure and the right of access to administrative documents;

- Decree of the President of the Republic December 28, 2000, No. 445 and subsequent amendments and additions - Consolidated text of legislative and regulatory provisions on administrative documentation [Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa];

- Legislative Decree No. 196 of June 30, 2003, and subsequent amendments and supplements. - Code regarding the protection of personal data;

- Legislative Decree No. 42 of January 22, 2004, and subsequent amendments and supplements. - Cultural Heritage and Landscape Code [Codice dei Beni Culturali e del Paesaggio];

- Legislative Decree No. 82 of March 7, 2005, et seq.mm.ii. (Legislative Decree Aug. 26, 2016, no. 179) - Digital Administration Code [Codice dell'amministrazione digitale CAD] et seq.mm.ii;

- Prime Minister's Decree of 22 February 2013 - Technical rules on the generation, affixing and verification of advanced, qualified and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3), 32(3)(b), 35(2), 36(2) and 71;

- Decree of the President of the Council of Ministers of 3 December 2013 - Technical rules on the preservation system pursuant to Article 20 (3) and (5-bis), Article 23-ter(4), Article 43(1) and (3), Article 44, Article 44-bis and Article 71(1) of the Digital Administration Code referred to in Legislative Decree No 82 of 2005;

- Decree of the President of the Council of Ministers December 3, 2013-Technical rules for the computer protocol pursuant to Articles 40 -bis, 41, 47, 57 -bis and 71, of the Digital Administration Code referred to in Legislative Decree No. 82 of 2005 [partially repealed by the AgID Guidelines as of January 2022];

- Prime Ministerial Decree No. 55 of 3 April 2013, Guidelines for the management of electronic invoicing processes towards the Public Administration.

- Decree of the Ministry of Economy and Finance June 17, 2014 - Modalities for fulfilling tax obligations related to computer documents and their reproduction on different types of media - Article 21 (5) of Legislative Decree No. 82 of 2005;

- Decree of the President of the Council of Ministers of 13 November 2014 - Technical rules on the formation, transmission, copying, duplication, reproduction and temporal validation of computerised documents as well as the formation and storage of computerised documents of public administrations pursuant to Articles 20, 22, 23-bis, 23-ter, 40, paragraph 1, 41, and 71, paragraph 1, of the Digital Administration Code referred to in Legislative Decree No 82 of 2005;

- AGID Circular No. 65 of 10 April 2014 - Procedures for the accreditation and supervision of public and private entities performing computerised document preservation activities pursuant to Article 44-bis, paragraph 1, of Legislative Decree No. 82 of 7 March 2005.

- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market.

- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

- AgID Guidelines on the formation, management and preservation of electronic documents, published in September 2020, updated in May 2021 and fully applicable from January 1, 2022.

4. ROLES AND RESPONSIBILITIES

The Preservation Officer, as required by current regulations, defines and implements the overall policies of the preservation system and governs its management with full responsibility and autonomy.

In particular:

a) defines the preservation policies and functional requirements of the preservation system, in accordance with current legislation and taking into account international standards, because of the specificities of the digital objects to be preserved (computer documents, electronic aggregations, electronic archives), the nature of the activities that the Preservation Object Holder performs, and the characteristics of the adopted electronic document management system;

b) manages the preservation process and ensures its compliance with applicable regulations over time;

c) generates and signs the deposit report in the manner prescribed in the preservation manual;

d) generates and signs the Dissemination Information Package with a digital signature or a qualified electronic signature, in the cases provided by the preservation manual;

e) performs the monitoring of the proper functionality of the preservation system;

f) performs the periodic verification, at least every five years, of the integrity and readability of electronic documents and document aggregations of archives;

g) in order to ensure the preservation of and access to electronic documents, take measures to promptly detect any degradation of storage systems and records and, where necessary, restore proper functionality; take similar measures with regard to the obsolescence of formats;

h) arranges for the duplication or copying of electronic documents as the technological environment evolves, in accordance with the provisions of the preservation manual;

i) arranges the necessary measures for the physical and logical security of the preservation system;

j) ensures the presence of a public official in cases where their intervention is required, guaranteeing the same the assistance and resources necessary for the performance of the activities assigned to them;

k) ensures that the competent bodies provided for in the current regulations have the necessary assistance and resources to carry out verification and supervision activities;

l) provides for central and peripheral state administrations to submit electronic documents, electronic aggregations and electronic archives, as well as the tools that guarantee their consultation, to the Central State Archives and the territorially competent State Archives, respectively, in accordance with the established timeframes;

m) prepares the preservation manual and ensures that it is updated periodically when there are relevant regulatory, organizational, procedural or technological changes.

Preservation Manager of Habacus S.r.l. **(First Name Last Name)**	Paolo Cuniberti
Role	CEO & Founder
Assignment start date	2022
End date of assignment	-

The Preservation Manager, under his/her own responsibility, may delegate the performance of their activities or part of them to one or more individuals, who within the organizational structure, have specific skills and experience:

Process reference person (First Name Last Name)	**Jacopo Gasparetti**
Role	Tech Lead
Assignment start date	2022
End date of assignment	-

Process reference person (First Name Last Name)	Gabriele Cascino
Role	Project Manager
Assignment start date	2022
End date of assignment	-

The Preservation Manager, under their own responsibility, may delegate the performance of their activities, or part of them, to an **accredited Third Party**, where a **Preservation Manager** is identified and appointed.

Habacus S.r.l. from 10/03/2022 has entrusted the performance of preservation activities to the following Preservation Manager:

Company name	**InfoCert S.p.A.**
Registered Headquarters:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691
Operational Locations:	Piazza da Porto, 3, 35131 Padova Via Via Carlo Bo, 11, 20143 Milano Via Marco e Marcelliano, 45, 00147 Roma Tel: +39 06836691
Website	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Tax code/VAT number	07945211006
REA Number	RM – 1064345

InfoCert has obtained the AgID Cloud Marketplace qualification (CSP Type B Infrastructure and SaaS for LegalDoc service) since 2019. From February 2022, InfoCert is also listed among the first Italian companies in the AgID marketplace list of preservation services. The details of the activities delegated to the Registrar can be found in the ''Specifics of the Contract - Deed of Entrustment''.

This document, therefore, supplements and details the InfoCert Preservation Manual available in the ''Preservation>Documentation'' section of the infocert.it website (https://www.infocert.it/).

More specifically, consult InfoCert's Preservation Manual for the chapters on:

- Organizational Structure and Roles of the Preserver
- Technical details of the preservation system and handling of storage packages
- Preserver monitoring and controls, integrity and readability checks.

5. OBJECTS SUBJECT TO PRESERVATION

In general, a 'package' is defined as a container that encloses one or more objects to be preserved (computer documents, computer files, computer document aggregations), or even just the metadata referring to the objects to be preserved.

The basic concept is that the document to be preserved should always be accompanied by data describing it and enabling its management over time.

"**Submission Information Package**" refers to the set of documents that **Habacus S.r.l.** sends to the preservation system in a single session. Upon successful deposit, the preservation system returns a Deposit Receipt.

By "**Archival Information Package**" is meant an information package composed of the transformation of deposit packages, automatically formed by the preservation system and deposited in InfoCert data centers. The package so formed, is closed by an XLM file, called UNI SInCRO Preservation Index, digitally signed and time stamped by InfoCert's Service Manager.

"**Dissemination Information Package**" means an information packet sent by the preservation system to the user in response to his or her request, i.e., after a search, leading to the display of the preserved document.

The ultimate goal of the service is to make Dissemination Information Package always searchable, readable, intact, reliable, authentic, and usable by users in the target community, through the mediation of the producing entity, in compliance with the main national and international archival standards.

5.1 DETAIL OF THE DOCUMENT TYPES

This chapter provides a description of the lifecycle of each document type sent to InfoCert's LegalDoc preservation service adopted by **Habacus S.r.l.**, detailing formats, metadata, formation, management and deposit methods.

Document type	Proxy
Format	Digitally signed PDF
Metadata	*mod_del*
Starting date and retention period	*Starting date:* 2022 *Retention period*: preserved for 10 years
Description of the flow of forming, managing, depositing	The document is automatically produced by Habacus based on data inserted by the user. Then, it is digitally subscribed by the user and automatically preserved by Habacus.

Document type	Identity document
Format	PDF
Metadata	*doc_id*
Starting date and retention period	*Starting date:* 2022 *Retention period*: preserved for 20 years
Description of the flow of forming, managing, depositing	The document is uploaded by the user in pdf format on Habacus systems.

Document type	FEA module
Format	Digitally signed PDF
Metadata	*mod_ades*
Starting date and retention period	*Starting date:* 2022 *Retention period*: preserved for 20 years
Description of the flow of forming, managing, depositing	The document is signed digitally by the user during the certification process (Recognition section). It is automatically preserved by Habacus.

Document type	ISQ evidences
Format	Images and/or videos
Metadata	*Iqp_evid*
Starting date and retention period	*Starting date:* 2022 *Retention period*: preserved for 20 years
Description of the flow of forming, managing, depositing	Images and/or videos collected during the certification process (Recognition section).

6. THE PRESERVATION PROCESS

2022, InfoCert's LegalDoc preservation service is usable:

- **Automatically,** through integration with a solution called 'Trusted Onboarding

Platform' (TOP).

The service is provided in **SaaS** (Software as a Service) mode and ensures that integrity, readability and legal validity of electronic documents is kept and guaranteed over time, in compliance with the relevant current legislation.

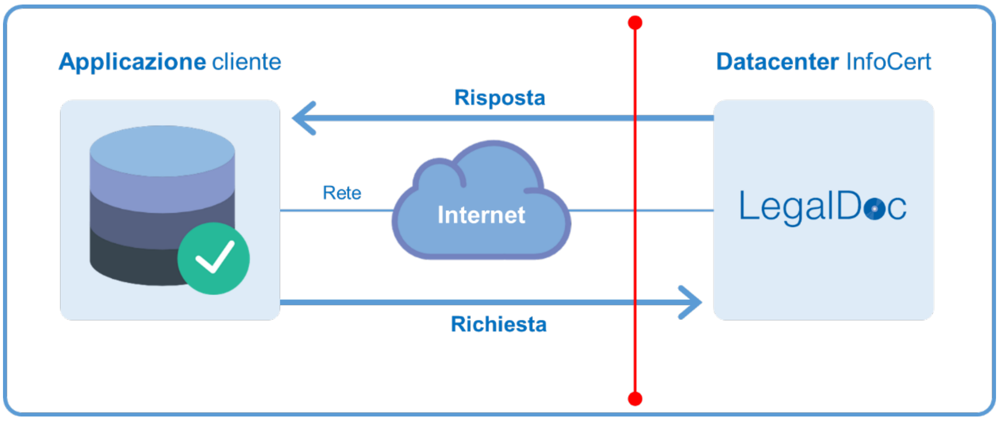


FIGURE 2 REPRESENTATION OF THE SERVICE THROUGH THE NETWORK

Main features:

- Submission Information Package acceptation;
- Storage of the Archival Information Package;
- Archival Information Package rectification;
- Logical erasure of the Archival Information Package;
- discarding of the Archival Information Package;
- Search function of retained documents;
- Exhibition of the Dissemination Information Package.

Each document is associated with a **Preservation Index**, as well as a unique identifier generated by LegalDoc ("**LegalDoc Token**").

The document represents the minimum unit of processing in the sense that it is stored and displayed as a whole.

It is not possible to extract parts of a document from LegalDoc.

6.1 DIGITAL SIGNATURE WITH HSM DEVICE OF ARCHIVAL INFORMATION PACKAGES

Upon successful completion of the preservation process, Archival Information Package is digitally signed by InfoCert's Preservation Service Manager, by means of an automatic signature system provided by the CA - Certification Authority - InfoCert, which uses a high performances HSM cryptographic device.

6.2 TIME STAMPING OF ARCHIVAL INFORMATION PACKAGE

Upon successful completion of the preservation process, each Archival Information Package is time stamped. The time stamp is requested to the TSS - Time Stamping Service - InfoCert, which returns it signed with a certificate issued by the TSA - Time Stamping Authority - InfoCert. The TSS is synchronized via radio with the I.N.RI.M in Turin (Azienda Nazionale di Ricerca Metrologica, formerly "Galileo Ferraris") and is protected against synchronization tampering by physical and logical measures, in full compliance with legal regulations.

6.3 ERROR ANALYSIS

At the time of submission, checks are automatically performed on the packages:

- Declared format of the document to be preserved (consistent with the 'Activation Technical Data Sheet' and the configuration of the environments);
- Correctness of the structure of the Parameters file (containing information for the readability over time of the document to be preserved);
- Correctness of the structure of the Indexes file (which contains the metadata of the document to be preserved, some of which are mandatory, consistent with the 'Activation Technical Data Sheet');
- Presence in preservation on the same path of a document with the same filename as the document to be preserved;
- Enabling User to the submission activity in that given environment (the association between user -username and password- and individual person is in charge of Habacus S.r.l.).
- In-use session validity (by default lasting one hour between login and logout);
- Maximum size of document to be preserved (default 256 megabytes, variable on request);
- Validity of the qualified digital signature used to sign the document to be preserved (optional).

6.4 PROCESS CONTROLS

Process controls are controls which are carried out during the processing of documents subject to the preservation process.

LegalDoc is a complex process, which moves a substantial amount of data, the integrity and consistency of which must be constantly ensured: for this reason, automatic controls are activated, requiring the intervention of the Preservation Service Manager only when any unusual not automatically manageable events occur. Such procedure, called the ''verifier,'' performs binary readability tests by continuously calculating the digital fingerprints of the preserved documents, with subsequent comparison with the hash of the document contained in the submitted Conservation Directives file: if the procedure does not detect any difference between the two hashes, the document is considered unaltered with respect to what was submitted.

In addition to the automatic verification of binary integrity, the Head of the Preservation Service and his appointed Managers are equipped with a special Console, which allows to manually and periodically carry out a sample readability check on the preserved document archive, by randomly choosing and exhibiting a sample of documents in the preservation system.

All checks are reported, and all reports are preserved in accordance with the relevant regulations.

7. RESEARCH AND EXHIBITION PROCESS

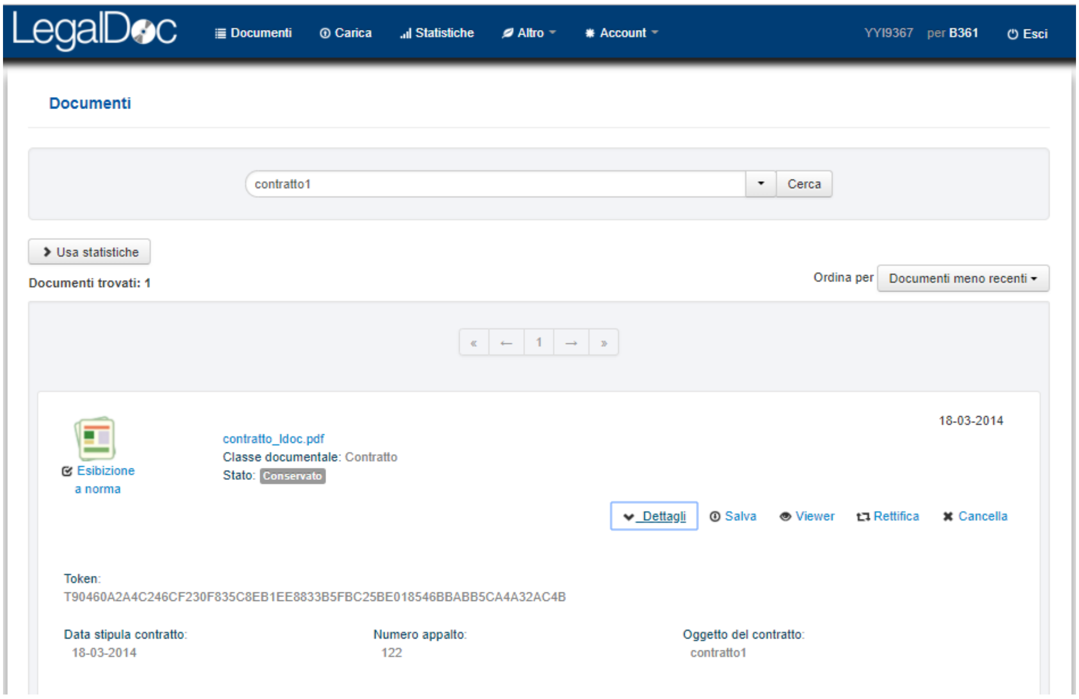
The LegalDoc service of researching and exhibiting retained documents can be used in the following modalities:

- **manual,** through the **LegalDoc WEB portal**.

Access to the search and exhibition of preserved documents takes place on the basis of credentials agreed with **Habacus S.r.l.**, password-protected and configured with specific rules that allow access only to certain document types, based on what is requested through **''Contract Specifics - Activation Technical Data Sheet".**

7.1 RESEARCH AND EXHIBITION IN LEGALDOC WEB

The LegalDoc WEB portal allows to research and extract from the system a document whose the preservation procedure is completed, using the token or metadata that have been filled during submission, and to access the so-called 'standardized exhibitor' to produce one or more Dissemination Information Packages.



contratto1

Documenti trovati: 1

18-03-2014

contratto_ldoc.pdf

Classe documentale: Contratto

Stato: Conservato

Token:
T90460A2A4C246CF230F835C8EB1EE8833B5FBC25BE018546BBABB5CA4A32AC4B

Data stipula contratto:	Numero appalto:	Oggetto del contratto:
18-03-2014	122	contratto1

FIGURE 3 LEGALDOC WEB INTERFACE

Through exhibition it is possible to:

- extract a document and display it on the screen;
- produce a paper copy of the document (or to produce a copy of it on other computer medium);
- extract the viewers stored in the preservation system, allowing them to be installed on the station where the exhibition is taking place;
- verify the validity of digital signatures and time stamps affixed in the preservation process;
- verify the integrity of the preserved document and all documents of the package;
- view the accompanying files, which qualify the preservation process by certifying that it has been carried out correctly:

  o The UNI SInCRO Preservation Index, otherwise known as the Archiving Package Index or Preservation Index (signed and timestamped by InfoCert's Service Manager)

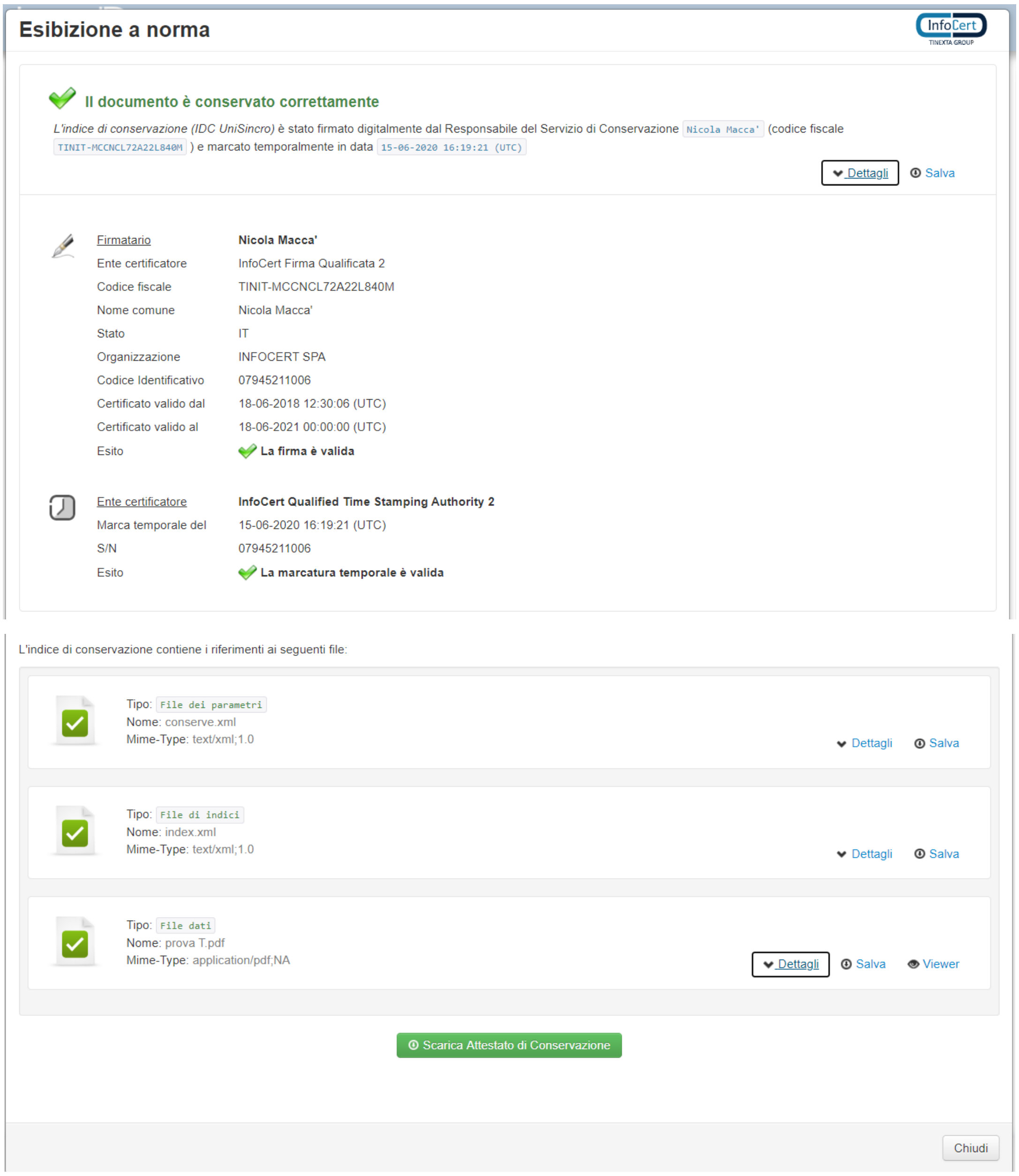
  o Parameter File (containing the information for readability over time)

  o Index File (containing the metadata of the preserved document)

  o Data file (preserved document)

  o Certificate of proper preservation (signed and marked by InfoCert's Service Manager).

The display of the document obtained by querying the LegalDoc system represents a complete and legally compliant exhibition.



Esibizione a norma

✓ Il documento è conservato correttamente

L'indice di conservazione (IDC UniSincro) è stato firmato digitalmente dal Responsabile del Servizio di Conservazione `Nicola Macca'` (codice fiscale `TINIT-MCCNCL72A22L840M`) e marcato temporalmente in data `15-06-2020 16:19:21 (UTC)`

Firmatario	**Nicola Macca'**
Ente certificatore	InfoCert Firma Qualificata 2
Codice fiscale	TINIT-MCCNCL72A22L840M
Nome comune	Nicola Macca'
Stato	IT
Organizzazione	INFOCERT SPA
Codice Identificativo	07945211006
Certificato valido dal	18-06-2018 12:30:06 (UTC)
Certificato valido al	18-06-2021 00:00:00 (UTC)
Esito	✓ **La firma è valida**

Ente certificatore	**InfoCert Qualified Time Stamping Authority 2**
Marca temporale del	15-06-2020 16:19:21 (UTC)
S/N	07945211006
Esito	✓ **La marcatura temporale è valida**

L'indice di conservazione contiene i riferimenti ai seguenti file:

Tipo: `File dei parametri`
Nome: conserve.xml
Mime-Type: text/xml;1.0

Tipo: `File di indici`
Nome: index.xml
Mime-Type: text/xml;1.0

Tipo: `File dati`
Nome: prova T.pdf
Mime-Type: application/pdf;NA

FIGURE 4 LEGALDOC EXHIBITOR

8. SECURITY AND DATA PROTECTION

8.1 COMPANY POLICY HABACUS S.R.L.

Habacus srl, due to the nature of its activities, is subject to the rules imposed by the GDPR legislation for the protection of user data.

8.2 POLICY INFOCERT

The technical description of the LegalDoc preservation service and the main physical and logical security measures adopted are contained in the ''**Specifics of the Contract - Technical Annex.''**

8.3 DESIGNATION OF PRIVACY OFFICER FOR THE PROCESSING OF PERSONAL DATA

Pursuant to paragraph 4.10 ''Security Measures'' of the AgID Guidelines and EU Regulation no. 679/2016, InfoCert as third preservation party entrusted by **Habacus S.r.l.**, is duly appointed as Personal Data Processor.

The appointment is included within the **''Specifics of the Contract – Appointment as Data Manager''**.

Data processing is carried out:

- For the sole performance of the contract (provision of the service),
- with the adoption of the security measures ex art. 32 of the Regulation
- in compliance with the obligations provided for Data Processors by Article 28 of the Regulation.

In addition, all data requests made by InfoCert services are configured to collect the minimum set of data required for the provision of the service and in compliance with current regulations.

All timing, types of data and their quantity are set by **Habacus S.r.l.** pursuant to the **''Contract Specifics - Activation Technical Data Sheet**.''

InfoCert has adopted a special "Procedure for discard, hand-over and termination plan", aimed at minimizing as much as possible the processing of data, quantitatively and qualitatively.

9. FEATURES OF THE CONTRACT

The service is governed by the following technical and contractual documents, shared at service activation.

1. ***General Terms and Conditions***;
2. ***Activation Technical Data Sheet***, which contains all requirements in relation to document types, formats, metadata and access credentials to be requested; which contains all requirements in relation to document types, formats, metadata and access credentials to be requested.
3. ***Appointment as Data Manager,*** which formalises the outsourcing of the preservation process to InfoCert, the appointment of InfoCert as Data Processor in accordance with EU Regulation No. 679/2016 GDPR, and expressly states which activities are in fact carried out by InfoCert and which, on the contrary, remain the responsibility of the client***;***
4. ***Technical Annex,*** which describes how the service is provided and the technical-infrastructure used for its provision;