Pursuant to paragraph two of Article 17 of the Protection of Documents and Archives and Archival Institutions Act (Official Gazette of the Republic of Slovenia [*Uradni list RS*], Nos 30/06 and 51/14), the minister responsible for culture hereby issues

RULES

on the uniform technological requirements for the capture and preservation of records in digital form

I. INTRODUCTORY PROVISIONS

Article 1

(Purpose and area)

These Rules shall prescribe in detail the manner, scope and implementation of the individual phases of preparation and execution of capture, digital preservation and accompanying services for the long-term preservation of records in digital form, internal rules according to their purpose and scope, the application for the approval of internal rules and pertaining documentation, the adoption of model internal rules, the demonstration of professional qualifications of internal assessors, the procedure of capture and digitisation, the conditions for conversion to microfilm, the content of additional professional and technical instructions for the selection of archival records in digital form, the conditions for the certification of hardware, software and services, the application forms for the registration of equipment and services providers, the equipment and services certification.

Article 2

(Application of the Rules)

(1) These Rules shall apply to the persons referred to in Article 17 of the Protection of Documents and Archives and Archival Institutions Act (Official Gazette of the Republic of Slovenia [Uradni list RS], Nos 30/06 and 51/14; hereinafter: the Act), the applicants requesting the registration of the equipment or service providers, the applicants requesting the certification of hardware and software and services, and to the National Archives.

(2) Pursuant to these Rules, the National Archives shall create and maintain checklists for the transparent certification of equipment and services and the assessment of internal rules established by the Act and the Decree on the Protection of Documentary and Archival records (Official Gazette of the Republic of Slovenia [Uradni list RS], No. 42/17; hereinafter: Decree), and publish them on its website.

(3) The checklists referred to in the preceding paragraph shall be used by the persons referred to in Article 17 of the Act for the purpose of self-assessing and verifying the implementation of internal rules and model internal rules, by applicants requesting the certification of hardware, software and services, and by auditors in the procedures for the approval of internal rules and certification.

Article 3

(Definitions)

For the purpose of these Rules, the following definitions shall apply:

1. "aggregation" shall mean any form of document merging into a single integrated unit of records, e.g. a case, a file, a dossier;
2. "audio-visual records" shall mean pictorial or sound records on different media in analogue or digital form;
3. "deletion" shall mean the physical destruction of a record in such a manner that no metadata about the deleted record are created; For example, a draft document is deleted after its final version has been published.
4. "certification of equipment and services" shall mean the procedure by which the National Archives acknowledges compliance of offered equipment, capture and digital preservation, and accompanying services with applicable regulations;
5. "digitised record" shall mean an electronic copy of a record in physical form created during the procedure of converting records from physical to digital form;

6. "digital preservation" shall mean the preservation of records in digital form;
7. "electronic signature" shall mean a set of data in electronic form that are contained in, attached to or logically associated with other data and shall serve for data authentication and the identification of the signatory;
8. "electronic archiving" shall comprise the procedures for submitting archival records in digital form to competent archival institutions, the processing and long-term preservation of such records in accordance with the applicable legislation and shall also enable the efficient management and use of such records;
9. "record units" shall mean documents, files, entries in the official register, or other forms of registered records or groups of records;
10. "register" shall mean a list of records;
11. "registering" shall mean the process of systematically entering data about records in the register;
12. "Geographic Information System" shall mean a system for the collection, management, preservation, analysis and display of spatial data having the characteristics of records;
13. "records" shall mean current, semi-current and archival records in digital form as defined by the Act;
14. "information assets" shall mean the assets and resources (facilities, hardware and software, people, work procedures for the capture and digital preservation and accompanying services, records) managed by a person itself or other persons and which are necessary for the capture, digital preservation and accompanying services and are protected from danger (such as human error, intentional acts, impacts of environment, organisational and technical errors);
15. "elimination" shall mean the preparation procedure for the destruction of records with expired retention periods;
16. "derived spatial data" shall mean data that were generated in the system following a specified procedure for input spatial data processing and are considered to be new spatial data;
17. "born-digital records” shall mean records that have been originally created in digital form;
18. "classification" shall mean the procedure for the classification of records according to content and business activities of a person;
19. "business continuity plan" shall ensure the continuous operation of activities that are necessary to support the functioning of the digital preservation system during disruptions or interruptions of the normal functioning and the recovery of the digital preservation system normal operation in an adequate period according to risk assessment;
20. "selection" shall mean the procedure for the selection of archival records;
21. "equipment" shall mean all software and hardware which entirely or partly enables the capture and digital preservation or accompanying services;
22. "person" shall mean an entity under public law performing the capture and preservation of records in digital form, a provider of capture and digital preservation or accompanying services, or a person seeking to enforce the validity and probative value of their records in accordance with the provisions of Article 31 of the Act (the entity referred to in paragraph one of Article 17 of the Act);
23. "conversion" shall mean the procedure of changing the form of the record;
24. "adopter of model internal rules" shall mean a legal person who has adopted the model internal rules;
25. "production environment" shall mean the environment for regular use in which capture, digital preservation and accompanying services are performed;
26. "spatial data" shall mean any data that directly or indirectly refer to an individual location or geographic area;
27. "procedures" shall mean operations that include capture, digital preservation and the related activities (e.g. conversion, elimination and destruction, selection and submission) carried out by the owner of the records;
28. "class" shall mean a substantive unit of record classification and a basic component in the classification plan. Class is defined by a class identifier, content description and a retention period. In accordance with legislation or internal acts regulating classification, classification procedures classify aggregations (e.g. files) or individual documents into classes.
29. "audit trail” shall mean an unaltered record, documented in detail, which unequivocally, incontestably and comprehensively documents the recording and modification of records from their origin to their present valid version. It shall at least show who, when, which data and what kind of operation was carried out on an individual record and shall enable subsequent recognition of the time, person, manner and content of additional processing of data to which the audit trail relates;
30. "pictorial material (in physical form)" shall mean artistic pictures and drawings, photographs, slides, negatives, negatives on glass, prints, posters, leaflets, postcards and graphics;
31. "administrator of model internal rules" shall mean a legal person who is the administrator of model internal rules that are also available to other persons;

32. "administrator" shall mean the person given administrative rights. These Rules shall differentiate between the system administrator, the database administrator and the software administrator;
33. "administrator rights" shall mean rights relating to the responsibilities of administrators whose task is to guarantee the technical and substantive proper operation of the information system, database and software. The division of roles and restriction of rights shall provide adequate assurance of compliance with the principles applying to records, which are defined by the Act;
34. "submission information package" shall mean a comprehensive set by means of which entities under public law submit archival records in digital form to the competent archival institution in accordance with additional professional and technical instructions provided by the competent archival institution;
35. "services" shall include capture and digital preservation or accompanying services rendered by a provider;
36. "destruction" shall mean the procedure of removing current records with an expired retention period in such a manner that their retrieval is no longer possible. After records are destroyed, certain metadata that prove the existence and destruction of records shall be retained.
37. "manager of the official register" shall mean a person who acts as a substantive administrator of the register in accordance with the legislation governing the establishment and management of registers;
38. "official register" shall mean any register created pursuant to any law, implementing regulation or general legal act, which is issued for the purpose of exercising public authority.
39. "role" shall mean a set of responsibilities and tasks defined by internal rules relating to the capture and preservation of records;
40. "type of records" shall mean textual and mixed records, film and audio-visual records, websites, e-mail, databases, official registers and spatial data.

II. INTERNAL RULES FOR THE CAPTURE AND, DIGITAL PRESERVATION OF RECORDS AND ACCOMPANYING SERVICES

1. Preparation and organisation for capture and digital preservation of records in digital form, and the provision of accompanying services

Article 4

(Preparation for capture, digital preparation and accompanying services)

(1) Prior to the adoption of internal rules, a person shall execute preparation and organisation for capture, digital preservation and accompanying services. A person drafting the amendment to internal rules shall additionally execute the preparation and organisation for capture, digital preservation and accompanying services to the extent necessary to enable the substantive drafting of the amended internal rules.

(2) A person submitting the application for the approval of internal rules or model internal rules referred to in Article 20 of the Act shall also attach a report on the completed preparation referred to in the preceding paragraph.

(3) The report referred to in the preceding paragraph shall include at least the following information:
1. the scope of capture, digital preservation and accompanying services, which shall be regulated by internal rules;
2. a description of the risk assessment methodology and risk management plan;
3. an analysis of records' management, comprising at least of:

- a description of business, legal and technological requirements which the applicant must comply with when performing procedures or services;
- an inventory of the information assets relating to capture and digital preservation of records or accompanying services;
- an inventory of the types of records that are being created or will be captured and preserved, indicating records that have the characteristics of current and archival records;
- a summary of the assessment of the existing information system and information security, including a list of key risks;

4. a plan for the performance of procedures or services and for the establishment or renewal of the information system.

2. General provisions relating to internal rules

Article 5

(Type and scope of internal rules)

(1) A person shall draw up and adopt internal rules based on the findings of preliminary preparation and organisation for capture, digital preservation of records and accompanying services. The internal rules shall unambiguously specify:

- the type of internal rules (whether they apply to own operations, the provision of services or model internal rules),
- the scope of procedures or services; and
- the types of records whose capture and digital preservation or accompanying services are governed by internal rules.

(2) The internal rules, depending on their type, the scope of operations and the types of records, shall contain all the parts referred to in paragraphs one, two and four of Article 8 of the Decree.

Article 6

(Model internal rules)

(1) A person preparing model internal rules shall determine for whom they are intended.

(2) The person who has prepared model internal rules shall draw up the instructions for their adoption. The instructions shall contain at least the following information:

- a definition of the permitted scope of adaptation of provisions or parts of provisions that refer to the status, internal organisation or other internal characteristics of the adopter (personalisation),
- a description of the adoption of model internal rules with instructions for personalisation;
- a description of the preparation for the capture, digital preservation of records and accompanying services of the adopter;
- a notification that the person adopting model internal rules should inform the National Archives of the adoption;
- a description of the activities to be carried out by the adopter of model internal rules in order to be informed by the drafter of any amendment to these rules.

(3) For the reasons specified in Article 22 of the Act, the person who has prepared or maintains model internal rules shall inform the adopters of any amendment to internal rules in the manner specified in the instructions for adopting the internal rules referred to in the preceding paragraph.

Article 7

(Obligation to submit internal rules for confirmation)

(1) The person referred to in Article 19 of the Act shall define in the internal rules the filing of an application for the approval of internal rules, and responsibilities in this regard. This obligation shall also apply to any amendments made to internal rules.

(2) Where model internal rules are intended for entities under public law, the preparator shall be obliged to submit them to the National Archives for approval. This requirement shall not apply to state administration authorities.

Article 8

(Application for the confirmation of internal rules)

(1) The application for the confirmation of internal rules shall be made using the prescribed form in Annex 1, which is an integral part of these Rules (hereinafter: Annex 1), or through the online application containing all the components listed in Annex 1 to these Rules.

(2) The application for the confirmation of model internal rules shall be made using the prescribed form in Annex 2, which is an integral part of these Rules (hereinafter: Annex 2), or through the online application containing all the components listed in Annex 2 to these Rules.

(3) Prior to submitting the application for the confirmation of internal rules, their preparator shall perform a self-assessment of their compliance. by entering in the relevant checklist, with respect to each request (checkpoint), data on the provisions of internal rules that are to be in the form of references and are to ensure compliance of the internal rules with the Act, implementing regulations and rules of the profession. The checklist shall be published on the website of the National Archives in accordance with Article 2 of these Rules.

(4) The application shall be accompanied with:

- a report on the preparation for capture, digital storage of records and accompanying services;
- a list of the documents constituting the internal rules, and the listed documents,
- the self-assessment referred to in the preceding paragraph.

(5) The list referred to in indent two of the preceding paragraph shall contain at least the following information:

- the title of the document;
- the version of the document or the identification code of the document entered in the register of current records; and
- the confirmation date of the document.

(6) The information contained in the list of documents constituting the internal rules and the names and codes of the documents or versions of the documents accompanying the application for the confirmation must be harmonised.

(7) Where, in the self-assessment referred to in point three of this Article, the drafter refers to a certificate of conformity (e.g. an ISO standard certificate) issued by a competent body or an independent organisation, the application for the confirmation of internal rules should be accompanied by this certificate and proof of the scope of the compliance verification.

(8) The internal rules shall be signed by authorised persons within the organisation or their approval of the competent person shall be proved otherwise.

Article 9

(Internal rules management)

(1) A person shall specify by internal rules the means which ensure that:

1. all internal rules documents include the version code, the date of adoption and entry into force, while the publication in the official journal and the date of publication may also be used to indicate the version;
2. unauthorised amendment to internal rules is prevented,
3. the internal rules are published in the manner prescribed by the person and accessible to all for whom they are intended;
4. the amendments to the internal rules are notified to all persons whose work is related to these amendments;
5. the internal rules are readable, understandable and useful;
6. the use of outdated versions of internal rules is prevented;
7. the outdated versions are preserved,
8. the internal rules are maintained, reviewed regularly (at least once a year) and updated when necessary.

(2)For the performance of tasks defined by these Rules, a responsible person (the administrator of internal rules) shall be specified in the Internal rules.

(3) Should the new internal rules replace the old ones, the end of the validity period of the old internal rules and any exceptions shall be determined.

(4) The internal rules of entities under public law shall be deemed to be archival records.

Article 10

(Monitoring the implementation of internal rules)

(1) Internal rules shall define the obligation to designate responsible persons and assessors of internal rules implementation as laid down in Article 10 of the Decree.

(2) The person's management shall ensure that the internal assessors, assessing the implementation of internal rules, have sufficient qualifications in the fields of records' management, archival science, information infrastructure and security, and in the fields which they assess; however, they shall not assess those activities in which they are directly involved. They shall be acquainted with the purpose and content of the internal rules under review, as well as with the internal assessment procedures. A person may also involve external assessors in the assessment, who shall have the same qualifications as internal assessors.

(3) After each assessment, the head of the assessment shall draw up a report assessing the implementation of internal rules, which contains at least the following information:

1. the time and place of the assessment,
2. the names and surnames of the assessors,
3. the purpose of the assessment (regular, repeated or unscheduled assessment);
4. the specification of parts of the internal rules that have been assessed (title of document or annex, version, date of approval);
5. the findings and evidence of any deviations in the implementation of internal rules,
6. recommendations and proposals for measures to eliminate any deviations in the implementation of internal rules, including their type (prevention, corrective) and implementation deadlines; and
7. persons responsible for the implementation.

(4) The report referred to in the preceding paragraph may include proposals for amendments to the provisions of the assessed internal rules.

(5) When internal rules regulate the capture and digital preservation of public or private archival records that are laid down by the Act or a decision of the National Archives, the person shall send a report assessing the implementation of internal rules to the competent archival institution.

Article 11

(Qualifications of internal assessors)

(1) Internal assessors shall demonstrate professional qualifications in the records' management, archival science, information infrastructure and security, and shall at least:

- have attained the level of education under the Bologna first-cycle study programmes or study programmes corresponding to the Bologna first-cycle degree;
- have two years of work experience in the field to be assessed;
- have passed the professional competence test at the National Archives, which is laid down in the Rules regulating professional qualifications for work with records;
- have completed training on the quality system.

(2) The internal assessment of the implementation of internal rules may also be performed by internal assessors who have attained the level of secondary school education, have at least five years of experience in the field to be assessed, and fulfil requirements referred to in indents three and four of the preceding paragraph.

(3) The National Archives shall provide additional training for internal assessors verifying the implementation of internal rules at least once a year. Internal assessors shall be obliged to take part in additional training once in two years. The first additional training shall be attended two years after the passing of the professional competence test referred to in indent three of paragraph one of this Article.

Article 12

(Responsibilities for implementing internal rules)

(1) In internal rules a person determines work posts that are related to the performance of procedures or services. General, specific and security requirements shall be defined for such work posts.

(2) The work posts referred to in the preceding paragraph may also be defined by determining the roles and related responsibilities for the implementation of internal rules. For each role, internal rules shall determine the method of assigning the role (e.g. an act regulating the organisation and systematisation of work posts, a decision, a contract) and define the general, specific and security requirements to be fulfilled by the responsible person who will assume those responsibilities.

(3) In accordance with the risk assessment, the person shall ensure that tasks are divided in such a manner so as to enable individuals to access the information they need, while preventing undetected misuse of the information to which they have access.

Article 13

(Access to information assets)

With respect to each work post or role, related to the performance of procedures or services, the person shall determine in internal rules information asset to which the employees will have authorised access in their workplace.

Article 14

(Qualifications of employees of entities under public law and employees of service providers)

(1) With respect to all employees of entities under public law and employees of service providers who are involved in the performance of procedures or services, a person shall specify in internal rules the required professional qualifications and further training to maintain the required qualification level.

(2) For the purpose of ensuring the qualifications referred to in the preceding paragraph and transparency of assignments, internal rules shall determine responsible persons and the manner of documenting professional qualifications.

3. General provisions relating to work procedures for capture, digital preservation and accompanying services

Article 15

(Description of procedures for capture, digital preservation or accompanying services)

(1) Internal rules shall contain the provisions laying down the performance of procedures or services. These provisions shall ensure the accessibility, usability, integrity, authenticity and sustainability of captured and preserved records.

(2) All procedures which are regulated by internal rules shall be specified in these rules, such as:

1. the conversion of records from physical to digital form (digitisation),
2. the conversion of records from physical or digital form to microfilm (microfilming),
3. the conversion of records from one digital form to another,
4. other forms of conversion as defined in Article 15 of the Decree,
5. the capture of digitised records and pertaining metadata into the information system,
6. the preservation of digital records,
7. the selection of archival records,
8. the submission of archival records to the competent archives,
9. the elimination and destruction of records,
10. the transfer of records between information systems.

(3) Each description of the procedure referred to in the preceding paragraph shall clearly specify:

- the purpose of the procedure and the scope of individual activities within the procedure,
- the responsible person who directs and supervises the procedure,
- the activity providers involved in the procedure and their responsibility,
- the criteria for determining the effectiveness of the procedure and any conditions for initiating the procedure,

the activities to verify the effectiveness of the procedure and possible elimination of identified errors, and the responsible person for each activity.

Article 16

(Registering of records)

(1) Records shall, as a general rule, be registered at the time of their creation or upon receipt, but at the latest at the time of their capture in the information system or their conversion into digital form.

(2) A person shall define the registers to be kept for those records that are captured and stored in accordance with internal rules.

(3) Register data shall be determined for each register of records in the information system. The register of records shall contain at least the following register data:

1. the unique identification code;
2. the date and time of creation or receipt,
3. the retention period,
4. the title or brief description of the contents of the records,
5. the name of the entity (author, sender or recipient).

Article 17

(Classification of records)

(1) A person shall define in internal rules the procedures for the classification of records, which are based on the classification plan.

(2) The record classification plan shall be an integral part of the internal rules. For different types of records different plans may be used.

(3) The classification plan referred to in paragraph one of this Article shall form the basis for the records classification and shall consist of classes. The classification plan and its content may be defined by sectoral regulations (e.g. the classification code plan in the Decree regulating administrative operations) or may be prescribed by the head of the organisation.

(4) An administrator of the record classification plan shall be designated.

Article 18

(Determining the retention period of records)

For each record unit that is subject to registering, a retention period shall be determined at the latest at the end of the registering, in accordance with the record classification plan.

4. Metadata

Article 19

(Mandatory metadata)

(1) For each type of records, internal rules shall specify a list of mandatory metadata and the manner of their entry (automatic, manual).

(2) The metadata referred to in the preceding paragraph shall be captured in the register of records.

Article 20

(Mandatory metadata of the service provider)

(1) A service provider shall determine by internal rules the types of records for which the service is provided and a minimum set of metadata to be captured or preserved for each type of records.

(2) The metadata referred to in the preceding paragraph shall be included in the register of records defined by internal rules for the provision of services.

Article 21

(Metadata for textual and combined records)

The minimum set of metadata in the register of textual and combined records shall be:

1. the unique identification code;
2. the title or short content description,
3. the date (receipt, creation),
4. the retention period,
5. an indication of the entity (author, sender or recipient).

Article 22

(Audio records)

(1) The minimum set of metadata in the register of audio records shall be:

1. the unique identification code;
2. the title or short content description,
3. the time of creation or date of recording,
4. the retention period,
5. an indication of the producer, recorder or external contractor, where this is not the creator of these records,
6. the original format,
7. the original duration or time of playback,
8. the type of medium when a portable medium is in use.

(2) The minimum sufficient requirements shall be laid down for the following characteristics of audio records:

- the sampling frequency,
- the bit rate.

(3) When audio records have the characteristics of archival records, metadata relating to the characteristics referred to in the preceding paragraph shall be captured and preserved, but not necessarily in the register of records.

Article 23

(Metadata for the film and audio-visual records specified in Article 43 of the Act)

(1) The minimum set of metadata in the register of film and audio-visual records specified in Article 43 of the Act shall be:

1. the unique identification code;
2. the title;
3. a short content description,
4. the year of creation,
5. the retention period,
6. the format (codec),
7. the length (in minutes),
8. the frame size, frame ratio, number of images per second,
9. the source language,
10. the producer,
11. the data rate,
12. the colour subsampling,
13. other responsible persons (director, screenwriter, cameraman, main actors), if there are any.

(2) For the film and audio-visual records referred to in the preceding paragraph the following data and the quality of the records shall be determined:

- the wrapping and version,
- the sampling frequency,
- the minimum bit rate.

(3) When film and audio-visual records have the characteristics of archival records, the data shall be captured and preserved, but not necessarily in the register of the records.

Article 24

(Metadata for other film and audio-visual records)

(1) The minimum sufficient set of metadata in the register of other film and audio-visual records shall be:

- the unique identification code;
- the title or short content description,
- the date and time of creation,
- the retention period,
- the format and codec.

(2) The quality of the recording for film and audio-visual records referred to in the preceding paragraph shall be determined by:

- the sampling frequency,
- the bit rate.

(3) When film and audio-visual records have the characteristics of archival records, the data referred to in the preceding paragraph shall be captured and stored, but not necessarily in the register of the records.

5. Websites

Article 25

(Need for the capture and digital preservation of websites and registering)

The entity under public law that publishes records on the website (internet, intranet) and has recognized the need to register and store them shall document:

- the structure of the websites (map),
- the information on which websites or subsites the records are published.

Article 26

(Capture of metadata on website contents into the register)

(1) The structure of the websites referred to in the preceding Article shall be documented with at least the following metadata:

- the title or short content description,
- the composition (in the case of more complex contents consisting of multiple sources or types of records),
- the period of publishing,
- the identifier of published content (subsites) that uniquely and permanently identifies an object in the structure of websites (e.g. URN).

(2) The entity under public law shall for each website or subside containing archival records in its internal rules related to the capture determine the following:

- the frequency of capture;
- the format and scope of records, which, in addition to content preservation, will also enable the preservation of the display, functionality and structure to the largest extent possible, however, in accordance with the purpose of digital preservation;
- a description of the capture and digital preservation operations;

- the responsible persons and their tasks related to the capture and digital preservation of these records.

6. Electronic mail

Article 27

(List of e-mailboxes for capture and digital preservation)

(1) A person who captures and stores e-mail shall compile a list of e-mailboxes with contents having the characteristics of records.

(2) The list of e-mailboxes referred to in the preceding paragraph shall contain at least the following information:

- the source (e-mailbox or parts thereof, e.g. folders),
- the format of the record,
- capture method (manual, automatic),
- the scope of metadata required for keeping the register and ensuring integrity, usability and authenticity,
- the persons responsible for capturing and preserving the content of e-mailboxes and their responsibilities.

(3) The procedures for the capture and storage of the e-mail content shall be defined in accordance with the general requirements for the procedures' descriptions referred to in paragraph three of Article 15 of these Rules.

(4) If the mailbox referred to in paragraph two of this Article ceases to be used, the contents which are the subject of capture and digital preservation shall be converted immediately into the form for long-term preservation.

Article 28

(Register of captured e-mails)

(1) If the internal rules are used to regulate the capture and digital preservation of e-mails, they shall also be used to regulate the keeping and scope of the register of the captured e-mails. A person may also keep the register by capturing the content of electronic messages in the electronic records management system.

(2) In addition to the contents of the message in the electronic records management system the person keeping the register referred to in the preceding paragraph shall also capture metadata from the message header.

(3) The register referred to in paragraph one of this Article shall include at least the following metadata from the message header:

1. the address of the recipient of an electronic message (addressee of a message, the "To" field in the message header),
2. the address of the recipient of an electronic message (for information, the "cc" field in the message header),
3. the address of the reply recipient (the "From" field in the message header),
4. the address of the sender of an electronic message (the "Sender" field in the message header),
5. the title/subject of an electronic message (may also be the "Subject" in the message header),
6. the date and time of the electronic message (the "Date" field in the message header).

7. Databases and official registers

Article 29

(Common requirements for databases and official registers)

(1) With internal rules the person shall regulate the management of databases and official registers. For this purpose, the person shall compile a list of all databases and official registers. Each database shall be documented at least with the following:

- a description of the technical environment,
- a description of the data structure, including data model and code lists,
- data sources at the level of the user interface entry fields for entering or editing data,

- a description of the terms used (semantics),

in order to ensure that the information may be used at a later stage outside the original environment.

(2) Changes to the technical environment in which the database and official register or data structures are located shall be documented with at least the following:

- descriptions of changes,
- the implementation plan for changes (including a plan of testing and verifying the integrity and regularity of the implementation),
- justification for any deletion or omission of the transfer of the selected data,
- documented evidence of implementation in accordance with the change implementation plan.

Article 30

(Additional requirements for entities under public law regarding official registers)

(1) For the official registers of entities under public law, any change in the value of data shall be documented. If the data value changes, the old value shall be retained in such a manner that the previous value can be viewed at a given date. By providing supplementary professional and technical instructions, the competent archival institution may limit the selection of data for which old values should be preserved.

(2) For the official registers of entities under public law, the legal bases used in the management of individual official registers shall be documented. This shall include all regulations, including internal ones, governing this management, including their amendments.

Article 31

(Additional requirements for entities under public law regarding official registers – notification to a competent archival institution)

(1) The official register manager shall notify the competent archival institution in writing of the intended change in the data model for official registers at least ten working days prior to its entry into force, in order to obtain supplementary instructions.

(2) The official register manager shall notify the competent archival institution of any changes in the data structure within one month of the change taking effect.

(3) Based on the notification referred to in paragraph one of this Article, the competent archival institution shall supplement written professional or technical instructions for the selection of archival records.

8. Electronic records management system

Article 32

(Use of the electronic records management system for registering and managing records)

(1) Persons using the electronic records management system (hereinafter: ERMS) to register and manage records in electronic or physical form shall determine, by way of internal rules, the business functions (e.g. registering, content classification, e-mail capture, access rights management) they perform with the ERMS assistance.

(2) Persons regulating the management of records with internal rules shall determine the implementation of individual procedures for records management (e.g. registering, classification, elimination, destruction) in accordance with paragraph three of Article 15 of these Rules. Where the management of records is governed by a regulation (e.g. the Decree on administrative operations, the Rules of Court), the internal rules may refer directly to this regulation.

Article 33

(Spatial data documentation)

(1) A person shall keep a register of spatial data. The spatial data register shall keep information on spatial data and online services relating to them.

(2) Archival spatial data shall be registered in the spatial data register at least with:

1. the metadata on data in a standardised format (e.g. based on the Act governing the infrastructure for spatial information (hereinafter: ZIPI) and the Directive establishing an infrastructure for spatial information in the European Community (hereinafter: the INSPIRE Directive);
2. a coordinate system and projection;
3. a description of the spatial data structure, including the definition of spatial data attributes, data model and code lists;
4. the organisation of data into spatial layers, time series and other objects and structures, if they exist;
5. the visualisation rules or a definition of cartographic display, if they exist;
6. the source of spatial data (information on the source of the downloaded data, the methodology of creation or capture, the time of capture, spatial extent and spatial accuracy);
7. the time period of the validity of individual spatial data, which must make it possible to determine the state of the data for any time in the past.

(3) Each of the online spatial services relating to archival spatial data shall be registered in the register at least with the following:

1. a list of spatial data included in the service;
2. the application scheme of the service, if it exists;
3. the metadata on service in a standardised form (e.g. based on the ZIPI and the INSPIRE Directive);
4. the coordinate system and projection;
5. a description of the rules for displaying information, which includes the production of cartographic (e.g. display styles) or descriptive information;
6. a description of the logic for processing or converting basic data into derived spatial data;
7. the time period of the service validity, which must make it possible for the state of the service to be determined for any time in its past.

Article 34

(Requirements for the Geographic Information System)

(1) The documentation on the Geographic Information System (GIS) shall contain at least the following information:

- a description of the system (the software tool or solution name, version, data on the database used, if any);
- the list and method of organising spatial data in the system (as provided in the preceding Article);
- a description of the logic for processing or converting basic data into derived spatial data.

(2) A person shall regulate by internal rules the documenting of changes to GIS or parts thereof (e.g. databases, a coordinate system) with at least the following:

- a detailed description of the changes,
- a change implementation plan (also includes a plan for testing and verifying the integrity and regularity of implementation),
- justification for any deletion or omission of the selected data transfer,

evidence of the implementation of changes to GIS or parts thereof in accordance with the change implementation plan.

10. Conversion of records into record format for long-term preservation

Article 35

(Valid long-term digital preservation formats)

(1) Internal rules shall define the valid formats used by a person to secure the long-term digital preservation of individual types of records the management of which is regulated by internal rules.

(2) The selected formats for long-term digital preservation shall meet the general requirements referred to in Article 42 of the Decree. The National Archives shall compile, keep and publish on its website a list of the most commonly used formats suitable for long-term preservation of individual types of records.

Article 36

(General definition of the conversion procedure)

Internal rules shall define the procedure for the conversion into a long-term digital preservation format, including:

1. the scope of the records to be converted;
2. the registration and tagging with metadata from the register of records;
3. long-term digital preservation formats for individual types of records in digital form;
4. format conversion software (converter): name, version, manufacturer;
5. software for conversion verification and validation (validator): name, version, manufacturer;
6. defined procedure phases: design, test, conversion, verification and validation of conversion (criteria and method of verifying the correctness and suitability of record conversion), approval;
7. measures in the event of established irregularities.

Article 37

(Person responsible for conversion and related tasks)

(1) Internal rules shall determine the person responsible for converting the records into long-term digital preservation formats.

(2) The person responsible for carrying out the conversion shall be responsible for at least the following:

- the monitoring of valid long-term digital preservation formats for individual types of records,
- the timely conversion of the records into a new format,
- the planning and execution of all phases of record conversion,
- the documentation of the entire conversion procedure,
- cooperation with an outsourced contractor responsible for the conversion.

(3) When a service provider converts records into a long-term digital preservation format, the contracting authority shall designate in its internal rules the person responsible for cooperating with the contractor and is responsible for the timeliness and adequacy of the conversion. The service provider shall, in its internal rules, define cooperation with the contracting authority's responsible person.

Article 38

(Conversion and capture records originally created in physical or analogue form – digitisation)

Internal rules shall establish the procedures for the conversion and capture of records originally created in physical or analogue form (digitisation), which shall include at least the following:

1. criteria for the selection of records, taking into account the size of the records, their condition, quantity and the frequency of use;
2. a review of the records;
3. the registering of all units of records irrespective of the format or medium, mode of creation, and other technological features;
4. the preparation of records that comprises:
    a) arrangement of records, page numbering or checking the numbering,
    b) the cleaning, removal of staples and adhesive tapes,
    c) restoration procedures (if necessary),
    d) classification (by content, chronological order, series),
    e) the drafting of technical instructions for digitisation (checklist),
    f) the transcription of illegible text (if possible),
    g) the preparation of metadata and data wrapping;
5. the proper conversion and capture of the content of records in digital form, which:

a) encompasses all key content-related data;
b) captures or creates all necessary metadata, including the data providing the integrity (intactness of contents), authenticity (provability of connection of reproductions with the content of original records and/or their origin) and applicability of records (enabling complete interpretation of data as reasonable information with the possibility of identifying the units of records), and provides for the strictly controlled and documented addition of such data,
c) encompasses added content-related and technical metadata that are clearly separated, saved and indicated differently from the original data and all significant notes and data on the capture procedure and originals;

6. the digitisation process to ensure:

a) digitised records with a minimum of 300 dpi,
b) digitised records with a minimum of 600 dpi for the records smaller than A6 (148 x 105 mm) or having a font size equal to or smaller than 5 pt,
c) digitised records with a minimum of 600 dpi for pictorial materials,
d) depending on the type of digitisation, the 8-bit colour depth for grayscale digitised image and the 24-bit colour depth for colour digitised records,
e) the formats of digitised records for long-term digital preservation that are published by the National Archives on its website,
f) digitised records at least in target resolution, but not created by means of interpolation,
g) digitised records, where resolution is not changed during format conversion,

7. the automatic or manual control of the proper digitisation to eliminate errors or deviations,

8. the registering of digitised records; and

9. the storage of a sufficient quantity of documentation to prove that the applied tools, methods and procedures of digitisation provide for reliable capture in digital form.

Article 39

(Conversion of records to microfilm)

For the needs of long-term preservation, the procedure of conversion to microfilm shall comprise at least the following:

1. the selection and examination of the records to be converted to microfilm,

2. the registering of all units of records irrespective of the original format or medium, mode of creation, and other technological features;

3. the preparation of records, which encompasses:

a) the removal of wrappers, untying (if necessary),
b) the arrangement of records, page numbering or checking the numbering,
c) the cleaning, removal of staples and adhesive tapes,
d) restoration procedures (if necessary),
e) classification (by content, chronological order, series),
f) drafting technical instructions for microfilming,
g) the transcription of illegible text (if possible),
h) the preparation of baseline records,
i) drafting a detailed description of the content,
j) the preparation of metadata and data wrapping;

4. the determination of:

a) microfilm types (e.g. silver halide, vesicular, diazo),
b) the format (e.g. 16 mm, 35 mm),
c) recording equipment (e.g. step-and-repeat or traditional cameras, continuous flow/rotary or production cameras, special cameras, output computer technology or COM),
d) technical data (e.g. image reduction rate, resolution and re-enlargement, density);

5. the processing of images;

6. the automatic or manual control of the proper conversion to microfilm to eliminate mistakes or deviations; (e.g. checking the density and resolution, the sharpness and resolution of the image, the correctness of recorded records and accompanying data, the correct sequence of records);

7. a review of the metadata (technical and content-related);

8. the provision of adequate storage for microfilms, including at least:

   a) physical storage (e.g. correct loading onto the reel, appropriate technical protection),
   b) micro-climate conditions (temperature, relative humidity),
   c) the cleaning of equipment,
   d) the storage place,

9. the storage of a sufficient quantity of documentation to prove that the applied tools, methods and procedures of conversion to microfilm ensure the preservation of the integrity and authenticity of the contents of the converted records.

Article 40

(Conversion of official registers and other conversions)

(1) The provisions of the Articles of this sub-chapter and the professional-technical instructions of the competent archival institution shall apply *mutatis mutandis* to other conversions and to the conversions of specific records from specific fields (e.g. public registers, images, spatial data).

(2) The conversion of official registers to a long-term preservation format shall be mandatory when:

- the keeping of the register ends,
- the keeping of the register is changed,
- in the phase of preparing the register for submission to the competent archival institution, or
- this is required by professional-technical instructions of the competent archival institution.

Article 41

(Additional requirements for service providers)

(1) Prior to converting records to a digital form or microfilm, a service provider shall obtain information about the records from the contracting authority's register of records.

(2) If the contracting authority does not have an established register of the records to be converted, the service provider shall obtain the contracting authority's detailed instructions and the necessary metadata to establish a register of the converted records.

11. Selection and submission of archival records in digital form and cooperation with a competent archival institution

Article 42

(Selection)

(1) An entity under public law or a selection service provider shall specify by internal rules the procedure for selecting archival records in digital form in accordance with written professional and additional professional-technical instructions provided by the competent archival institution.

(2) The selection procedure shall be regulated by internal rules in accordance with paragraph three of Article 15 of these Rules.

Article 43

(Submission)

(1) An entity under public law shall regulate by internal rules the procedure for the submission of archival records in digital form to the competent archival institution on the basis of written professional-technical instructions issued by the competent archival institution.

(2) The submission procedure shall be regulated by internal rules in accordance with paragraph three of Article 15 of these Rules.

Article 44

(Content of professional-technical instructions)

(1) Professional-technical instructions, which must be issued no later than at the beginning of the selection of archival records in digital form, shall determine the scope of the records to be submitted, the conditions for the protection of records until they are submitted to the competent archival institution, the procedure and manner in which the records are submitted, and the formats and media of the records.

(2) The scope of archival records and supporting documentation shall be determined by professional-technical instructions in a manner that specifies the content of records, data and associated metadata, which, as a whole, enable the long-term preservation of the content of archival records in terms of their integrity and usability.

(3) The procedure for preparing archival records for submission shall be specified by professional-technical instructions in a manner that includes the selection, possible conversion of the records to other formats, the submission or export of records from the source information environment, and other procedures until a submission information package for the purpose of submitting the records to the competent archival institution and documenting the aforementioned activities is prepared. The professional-technical instructions shall also specify the obligation to inform the competent archival institution of the implementation of all those activities.

(4) The content-related and technical arrangement of the archival records to be submitted to the competent archival institution shall be defined by professional-technical instructions in the manner that at least specifies the structure of the submission information package, which shall include the arrangement of the basic content, supporting documentation and metadata.

(5) The professional-technical instructions shall specify the authorised and/or unauthorised formats of records in the submission information package or parts thereof.

(6) The professional-technical instructions shall also determine the media of records and the manner in which the submission of the submission information packages to the competent archival institution shall be made.

(7) The professional-technical instructions shall determine the procedure and method of submitting the records to the competent archival institution so as to:

- ensure that the competent archival institution is informed about the intention of submitting the records;
- enable the content of the professional-technical instructions to be amended or supplemented due to their obsolescence, substantive deficiencies or definition of details immediately prior to submitting archival records in digital form;
- enable the use of certain software tools to support the preparation of the submission information package and other activities to maintain the integrity, authenticity and usability of the records.

(8) The professional-technical instructions may also determine how frequently the submission information packages are to be created and submitted to the competent archival institution.

12. Elimination and destruction of records with expired retention periods

Article 45

(Procedure for the elimination and destruction of records with expired retention periods)

(1) A person shall define by internal rules the procedure for the elimination and destruction of records in digital form with expired retention periods in accordance with paragraph three of Article 15 of these Rules.

(2) The procedure referred to in the preceding paragraph shall determine the criteria in accordance with which the elimination and destruction of the records shall be carried out.

(3) The destruction of the records shall be documented by minutes as laid down in Article 26 of the Decree.

(4) The minutes referred to in the preceding paragraph shall be kept permanently.

Article 46

(Additional requirements for entities under public law)

An entity under public law with an obligation to notify the competent archival institution about the intended destruction of records with expired retention periods (as defined in the written professional instructions referred to in Article 34 of the Act) shall include this obligation in its internal rules.

13. Ensuring the integrity and authenticity of records

Article 47

(Technological means to preserve the integrity and authenticity of records)

(1) A person shall specify by internal rules the technological means to ensure that the integrity and authenticity of records are preserved for the entire period of the preservation of records in digital form (e.g. fingerprint, hash value, electronic signature, time stamp).

(2) A person shall adopt organisational measures to specify the use of technological means to ensure the integrity and authenticity of records.

Article 48

(Verification of the electronic signature validity)

A person who captures and preserves records that are originally born digital shall verify their validity when capturing records that contain an electronic signature. The validation data shall be added as metadata to the document so that the validity of the electronic signature in the further handling of records no longer needs to be verified.

14. Business continuity

Article 49

(Creation of backup copies)

(1) In order to protect the records in digital form against loss or damage, a person shall further specify a backup policy for these records.

(2) The frequency of backup shall be determined on the basis of a risk assessment.

Article 50

(Storage of backup copies and responsibility)

(1) A person in a remote location (secondary location – address and place) shall, in addition to a backup copy of the records, also store other data (e.g. a copy of the user software and pertaining instructions) needed to restore the records stored in digital form.

(2) The backups referred to in the preceding paragraph shall be kept by the person according to the findings of the risk assessment in a remote location which is not in the same flood or seismic zone as the main location. The findings referred to in Article 57 of these Rules shall be taken into account.

(3) The person shall establish a procedure for regularly transferring the backup copies to a remote location and designate the persons responsible for doing so.

Article 51

(Additional requirements for entities under public law and digital preservation providers)

(1) An entity under public law and a digital preservation service provider that store public archival records in digital form shall ensure the storage of the backups referred to in Article 49 of these Rules that are necessary for the renewal of the digital preservation system in at least two geographically remote locations (address and place) which must not be in the same flood or seismic zone, nor in the same flood or seismic zone as the main storage site. The findings referred to in Article 57 of these Rules shall be taken into account.

(2) In the event of service termination, the digital preservation service provider shall ensure the export of stored records and all accompanying metadata and audit trails, which allow the contracting authority to preserve the integrity and authenticity of records.

Article 52

(Data recovery plan)

(1) A person shall draw up a plan to restore the data of the digital preservation system and designate its administrator. The plan shall include at least the following information:

- who can access and how they can access backup copies in remote locations,
- the procedure for setting up a digital preservation information system,
- the procedure for the use of backup copies for the possible restoration of the records,
- guidance on the mandatory documenting and storage of this documentation when recovering the data,
- the accessibility of the plan in case of system failure.

(2) The person shall test the data recovery plan or parts of it in accordance with the risk assessment at least once a year.

Article 53

(Business continuity plan)

(1) An entity under public law or a digital preservation service provider storing archival records shall, in addition to the data recovery plan, also draw up a business continuity plan for the digital preservation system (hereinafter: business continuity plan).

(2) The business continuity plan referred to in the preceding paragraph shall include at least the following information:

1. data on the main (primary) and remote (secondary) digital preservation locations (organisation, address, place, telephone);
2. rules on access to all digital preservation locations;
3. a description of remote locations: area (location data), communication links (telephone), physical and technical measures put in place (e.g. built-in motion sensors, alarm system, fire protection sensors, burglary-resistant doors, video surveillance), key hardware and software data (e.g. manufacturer, model) if installed in the room;
4. competences and responsibilities (of the responsible person) regarding the initial response to events that result in a major disruption or interruption of the digital preservation system or its essential operating procedures;
5. basic data on persons responsible in a crisis situation and their contact details with the method of communication (name and surname, work number, mobile number, main e-mail address and possible backup e-mail address);
6. data on external public emergency services (e.g. firefighters, emergency responders, police, insurance companies) and their contact details;
7. the listed critical business processes or tasks that are ranked by the necessity of being set up for the operation of the digital preservation system, and an action plan for their establishment;
8. the list of key equipment suppliers and contractors and their contact details;

9. the manner in which employees address and are informed of the plan (e.g. internal meetings, internal training or education, emergency simulations at least once a year);
10. the method of communication with colleagues and business partners in case of an emergency (in person, by telephone, mobile phone, e-mail);
11. the data recovery plan referred to in the preceding Article;
12. the method of checking the business continuity plan (responsible persons, timing).

(3) The digital preservation service provider shall, in addition to the backup copy of the records and other data required for the recovery of the records stored in digital form, also provide the replacement information infrastructure of the digital preservation system at a remote storage location, the availability of which enables the contracting authority of the digital preservation to be provided with a contractual storage volume and access to the stored records during the contract period.

(4) If the plan is set in motion, all procedures carried out shall be accurately documented and stored in order not to jeopardise the authenticity and integrity of records.

Article 54

(Acquaintance with the plan, testing and updating)

(1) All employees involved in the implementation of the activities in the plan shall be properly trained and fully informed of their roles and responsibilities regarding the implementation.

(2) The plan shall be tested at least once a year to the extent determined by the person concerned in accordance with the risk assessment.

(3) The plan shall be updated whenever there is an organisational change, change of personnel or change in the information system affecting it. In this case, the plan shall be retested to the appropriate extent.

15. Separation of individual organisations' records

Article 55

(Provision of measures to separate stored records)

A service provider shall put in place appropriate measures to separate records in digital form pertaining to individual organisations for which it provides the services.

16. Responsibility for information security

Article 56

(Person responsible for information security)

A person shall appoint a person responsible for information security (a chief information officer) and assign their responsibilities and duties.

17. Risk assessment and risk management plan

Article 57

(Responsibility and basic components of risk assessment)

(1) A responsible person shall be appointed who, on the basis of a documented and accepted methodology, produces and maintains a risk assessment, which identifies and manages risks that jeopardise the accessibility, usability, integrity and authenticity of the records in digital form.

(2) The basic components of the risk assessment shall be as follows:

1. an inventory of information assets (by group) and their administrators,
2. threats identified for individual groups of information assets,
3. vulnerabilities identified for individual groups of information assets,
4. an assessment of probability and damage (effect on records in digital form), if the threat arises,
5. an assessment of the degree of risk; and
6. the evaluation and assessment of acceptable risk levels (acceptable, unacceptable).

(3) The risk assessment shall include the risks associated with the record storage locations in view of seismic and flood threats. The data on flood and seismic risks areas, which are published in the Intensity Map (EMS-98) on the websites of the national authority responsible for the environment and spatial planning shall be taken into account.

(4) A person responsible for risk management (hereinafter: risk management officer) shall maintain a risk management plan determining a risk administrator for each identified risk, measures to manage the risk (reduction or elimination) and shall also monitor the deadlines for the introduction of measures.

(5) The risk assessment shall be documented and maintained as part of internal rules.

Article 58

(Updating of the risk assessment and risk management plan)

The risk management officer shall ensure that the risk assessment and the risk management plan are updated at least once a year and in case of risk changes to reflect the actual situation.

18. Physical and technical protection of premises and equipment

Article 59

(Determining the premises for the performance of procedures or services and their protection)

(1) Internal rules shall determine the premises to ensure the safe performance of procedures or services (protected area) in accordance with the importance of the information sources (records and equipment) in the area concerned.

(2) Security measures and procedures for the protection against unauthorised access and environmental threats (e.g. fire, spillage or intrusion of water, sudden changes in temperature or humidity, smoke, dust) shall be established and implemented for secured areas.

Article 60

(Rules on entering premises intended for the performance of procedures or services)

(1) A person shall accept and observe the rules of entry into secured areas, which apply to both employees and other persons (e.g. contractors).

(2) The entry of employees and other persons into the secured area shall be registered (manually or automatically) in accordance with the risk assessment, while the records shall be regularly reviewed by the persons responsible for individual secured areas.

19. Management of rights to access the system and records

Article 61

(Procedure for assigning, changing and revoking access rights)

(1) The procedures for assigning, changing and revoking rights to access information assets or records shall be specified and documented.

(2) The rules for assigning usernames with pertaining passwords or other identifiers shall be determined. The unique identification of all users must be ensured.

(3) A person responsible for managing the access rights shall be designated.

(4) The access right may be granted to a user or user group on the basis of the application which should contain at least the following:

1. the date of applying for the assignment or revocation of an access right;
2. data on the applicant (e.g. a head of the internal organisational unit, a project manager);
3. the justification and explanation of the application;
4. the data on the user to whom rights will be assigned or revoked;
5. the area, information subsystem (user solution) or records to which the user obtains access;
6. the method of access and the type of access right (e.g. reading, modification, deletion);
7. data on the administrator of the asset to which the application for access refers;
8. data on the person who granted the application (responsible person or administrator of the content of information asset);
9. data on the person who processed the application;
10. the date of granting access rights.

(5) The persons responsible for managing access rights to various information assets shall keep an up-to-date register of their management, including at least:

- requests for the assignment or revocation of user rights; and
- a list of access rights to systems for individual users.

(6) In order to verify and update access rights on a regular basis, the control of access to the information system and records (the process of reviewing users' access rights) shall be established.

Article 62

(Password policy)

When using passwords to access the information system and records a person shall, for this purpose, lay down the rules for their management, covering at least the following:

- the mandatory password composition,
- the timing and procedure for changing passwords regularly; and
- the procedure for the first and, if necessary, further delivery of passwords to users.

20. Audit trail

Article 63

(Scope of audit logs)

(1) For logging access to the digital preservation information system, the minimum scope of audit logs and retention periods shall be determined.

(2) The scope of audit logs and their retention period shall be determined for all types of stored records in digital form.

(3) The scope of audit logs shall cover at least when, by whom and what changes were made on individual information assets. The storage of audit logs in the records shall not include tracing all corrections made to the draft record unit.

Article 64

(Audit logs administration)

(1) Internal rules shall determine:

- the administrator for audit logs management (settings, method of processing and use),
- persons authorised to have access to audit logs records.

(2) Internal rules shall determine the manner of transferring the audit logs administration together with records (e.g. when an organisation transfers the records to another organisation).

21. Protection against malware and intrusion

Article 65

(Protection against malware and intrusion)

To protect against malware and intrusion, rules shall be laid down, which include the procedures for:

- protecting servers and workstations,
- installing and updating security software or hardware,
- verifying the operation of the security; and
- taking action in the event of infection with a virus.

22. System clock synchronisation

Article 66

(System clocks synchronisation)

In the entire computer and network infrastructure of a person the system clocks synchronisation shall be provided and described.

23. Security incident management

Article 67

(Procedure and person responsible for security incident management)

(1) The procedure and the person responsible for security incident management shall be determined. This includes identifying, reporting, registering, processing (analysing), documenting, and responding to incidents.

(2) The procedure shall also include securing and storing audit and other logs that may be useful in the procedures for responding to individual security incidents.

(3) The register referred to in paragraph one of this Article shall contain at least the following information:

- the type of incident,
- the date, time and location of incident,
- the cause of incident,
- measures taken in response to the incident (who, when and how the measure was taken).

Article 68

(Additional requirement for service providers)

In internal rules, service providers shall define the possibility for the contracting authority to access the premises where their records are processed and to examine audit and error logs created during the provision of services relating to those records.

24. Information technology equipment and infrastructure

Article 69

(Electrical and telecommunication installation)

Electrical and telecommunication installation shall be installed in such a manner that they cannot be inadvertently interrupted, unimpededly destroyed or misused.

Article 70

(Inventory of information assets)

(1) A person shall draw up and maintain a list of all relevant information assets or groups of the same information assets involved in the performance of procedures or services.

(2) For each information asset (or a group), a responsible person shall be appointed for the use or treatment of the assets in accordance with the prescribed or contractually specified requirements, rules and standards.

(3) An information asset (or a group of information assets) containing confidential data shall be subject to a security classification in accordance with the risk assessment, its criticality and sensitivity, and marked in accordance with internal acts and the regulations governing the management, processing and the use of individual types of classified data.

(4) Confidential data referred to in the preceding paragraph are data protected by the law (e.g. personal data, business secrets, confidential data under the act governing banking, classified information).

Article 71

(Hardware)

(1) Internal rules shall determine the manner and responsibilities related to the keeping of the list of hardware which is essential for the performance of procedures or services.

(2) The list of the hardware referred to in the preceding paragraph shall contain for each individual piece of hardware at least the following information:

- the type of hardware,
- the manufacturer,
- the series or model.

(3) Supporting communication and hardware equipment shall be installed under the conditions prescribed in the technical and user documentation of the hardware used.

(4) A person shall provide and maintain technical and user documentation for the hardware in use.

(5) Hardware for the capture and digital preservation of archival records and related accompanying services shall be certified by the National Archives.

Article 72

(Long-term digital preservation medium)

(1) A person shall specify the media to be used for long-term digital preservation.

(2) The medium shall comply with the conditions referred to in Article 43 of the Decree.

(3) The person shall ensure that the media are stored and used in a stable environment.

(4) Occasionally, but at least once a year, the quality of the recording on the media shall be checked for signs of deterioration, with replacements made, if necessary, before the recordings become unusable or before the end of their life expectancy.

Article 73

(Software)

(1) To perform procedures or services, a person shall use software that is classified as a single functional type according to the provider-contracting authority relationship and the functionality as defined in these Rules.

(2) Internal rules shall specify the manner and responsibilities for maintaining the list of software essential for the performance of procedures or services.

(3) The list of software referred to in the preceding paragraph shall contain, for each software, at least the following:

- the identification code or name,
- the commercial code of the software version,
- any additional components of the software, including the versions that make up the software, provided that they contribute to its functionality in accordance with the requirements of these Rules.

(4) The software used to capture or store archival records in digital form or accompanying services shall be certified.

Article 74

(Development or purchase of software)

(1) A person shall adopt a documented methodology for software development, if such a development takes place, to perform procedures or services.

(2) Prior to being used in the production environment, the software shall be checked or tested by a documented verification procedure, whereby, in addition to functionality, safety data shall also be verified.

(3) The person shall ensure that the production environment is separated from the environment intended for development and from the environment for testing.

(4) If data from the production environment are used in the development and testing process, confidentiality shall be protected with the same degree of care as it is protected in that environment. After use, the test data shall be appropriately destroyed.

(5) The person shall provide and maintain technical and user documentation for all software in use.

(6) In the case of own software development, the person developing such software shall be subject to the same certification requirements as the software provider.

25. Change management

Article 75

(Management of changes to the information equipment and infrastructure)

(1) A person shall specify and document the change management process which ensures that all changes (e.g. upgrades, maintenance) to existing information equipment and infrastructure are made in a controlled manner and verified prior to use.

(2) The change management process shall include at least: an application for change, impact assessment, approval, testing and introduction.

Article 76

(Additional requirements for digital preservation service providers)

(1) Digital preservation service providers shall keep the register of procedures in connection with the infrastructure and interventions in it that affect the reliability of storage.

(2) The records referred to in the preceding paragraph shall be kept for at least five years.

Article 77

(Additional requirements for the storage of archival records outside the competent archival institution)

When the storage of archival records in digital form is provided outside the competent archival institution, internal rules shall determine the responsible persons and their responsibilities for the performance of tasks defined in Article 46 of Decree.

26. Maintenance of information equipment and infrastructure

Article 78

(Maintenance of the information equipment and infrastructure)

(1) Support to and maintenance of information equipment (hardware, software) and infrastructure for the performance of procedures or services shall be provided in an appropriate response time.

(2) Responsible persons for regular maintenance shall be appointed.

(3) All maintenance operations shall be documented.

27. Supervision, security inspections and the provision of records on the operation of the system

Article 79

(Supervision, security inspections and provision of records relating to the operation of the system)

(1) A person shall determine the procedures for the regular monitoring of the operation of the information system to perform procedures or services in accordance with the requirements of the Act, Decree, these Rules and internal legal acts.

(2) The records on the operation of the system shall be kept at least until the inspection is carried out by the person concerned in accordance with the internal rules; subsequently, a new record shall be made on the performed inspection and the adequacy of the system.

(3) The person shall establish and document internal supervision of the implementation of information security measures, which shall at least include:

- a periodic implementation plan,
- the person responsible for this area.

(4) The person referred to in the preceding paragraph shall draft a report on the supervision, which shall also include the proposals for measures to eliminate deficiencies or to mitigate risks, and shall present it to the management.

Article 80

(Additional requirements for digital preservation service providers)

(1) In accordance with the risk management plan, digital preservation service providers shall arrange, by internal rules, for regular security checks of their information infrastructure, as laid down in Article 45 of the Decree.

(2) Digital preservation service providers shall record all their findings referred to in the preceding paragraph. The reports shall be kept at least until the inspection is carried out by an authorised person. Based on the inspection, a new report on the performed inspection and the adequacy of the system shall be produced.

28. Procurement of services

Article 81

(Provision of services to entities under public law)

(1) The capture and digital preservation of archival records or related accompanying services shall be provided to entities under public law only by providers that have previously had these services certified with the National Archives.

(2) If providers subcontract part of the services they offer to entities under public law, the services provided by sub-contractors shall also be certified.

Article 82

(Common risk assessment)

(1) Prior to signing a contract for the provision of services, the selected provider and the contracting authority shall prepare a common risk assessment for an individual service in the form of a written document, which shall take into account the specifics of the cooperation and contain at least the following information:

- the type and level of risk involved in the provision of a particular service,
- a description of the measures by type and level of risk,
- the division of responsibilities between the provider and the contracting authority according to the risk assessment.

(2) The selected provider and the contracting authority shall define by internal rules the scope, responsibilities and circumstances that require the updating of the common risk assessment.

Article 83

(Contractual arrangements for the procurement of services)

The outsourcing of services shall be contractually regulated by determining the precise scope of services, the level of service provision and the findings of the common risk assessment. The contract shall specify at least:

1. the precise scope of the service;
2. the level of service provision (e.g. availability, response time, accessibility, quality);
3. the responsibilities of the contracting authority and the outsourced contractor and their delimitation in implementing individual procedures in accordance with the scope of the service;
4. data protection and the signing of a confidentiality and data protection statement;
5. the right of the contracting authority to review the provision of the outsourced service on a regular basis, verifying in particular: the general organisation of the provider, information system management, security domain, documentation management and other areas relevant for the implementation of internal rules;

6. the provisions on data recovery, including audit trails and secure deletion of the contracting authority's data from the provider's data media after the service has been provided.

III. REGISTRATION OF EQUIPMENT AND SERVICE PROVIDERS

1. General requirements for equipment and service providers

Article 84

(Registration of the provider)

(1) Equipment and service providers shall be registered with the National Archives.

(2) The provider shall submit the application for registration on the prescribed form set out in Annex 3, which is an integral part of these Rules, or through the online application containing all the components listed in Annex 3 to these Rules.

Article 85

(Education and professional qualifications of the provider's employees)

(1) The service provider shall employ employees with a level of educational attainment as defined in Article 39 of the Act and Article 49 of the Decree. The employees shall have passed the professional competence test as prescribed in the special rules regulating the professional competence for handling records and shall also update their expertise with additional training.

(2) The employees referred to in the preceding paragraph shall have an employment relationship with the provider or shall perform work under another cooperation contract.

Article 86

(General conditions for the provision of services)

The service provider shall fulfil the general conditions for the provision of services as laid down in paragraph one of Article 49 of the Decree, which they shall prove by a written declaration set out in Annex 4, which forms an integral part of these Rules, and attach it to the application for registration.

IV. CERTIFICATION OF EQUIPMENT AND SERVICES

1. General requirements for the certification of equipment and services

Article 87

(First certification condition)

The provider of equipment or services, who wishes to file an application for the certification of equipment or services shall be previously registered with the National Archives.

Article 88

(Submission of an application)

(1) The provider shall submit an application for hardware certification on the prescribed form set out in Annex 5, which is an integral part of these Rules, or through the online application containing all the components listed in Annex 5 to these Rules.

(2) The provider shall submit an application for software certification on the prescribed form set out in Annex 6, which is an integral part of these Rules, or through the online program containing all the components listed in Annex 6 to these Rules.

(3) The provider shall submit an application for services certification on the prescribed form set out in Annex 7, which is an integral part of these Rules, or through the online application containing all the components listed in Annex 7 to these Rules.

(4) The provider shall submit an application for the certification of each piece of equipment and each service separately.

(5) The application shall be submitted in the Slovenian language, while the attached documentation may also be written in another language subject to prior approval by the National Archives.

(6) Prior to submitting the application for the certification of equipment and services, the provider shall perform a self-assessment of the equipment or services compliance by entering in the relevant checklist, with respect to each request (checkpoint), data on the equipment and services that are to be in the form of references and are to ensure compliance with the Act, implementing regulations and rules of the profession. The checklist shall be published on the website of the National Archives in accordance with the provisions of Article 2 of these Rules.

(7) Hardware and software may also be certified through a service certification procedure, but in this case, the equipment certification shall only apply to the certified service.

Article 89

(Application for accompanying services certification)

The application for obtaining a certificate for accompanying services may only be submitted for the following services:

1. the capture of digital records,
2. the conversion of records from physical to digital form,
3. the conversion of records from digital form to a long-term preservation form,
4. the arrangement or selection of records in digital form,
5. the elimination of records in digital form,
6. the provision of secure premises for the storage of records in digital form,
7. other services which in any way interfere with the integrity, security or authenticity of records.

Article 90

(Conditions for certification)

The basis for the certification procedures are the general certification conditions that were determined by the National Archives in accordance with Article 86 of the Act and are published on its website.

2. Hardware certification

Article 91

(Subject of the hardware certification)

(1) The application for certification may refer to the following hardware: servers, disk arrays, tape libraries and scanners for digitizing specific types of archival records.

(2) The specific types of archival records referred to in the preceding paragraph shall be the records, which, due to its medium, size, shape or other characteristics, require special handling or capture equipment for digitization. The following items are always classified as specific types of archival records: bound records, large-format records, records stored on non-durable media (parchment paper, glass, canvas), with added seals and records that are made with various reduction technologies (microfilm, microfiche).

Article 92

(Use of equipment within the voltage limits)

Hardware for the performance of operations or services shall comply with the regulation governing the availability of electrical equipment on the market and shall be designed for use within certain voltage limits.

Article 93

(Electromagnetic compatibility)

Hardware for the performance of procedures or services shall comply with the regulation governing electromagnetic compatibility.

Article 94

(Restriction of certain hazardous substances use in electrical and electronic equipment)

Hardware for the performance of procedures or services shall comply with the regulation governing the restriction of certain hazardous substances use in electrical and electronic equipment.

Article 95

(International recognition)

(1) Hardware for the performance of procedures or services shall be internationally recognised, which the provider will demonstrate by a statement of the manufacturer or representative.

(2) Hardware shall be deemed internationally recognised if used in at least three European Union countries where the manufacturer sells hardware and provides maintenance services for it.

Article 96

(Support and maintenance)

(1) The provider of hardware for the performance of procedures or services shall provide support and maintenance services for such equipment in the Republic of Slovenia within a reasonable response time, which it shall prove by the attached written statement, accompanied by all necessary information and other evidence

(an authorisation certificate from the principal manufacturer and the like) regarding support, the response time and services after the warranty period has expired.

(2) A reasonable response time shall be deemed to be no more than one working day to begin issue resolution. The minimum period following the expiry of the warranty period during which the manufacturer provides maintenance, replacement parts and coupling devices, shall be three years in accordance with the act regulating consumer protection.

Article 97

(Documentation)

(1) The provider shall provide technical and user documentation for the hardware it offers on the market and which is subject to certification.

(2) The user documentation referred to in the preceding paragraph shall be in the Slovenian language, while the technical documentation may be in the English language.

Article 98

(Redundancy)

The server and disk array shall enable:

- redundant power supply and redundant network connections,
- several types of redundant arrays of independent disks (RAID).

Article 99

(Optical resolution)

Scanners for the capture of specific types of archival records shall meet the requirements under Article 38 of these Rules.

Article 100

(Light source)

The light source shall provide uniform illumination of all parts of the surface without shadows and hot spots.

Article 101

(Metadata)

Scanners for the capture of specific types of archival records shall allow the export of technical metadata.

Article 102

(Colour depth)

Depending on the type of digitization, scanners shall provide at least the following colour depth:

- 8-bit grayscale, and
- 24-bit colour depth.

Article 103

(Output formats)

Scanners shall make it possible to export at least one of the formats specified in the list published on the website of the National Archives.

Article 104

Scanners designed for specific types of archival records shall enable at least:

- colour model selection (e.g. RGB, CMYK),
- GAMMA curve pre-settings,
- scanning area settings,
- whiteness settings,
- resolution settings,

- format settings.

Article 105

(Additional requirements for scanners designed for specific types of archival records)

Additional requirements for scanners designed for specific types of archival records are as follows:

1. For bound records, scanners are required to:
   - have a book holder that does not damage the records,
   - have adjustable glass pressure on records, where glass is used,
   - enable independent height adjustment for each half of the work surface.
2. For blueprints, large format maps and sensitive record media, scanners are required to have:
   - an A0 size flatbed scanner;
   - a streaming scanner for formats larger than A0 size, with the installed system for detection and prevention of damage to records;
3. For records on microfilm and microfiche or produced by other reduction technologies (e.g. cadastre on glass plate), scanners are required:
   - to enable the capture in the original size in accordance with the requirements of Article 38 of these Rules.
4. For slides, negatives:
   - for sizes smaller than 6 x 9 cm, scanners must feature an optical resolution of at least 2400 dpi, and
   - for other sizes, at least 1200 dpi.

3. Software certification

Article 106

(Types and functionalities of software)

(1) The type of the software that is subject to certification and the list of its functionalities (functional type) shall be determined according to the provider-client relationship.

(2) The types of software according to the provider-client relationship are as follows:

- custom software: the software is designed and specially developed for a specific organization, environment or users;
- customized software: the software is developed on the basis of a marketable software product with specific software adjustments for the client;
- marketable software: the software is supplied in completely identical form to more than one client;
- global marketable software: the software is supplied in completely identical form to more than a hundred organizations in at least three countries, as stated by the provider's written declaration. In this case, the requirements under Articles 108, 109 and 112 shall not be verified;
- internally developed software: the software is developed by a development team within the organization, where it is also used.

(3) The functional type of software and the software providing additional functionality combine a meaningful and logically rounded set of functionalities. The types of software that may be certified are as follows:

1. functional type 1: capture in digital form;
2. functional type 2: conversion,
3. functional type 3: keeping a register of records (without classification based on a classification system),
4. additional functionality 1: search, retrieval and display,
5. additional functionality 2: management of the record classification scheme,
6. functional type 4: support for the process of managing the records in digital form,
7. additional functionality 3: support for e-mail and e-signature,
8. functional type 5: support for requests concerning the official register.

(4) Functional software types may be certified independently. Software providing additional functionality may only be certified in combination with functional type software.

(5) In addition to mandatory functionalities, software may support any set of other functionalities.

(6) The software functionalities required under these Rules shall be finalized and shall operate upon the installation of the software version that is subject to certification. Software that only allows the required functionalities to be achieved with additional development, the use of internal scripting languages, and the like, for functions not included by default in the version that is subject to certification shall not meet the requirements under these Rules.

(7) The requirements to be met by each functional type of software are set out in Annex 8, which is an integral part of these Rules

Article 107
(Software data)

(1) The provider shall provide at least the following information in the software documentation:

- the identification code or the name of the software,
- the commercial product name of the software version,
- all its additional components together with the versions that make up the software and ensure its functionality. Additional software components shall be, like the software, indicated by means of an identification code or name and commercial product name of the version.

(2) The commercial product name of the software version or its additional parts shall mean the version that is available on the market or is in use.

Article 108
(Change management process and system)

In software development and maintenance, the process and system of change management shall be defined, documented and properly introduced to ensure that each published version of the software is available and has a unique and predictable code.

Article 109
(Software specification)

(1) The software specification exists and provides detailed acquaintance with all the software’s functional and non-functional characteristics and possible restrictions in its use.

(2) The specification shall also list the supported platforms and databases used by the software.

(3) Where the database is separable from other parts of the software and has a separate version management, or where the database is a platform or included software, the specification shall clearly indicate which version (or versions) of the database is included in the certification.

Article 110
(Instructions for installing software in the environment for regular use)

(1) Documented instructions shall be available for installing the software in the environment for regular use.

(2) Each described installation step shall include all necessary information that the provider can provide and that is necessary for making decisions in this step.

Article 111
(User documentation)

(1) The user documentation available for the software shall be in line with the final software (version) that is subject to certification.

(2) The user documentation may be in printed or electronic form or may be included in the software user interface.

Article 112
(Software testing)

(1) The software shall be tested using planned and controlled standard procedures that are fully documented, including test results and reports. The test shall be carried out in a manner that provides reasonable assurance of the software operation.

(2) The testing plan shall include the testing of software performance with boundary conditions and limit values that can reasonably be expected to compromise the records.

Article 113

(Management of the record classification scheme)

(1) The software shall enable the management of the record classification scheme, and only to persons with appropriate administrative rights within the software that is subject to certification.

(2) The software shall enable the capture, maintenance and presentation of metadata for classes in the record classification scheme.

Article 114

(Use of the record classification scheme)

The software shall enable the use of the record classification scheme, which is the substantive basis for classifying units.

Article 115

(Support for the record classification scheme hierarchy)

The software shall support at least three levels of hierarchy in the record classification scheme.

Article 116

(Support for the record classification scheme import)

The software shall support the import of all or individual parts of the record classification scheme at the initial setting or at any other time.

Article 117

(Support for metadata import)

When importing the entire or part of the record classification scheme , the software shall also enable the import of related metadata on retention periods and audit trails, if any.

Article 118

(Export of the record classification scheme)

The software shall enable the export of the entire or part of the record classification scheme, associated metadata and audit trails.

Article 119

(Capture, maintenance and display of metadata)

The software shall enable the capture, maintenance and display of metadata for files or other aggregations.

Article 120

(Automatic hierarchical code assignment)

The software shall enable the assignment of a hierarchical code to each class from the record classification scheme and to a file or other aggregation.

Article 121

(Designation of classes and files)

The software shall allow a person with appropriate administrative rights to assign a name to each class and to a file or other aggregation.

Article 122

(Preservation of metadata on dates)

As part of the metadata, the software shall store the date of creation of the class or file or other aggregation, and the date of disabling the use of the class or closure of the file or other aggregation.

Article 123

(Automatic integration of inherited characteristics)

When a new class or file or other aggregation is opened, the software shall automatically include in the metadata those characteristics that are inherited due to the position of that class, file or other aggregation in the arrangement of records.

Article 124

(Restriction of number of classes, files or other aggregations)

The software shall not impose any practical restrictions on the number of classes, files or other aggregations that may be defined.

Article 125

(Reallocation of codes to relocated classes)

Where a change in the record classification scheme necessitates the reclassification of files and records, the software shall ensure that the files and their content that are transferred to other classes are reassigned to include the new class designation. Data on previous codes shall also be included in the register.

Article 126

(Correct assignment of documents to files or aggregations during relocation)

The software shall ensure that during their relocation all records remain correctly assigned to the relocated file(s) or other aggregations and that all files remain properly linked.

Article 127

(reason for class relocation entry)

If a class is relocated, the software shall require a person with appropriate administrative rights to enter the reason for the relocation in the software as metadata.

Article 128

(Audit trail when relocating a class, file or record)

If a class, a file or an aggregation or a record is relocated, the software shall enter a record in the audit trail of the relocation.

Article 129

(Prevention of class deletion)

The software shall prevent the deletion of a class that has already been used to classify the records.

Article 130

(managing access permits)

The software shall allow persons with appropriate administrative rights to manage access permits for all users or groups of users in such a manner so as to enable them to:

1. restrict access to specific records units (e.g. files, records, entries in the official register);
2. restrict access to certain classes specified in the record classification scheme;
3. restrict access in accordance with the user’s security clearance (where applicable);
4. restrict access to specific options and functions (e.g. reading, updating or destroying certain metadata);
5. deny access after a specific date;

6. grant access to records units, classes and metadata to specific users or to persons or groups of persons with user rights for a limited period.

Article 131

(Tagging inactive users)

The software shall allow persons with appropriate administrative rights within it to tag individual users as inactive without deleting them from the system.

Article 132

(System functions setting)

The software shall allow the setting of system functions and related events only to persons with administrative rights for this system.

Article 133

(Considering access rights)

If the user requests access to any records unit, such as a records, file or class to which they do not have the access right, the software shall offer a response in accordance with one of the following rules (selected at the software configuration or later):

- it must not display any information about the subject in the manner that it would be possible to establish the existence of the subject;
- it shall confirm the existence of the subject and may also confirm the owner of the subject (displaying the identifier of the file or record) but without displaying the name and other metadata;
- it shall display only the name, the type of unit (class, records, etc.), the date of creation and the owner;
- it shall display the name and other non-protected metadata of the records unit.

Article 134

(Maintenance of audit trails inalterability)

The software shall ensure the inalterability of the audit trail, which automatically captures and stores data on:

- any action relating to any records unit, record collection or record classification scheme;
- the user who performs the action;
- the date and time of the action.

Article 135

(Automatic audit trail setting)

(1) The software shall enable an audit trail setting in such a manner that persons with administrative rights within the software or the system in which it is installed can set actions to be recorded automatically.

(2) Any changes to the audit trail setting shall also be recorded therein.

(3) The software shall not allow any changes to the settings of audit trail recording with respect to activities that prove the integrity and authenticity of the records.

Article 136

(Accessibility of data contained in audit trails on request)

The software shall ensure that the data contained in the audit trails are available for on-demand review in such a manner that enables the identification of individual events and that all data relating to them are accessible.

Article 137

(Export of audit trail data)

The software shall enable the export of audit trail data for specific records units (e.g. records, files, entries in the official register) or classes without any impact on the audit trail.

Article 138

(Information about the location and relocation of files and records in physical form)

(1) The software shall provide a tracking function that allows the recording of information about the location and relocation of files and records when they are in physical form.

(2) The tracing function shall record the information referred to in the preceding paragraph, including at least the following:

- the unique file or record identifier;
- the location;
- the date of sending/relocating the file from the location;
- the date of receiving the file at the location (in case of transfer).

Article 139

(Electronic signature and time stamp validity verification)

(1) The software shall make it possible to verify the validity of the electronic signature and the time stamp, if they exist, at least in accordance with the X.509 standard and for at least one format of records and of which for at least one format for the long-term preservation of records in accordance with the software's intended purpose.

(2) The procedure shall include the verification of at least the following:

- the validity of the signatory's digital certificate (not expired, not revoked, certified by the relevant authority);
- the validity of the certificate chain from the issuer's certificate to the trusted root certificate;
- the suitability of the certificate (applicable to electronic signatures);
- the mathematical validity of the signature on the data in accordance with the algorithms used;
- the time stamp validity.

(3) The software shall enable the persons with administrative rights within it to configure the equipment by storing metadata on the verification of electronic signature validity.

(4) The user shall be shown in readable form all the key information concerning the verification carried out as referred to in paragraph one of this Article.

Article 140

(Defining record confidentiality types)

The software shall enable and take into account definitions of record confidentiality types.

Article 141

(Retention periods)

(1) The software shall enable the entry of a large number of retention periods at all levels of records units (e.g. a file, a record) and the implementation of procedures for the selection of archival records and the elimination of records with expired retention periods.

(2) The software shall ensure that for each class and file or aggregation at least one retention period is always specified.

(3) The software shall preserve the unaltered history of changes and deletions (audit trail) relating to retention periods and procedures for the selection or elimination, including the date of change or deletion and the user who made the change.

(4) The software shall ensure that any change in retention periods is immediately applied to all classes and records units to which this change relates.

Article 142

(Import and export of retention periods)

The software shall enable the import and export of a large number of retention periods.

Article 143

(Retention period for selection and elimination)

The selection or elimination of each record shall be governed by a retention period related to the type of class and file or aggregation, to which the record belongs, and to any valid suspension of destruction.

Article 144

(Decisions regarding selection and elimination)

(1) The software shall enable at least the following decisions regarding the selection and elimination to be made:

- the transfer to permanent preservation,
- preparation for the review,
- destruction after confirmation by a person with appropriate administrative rights within the software,
- the submission to e-archives or transfer to other e-repositories.

(2) The software shall enable the user with appropriate rights to withhold the destruction or transmission of a class, file or aggregation, or a record.

(3) The software shall enable a reviewer to enter comments specifying the reasons for the decisions made during the review.

(4) The software shall keep an unaltered history of all decisions made by the reviewer during the review, including the reasons for the decisions referred to in paragraph one of this Article.

Article 145

(Review procedure support)

(1) The software shall support the review procedure by presenting the classes and files or aggregations for the review, along with their metadata and information on retention periods.

(2) The software shall automatically record the date of review.

Article 146

(Transfer or export of content to another system or organization)

(1) Whenever the software transfers or exports any records unit (e.g. a class, a file, a group of records in the official register), the transfer or export shall contain all subordinate records units:

- (with respect to classes) all files and records in the class;
- (with respect to files or aggregations) all records in the file or aggregation;
- all or selected metadata related to any part of the records;
- all or selected audit trails for all included parts of the records.

(2) The software shall be capable of transferring or exporting parts of records in a continuous sequence of operations in such a manner that:

- the content and composition of the records units are not altered,
- all records unit files are exported as a complete unit,
- all links between the records unit and its metadata and audit trail are preserved,
- all links between the parts of records are preserved so that they can be restored in the receiving software.

(3) The software shall ensure the export of the entire class content from the records classification scheme in a single sequence of operations and shall also ensure that:

- the position of each records unit is preserved according to the records classification scheme in order to restore the arrangement of records;
- a sufficient amount of metadata is preserved to restore the entire hierarchy of arrangement above the records unit that is being exported.

Article 147

(Transfer of selected records units to another system or organization)

The software shall enable the following actions to be performed when exporting or transferring any selection of records units:

- the export or transfer of records units along with their retention periods in such a manner that these retention periods can be reused in the system to which the records have been exported or transferred;

- the printout of a report or reports on the retention periods applicable to each selection of records units and the characteristics of those retention periods,
- the export or transfer of records units along with their access permits in such a manner that these permits can be reused in the system to which the records have been exported or transferred;
- the printout of a report or multiple reports on access permits for each selection of records units and their characteristics.

Article 148

(Preservation of metadata during transfer)

(1) The software shall preserve all classes, records units and other information which were transferred at least until it is confirmed that the transfer has been successful. Once the software has received confirmation of a successful transfer, it shall allow the transferred content to be destroyed, with the exception of metadata that are retained in the register of the records and which prove their existence.

(2) The metadata referred to in the preceding paragraph shall contain at least the following information:

1. date of transfer,
2. unique identification code of the records unit,
3. title, if it exists,
4. description, if it exists,
5. user responsible for the transfer,
6. reason for the transfer (which may be related to the retention period, selection, elimination or a manually entered reason).

Article 149

(Preservation of metadata after the destruction of classes or records units)

(1) After destroying classes or records units, the software shall ensure that metadata proving their existence are kept in the register.

(2) The metadata referred to in the preceding paragraph shall contain at least the following information:

1. date of destruction,
2. unique identification code of the records unit,
3. title, if it exists,
4. description, if it exists,
5. user responsible for destruction,
6. reason for the destruction (which may be related to the retention period, selection, elimination or a manually entered reason).

Article 150

(Provision of control and functionality)

The procedure of capture in the software shall provide control and functionalities that allow users to:

- capture the records unit regardless of the format, the encoding method and other technological features, without changing the content;
- link the records units to the records classification scheme.

Article 151

(Capture of parts of records units)

(1) The software shall capture all parts of the records unit if the unit contains more than one part.

(2) When capturing the records units containing more than one part (e.g. an annex or several enclosures or attachments), the software shall enable the records unit to be managed in such a manner that the relationship between the parts of the records unit and the integrity of the records unit is preserved.

(3) Where the software changes the links in the records unit during capture, it shall record all details of any changes made in the audit trail.

(4) The software shall enable the capture of the records unit even if the software with which it was created is not available (i.e. regardless of the format).

Article 152

(Capture of records unit metadata)

(1) The software shall ensure that all mandatory metadata are present for each captured records unit.

(2) The software shall store the time of capturing the records units in the metadata and in the audit trail.

(3) The software shall support the assignment of multiple keywords (or key terms) to each records unit.

Article 153

(Limiting the option of changing the title of a records unit)

The software shall enable to limit the option of changing the title of a records unit, where it exists, to a person with appropriate rights.

Article 154

(Automatic metadata capture during bulk imports)

The software shall enable the automatic capture of metadata related to records units during a bulk import, with the option of manually entering the missing or incorrect metadata.

Article 155

(Verification of capture and validity of metadata in bulk imports)

When, during import, the software captures the metadata of individual records units, it shall verify them by applying the same rules as for the manual capture of the records. When errors are detected in this verification process (e.g. when there are no mandatory metadata or when errors occur in the format), the software shall report them to the user who performs the import, indicate the missing metadata and record errors and actions in the audit trail.

Article 156

(Import of audit trails in bulk imports)

(1) The software shall enable the import of audit trails that show the history of the imported records units.

(2) The software must not import audit trail records into its audit trail; it must store them separately.

Article 157

(Capture of e-mail)

(1) The software shall enable the capture of incoming and outgoing e-mail messages, including attachments, if they exist, in the form of records, automatically extracting at least the following metadata:

- the address of the recipient of an electronic message (the message recipient, the "To" field in the message header),
- the address of the recipient of an electronic message (for information, the "Cc" field in the message header),
- the address of the reply recipient (the "From" field in the message header),
- the address of the sender of an electronic message (the "Sender" field in the message header),
- the title/subject of an electronic message (may also be the "Subject" field in the message header),
- the date and time of an electronic message (the "Date" field in the message header).
- the electronic signature, if it exists (e-signature field in the message header), including details of its verification.

(2) When capturing e-mail messages, the software shall automatically capture the metadata of the address with the value of the "Subject" field in the message.

(3) The software shall enable the user who captures the e-mail to edit the title of the record.

Article 158

(Restriction of search and retrieval)

If a user performs any search that includes a content search (usually a full-text search or a free-text search query, although other formats are possible), the records units for which the user is not authorized to access must never be included in the list of search results.

Article 159
(Search and retrieval)

(1) The software shall enable users to define any metadata as search terms.

(2) The software shall enable users to determine whether the search engine should search for a specific type of a records unit (e.g. records, files) or all records units that meet the search conditions.

(3) The software shall enable users to limit the scope of the search to any collection of records specified at the time of the search.

(4) The software shall enable users to search across heterogeneous metadata formats (e.g. date or numeric formats) if these formats exist.

(5) The software shall enable users to search through the text of records units.

(6) The software shall show the total number of search results and display (or allow the user to request a display of) the results (the "hit list").

(7) The software shall provide a search function that allows the simultaneous use of multiple Boolean operators, namely:

- AND;
- OR;
- NOT;

to obtain an unlimited number of search terms.

(8) The software shall enable users to search by keywords, when search items have them.

Article 160
(Printing the content of records units)

The software shall enable the printing of the content of records units in such a manner that the existence of any attachments, but not necessarily their content, and metadata about the records, which are entered in the register of records, is visible.

Article 161
(Printing the records classification scheme and retention periods)

(1) The software shall enable the printing of retention periods.

(2) The software shall enable the printing of the records classification scheme in its entirety or of its selected part.

Article 162
(Generating reports)

(1) The software shall enable the generation of a report on the total number and location of the records units:

- with the option of classification by size or location of storage;
- classified by file format;
- classified by access control and level of security (if applicable).

(2) The software shall enable the generation of a report by listing the records units by their structure.

Article 163
(Generating audit trail reports)

(1) The software shall enable a person with appropriate rights to generate an audit trail report for a selected search item, such as a class, file, record or by user or period.

(2) The software shall generate reports on the result of the selection and elimination by indicating the records units that have been successfully destroyed, as well as reports on any errors.

(3) The software shall generate reports on the result of exports by indicating the classes and records units that have been successfully exported, as well as reports on any errors.

(4) The software shall generate a report detailing any failure during transfer, import, export, destruction or deletion. The report shall list all records units and the related metadata intended for transmission that caused the errors and all entities whose transfer, import, export, destruction or deletion has failed.

Article 164

(Configuration option to flag and delete records units)

(1) The software shall provide a configuration option to prevent any person with administrative or user rights within the software from deleting or relocating any records unit that has already been captured.

(2) The software shall enable persons in the user role to flag classes and records units as candidates for deletion.

(3) In exceptional cases, the software shall enable persons with appropriate administrative rights to delete records units outside the selection and elimination procedure in order to eliminate human error.

(4) Each time the deletion referred to in the preceding paragraph is made, the software shall:

- record the deletion in the audit trail,
- generate a report for the administrator,
- delete the entire content of the class or records unit,
- ensure that no record is deleted if this changes another records unit (e.g. when the records unit is part of two records and one of them is deleted),
- draw particular attention of the person with appropriate administrative rights to any connection between another records unit and the unit flagged for deletion, and shall require confirmation prior to deletion,
- always preserve the integrity of metadata.

Article 165

(Modification of metadata)

(1) A person with appropriate administrative rights within the software shall be allowed to modify any metadata entered by the user (usually at the request of the latter due to input errors).

(2) Data on any modifications in metadata shall be preserved in the audit trail.

Article 166

(Restrictions on metadata)

(1) The software shall allow different groups of metadata to be determined for different types of records during the configuration.

(2) The software shall not limit the number of metadata allowed for each unit (e.g. a file, a record).

(3) The software shall allow the administrator to specify at the time of configuration whether each metadata element is mandatory or optional.

Article 167

(Metadata formats)

The software shall support at least the following metadata formats:

- textual,
- alphanumeric,
- numeric,
- date.

Article 168

(Information on the source of metadata)

(1) The software shall enable that during configuration the source of each metadata is identified.

(2) The metadata sources referred to in the preceding paragraph shall include, for example, a manual entry (with a keyboard), drop-down list, automatically obtained value from the preceding level in the hierarchy of the records classification scheme, an insight spreadsheet or a reference to another application.

Article 169

(Preventing any metadata corrections)

The software's settings shall enable the prevention of the modification of the selected metadata that are collected directly from other applications, the operating system or software, such as data from downloaded e-mails.

Article 170

(Enabling conversion of formats)

The software shall enable, during the time of capture, preservation or export, the conversion of records units from at least one original format to at least one format suitable for long-term preservation.

Article 171

(Preservation of metadata during conversion)

At the time of conversion, all key content-related data and metadata shall be preserved and conversion metadata shall be generated, including at least:

- date of conversion,
- original format and its version,
- information on the software used for the conversion.

4. Services certification

Article 172

(General conditions for services certification)

The certificate for the provision of services shall be granted on the basis of:

- the registration of a specific service provider,
- the internal rules approved by the National Archive; and
- the already certified hardware and software, or the certificate for such equipment is granted within the service certification.

Article 173

(Service certification requirements)

(1) Only services regulated by internal rules approved by the National Archives shall be certified.

(2) The services referred to in the preceding paragraph are as follows:

- capture,
- digital preservation,
- accompanying services referred to in Article 2 of the Act.

V. TRANSITIONAL AND FINAL PROVISION

Article 174

(Validity of already approved internal rules and awarded certificates)

The approved internal rules and certified services and equipment, which were drafted on the basis of the Uniform Technological Requirements - Version 2.1, issued by the National Archives on 10 July 2013, shall remain valid until their expiry.

Article 175

(Completion of procedures)

The procedures for the approval of internal rules and for the certification of equipment and services initiated prior to the entry into force of these Rules shall be completed in accordance with the Uniform Technological Requirements - Version 2.1 that were issued by the National Archives on 10 July 2013.

Article 176

(End of validity)

On the day these Rules enter into force, the Uniform Technological Requirements - Version 2.1, issued by the National Archives on 10 July 2013, shall cease to apply.

Article 177

(Entry into force of these Rules)

These Rules shall enter into force on the fifteenth day following their publication in the Official Gazette of the Republic of Slovenia.

No. 0070-22/2018

Ljubljana, 31 August 2020

EVA 2016-3340-0024

Vasko Simoniti

Minister of Culture

Annex 1: Application for the approval of internal rules

Annex 2: Application for the approval of model internal rules

Annex 3: Application for the registration of a provider of digital preservation equipment and services

Annex 4: Statement of compliance with the general conditions for the provision of services

Annex 5: Application for the hardware certification

Annex 6: Application for the software certification

Annex 7: Application for the services certification

Annex 8: Requirements to be met by each functional type of software