DECISION

No.357, date 24.4.2013

ON APPROVAL OF REGULATION " ON ELECTRONIC DOCUMENT MANAGEMENT IN THE REPUBLIC OF ALBANIA "

Pursuant to Article 100 of the Constitution, Article 3 of Article 21 of Law no. 10 273, dated 29.4.2010 "On Electronic Document" and Law no. 9880, dated 25.2.2008 "On signing electronic ", with the proposal of the Minister of Innovation and Information Technology of Communication, Council of Ministers

DECIDED:

1. Adoption of the regulation "On electronic document management in the Republic of Albania ", according to the text attached to this decision.
2. All public administration units will be assigned, which will use the electronic document for the implementation of this decision.

This decision enters into force after its publication in the Official Notebook.

PRIMEMINISTER
Sali Berisha

REGULATION
ON ELECTRONIC DOCUMENT MANAGEMENT IN THE REPUBLIC OF ALBANIA

CHAPTER I
GENERAL PROVISIONS

1. Purpose

The purpose of this regulation is to determine the general rules for the use of electronic document, in accordance with law no. 10273/2010 "On electronic document", which, saving time and financial costs, ensures that these documents are available, authentic, accessible during their lifecycle.

2. Objects
   - 2.1 This regulation defines the creation, sending, receiving, protection, storage, protocols, archiving, according to the legislation in force and the specifications set forth in this regulation for public administration bodies.
   - 2.2 This Regulation shall be implemented by any public administration body, who shall create technological, organizational and human resources required for the functioning of the system management of electronic documents.

3. Definitions
   - 3.1 The Electronic Document Management System (SMDE) includes the complete set of tools specifically designed for information and communication technology (ICT) manage the creation, use, maintenance and making available of documents, by purpose to provide evidence of institutional activities.

3.2 Electronic document management equipment is the technical equipment that enable management of the electronic document according to the formats set out in annex no. 1, in interaction with the technical equipment of the creation of the electronic signature, according to the signing electronic law.

3.3 The volume will be called a set of documents that have links or belongs to the same issue or topic, which are stored together.

4. Organization and functions

Public institutions, according to this regulation, for the use of the electronic document, should provide:

4.1 Use of an electronic document management system;

4.2 Appoint the responsible person / administrator and his deputies to take action on definition of standards regarding the creation, maintenance and use of electronic documents from the system.

5. Duties and responsibilities of the institution on SMDE management

Public institution through the head of the institution or persons authorized by him / her:

5.1 Approves access rights to SMDE and possible changes to an employee or group of employees.

5.2 Approve measures to ensure the upgrading of the system in an ICT more advanced, when the first is unable to perform the functions provided.

5.3 During technological upgrade (upgrading) should be ensured the preservation of its integrity data and documents stored in the system; and:

1. Periodically reviews and renews / converts documents into the latest formats.
2. Review and, if necessary, update (update) the technological devices (software & hardware) used by the system, which enable the functions defined in the item 6 of this regulation.

5.4 Determines the structural, detailed responsibilities and job descriptions for each role, for good functioning of the system as well as responsibilities for access to one's control measures electronic document, which is recorded in metadata.

5.5 Approves technical and organizational measures to ensure authenticity, integrity, availability of electronic document.

5.6 Determines the technical performance monitoring of SMDE performance, for it identified shortcomings in the process of working on systems and other methods to eliminate them.

6. SMDE Functions

The electronic document management system, must meet the functional requirements of based on international standard ISO / 161 75-2; Enabling functions of following:

6.1 Creating, Sending, Receiving, Protecting, Preserving, Protocoling, Archiving, according to the applicable legislation and the technical specifications set out in this regulation.

6.2 Identifying and Authenticating Users.

6.3 Protecting information about each user versus others.

6.4 Allow tracing of any modification of the information being processed, identify his author as well as perform the registration of each user's activity in such a way as to guarantee the security and integrity of the system.

6.5 Verify and Ensure Compliance with the Specifications in accordance with the Law for the electronic document.

6.6 Verify and Ensure Compliance with the Specifications in accordance with the Law for the electronic signature, in order to enable the creation and verification of a signature qualified electronics.

6.7 Ensure that an input / output DE is recorded only once in the system and provide the union of documents in groups of clearly defined documents that are related or belong to the same topic or topic,volume.

6.8 Automatically fill the data into DE metadata.

6.9 Provide search methods at each level of the system as well as generate the results of this search.

6.10 With the circulation within the institution, all DE versions should be kept.

6.11 Before submitting the SMDE electronic document, it first generates its protocol from the system.

6.12 When transferring DE to another information technology system, the document should not miss any additional data, including the necessary metadata according to Annex no. 1.

6.13 To prevent unauthorized or accidental deletion or destruction of DE.

6.14 Print the contents of DE and their metadata, information on signing electronic, as well as other additional data contained in SMDE.

6.15 Generate paper copies of the electronic document, or a converted copy of metadata, which records the data of the creator and the DE signatory, containing the title (institution) and position of the signatory (employee), name, surname, date of creation and date signing.

6.16 Be able to carry out a DE transfer procedure, to be stored on State Archives.

6.17 To verify the existence of a DE at a given time.

6.18 Perform other functions according to user specifications.

6.19 To enable the recognition of documents in audio and video format.

6.20 To enable the re-entry of DE and their accompanying data into the system by physical storage mediums.

6.21 The electronic document management system must fulfill the obligations that:

derive from law no. 10 325, dated 23.09.2010 "On the state database" and the acts by-law issued in its implementation.

6.22 SMDE must accept and process document formats as per specifications mentioned in Annex no. 2.

CHAPTER II
CREATION AND TRANSLATION OF THE ELECTRONIC DOCUMENT

7. Creation and content of electronic document

7.1 The structure of a DE is done in accordance with the requirements and specifications of the law electronic document.

7.2 Institutions applying the use of DE must meet the requirements and criteria according to the law on the electronic document and this regulation.

7.3 After creating an DE, the creator signs it with a qualified electronic signature, according to the law on electronic signature.

7.4 The exterior appearance of an DE must meet the same criteria as paper document.

7.5 Before sending the electronic document, it must be checked that the electronic signature, attached to it, is valid and verifiable.

8. Receiving and processing electronic document
    8.1 A state institution, upon receipt of the electronic document, treats it in the same procedures that deal with the written document, as defined in the law "On Archives".
    8.2 When receiving a document in writing from an institution that does not have SMDE, the recipient institution returns it electronically and handles it in the same manner as the electronic document.
    8.3 Institutions that use SMDE during their correspondence with institutions who do not use such a system, after the DE protocols to be sent, return it in a written form, attaching the protocol number.
9. Protection and preservation of electronic document
    9.1 Security measures adopted and implemented by a state-owned SMDE user institution should ensure the availability of processed and stored information in the electronic protocol, duplicates and restoration of functional status in case of emergency situations.
    9.2 Security of operation, access to an electronic protocol corresponds to security documents adopted by the public institution and is based on a security regulation according to international standards.
    9.3 Security measures, in conformity with security documents, should be checked and audited periodically.
    9.4 During the storage time, it should be ensured that the DE and the attached metadata are accessible, readable; and the electronic signature is verifiable.
    9.5 The timeframe for storing a document is determined by its importance and subject matter in accordance with the law on archives.
    9.6 The institution should ensure that DE and related data are backed up periodically from the central device to other physical media, as well as in an electronic backup system, internally and externally, established according to international standards in regulations for SMDE.
    9.7 Every institution that uses SMDE must keep for a period of time of 10-15 years, the documents .
10. Copy of electronic document on paper

Each DE may also be printed on paper in accordance with the conditions set out in Article 10 of the Law on Electronic Documentation.

KREU III
ELECTRONIC PROTOCOL

11. Minimum security requirements of electronic protocol
    11.1 The electronic protocol should be subject to the same standard procedures, as well as the standard protocol. It should only be maintained by the authorized person.
    11.2 Protocol / creation of a new entry in the electronic protocol should be protected from unauthorized interferences and modifications.
12. Electronic protocol of DE
    12.1 The electronic protocol receives DE only through SMDE.
    12.2 The electronic protocol records the DE received in the list / register of the documents received.
    12.3 At the time of registration, DE displays a serial protocol number, which should be unique, along with any other identifying information.

12.4 When an DE does not come from another SMDE but comes in hard copy, after its conversion in electronic form is filed in the same manner as DE.

12.5 Procedures for registration of entry and exit documents are carried out according to the criteria determined according to the technical-professional and methodological norms of the archival service in the Republic of Albania.

12.6 DE received are automatically collected from SMDE and entered into a list of received documents, starting from the earliest, in accordance with the law on the archives and internal regulations of the institution. Once approved by the responsible person, they pass on a list of protocols and, according to the specific needs of the institution, can be printed or transmitted for further processing within the institution.

12.7 In the case of DE being sent incorrectly, the responsible person revokes / rejects it.

12.8 At the same time, the system transmits a revocation message to the sending institution .

12.9 For security reasons, the contents of the e-protocol are stored periodically on separate files.

ANNEX NR.1

1. ELECTRONIC DOCUMENT METADATAS

1.1 The name of the natural person, the sender

1.2 Name of legal person, sending institution,

1.3 Document title

1.4 Date of dispatch of the document

1.5 The protocol number of the sending institution

1.6 Date of receipt of the document

1.7 Receiver Protocol Number

1.8 Index of the "file" to which the document is kept Institution code (NIPT) Name of institution to which it is sent

2. ELECTRONIC SIGNATURE METADATAS

2.1 Full Name of the Signatory Person

2.2 Position of the signatory person

2.3 Date and time of signature creation. Signature Purpose (Signature, Approval, etc.)

3. METADATAS OF ELECTRONIC "FILE"

3.1 Name of the institution

3.2 The name of the directorate or the relevant sector, who created the document or to whom it is addressed

3.3 The volume index to which this "file" belongs

3.4 Title or volume subheading (if any)

3.5 Volume creation date

3.6 Information on Destruction of "File"

Volume Storage Information

Information on backup "file"

4. PROCEDURE FOR PREPARING AND SUPPLEMENTING METADATES

The person responsible for completing the metadata should enter his full name, the date of completion; the name of the person responsible for their approval and the date of approval; if the latter changes from the first.

5. METADATAS OF ELECTRONIC DOCUMENT MANAGEMENT

5.1 Data on changes that may have been made to the metadata of the document or the electronic "file".

5.2 Data on access to electronic document or "electronic file" and / or possible restrictions on metadata or over the limit of changes that may be made on them.

6. METADATAS OF STORAGE "FILE" OF ELECTRONIC DOCUMENTS

6.1 Data on the "backup" of the electronic document (number, format, storage location, storage space, etc.).

6.2 Data on converting and restoring the document from "backup".

7. OTHER OPTIONAL METADATAS

7.1 File metadata and electronic file

a) The electronic document format
b) Data on the period of validity of the electronic signature
c) Address of the sending institution
d) Contact number of the sending institution
e) Type of document (warrant, instruction, memo, etc.)

ANNEX NR.2

2.1 ELECTRONIC DOCUMENT FORMS WHICH SHOULD BE KNOW SMDE

a) Microsoft/Apple Rich Text Format (RTF) latest version as per Microsoft Corporation.
b) Adobe Portable Document Format (PDF) latest version as per Adobe Systems Incorporated.
c) HTML according to the latest version from http://www.w3c.org d
d) XML latest version, Extensible Markup Language from http://www.w3c.org
e) XHTML latest version, from The Extensible Hyper Text Markup Language
f) Open Office, org XML File Format, from Open Office.org,Technical ReferenceManual Microsystems, http://xml.openoffice.org/xml_specification.pdf.
g) Secure Hyper Text Transfer Protocol. HTTPS, from RFC 2660S-HTTP
h) Microsoft Office formats (.doc, .docx,. ppt, .pptx etj.)
i) Any kind of "file" format that is judged reasonable.

2.2 REFERENCE STANDARDS

a) ISO 15489 Information and documentation — Records management
b) ISO 21127 Information and documentation — A reference ontology for the interchange of cultural heritage information
c) ISO 23950 Information and documentation — Information retrieval (Z39.50) — Application service definition and protocol specification
d) ISO 10244 Document management — Business process baselining and analysis
e) ISO 32000 Document management — Portable document format
f) ISO 2709 Information and documentation — Format for information Exchange
g) ISO 15836 Information and documentation — The Dublin Core metadata element