



EUROPEAN COMMISSION

SECRETARIAT-GENERAL

SEC(2020) 800

**Implementing Rules
for
Decision C(2020) 4482
on
records management and archives**

CONTENTS

SCOPE.....	5
CHAPTER I RECORDS MANAGEMENT	6
1. CAPTURE.....	6
1.1. What to capture.....	6
1.2. Purpose of capture	6
1.3. A two-stage process.....	6
1.4. Minimum criteria to be fulfilled by all capture systems.....	6
1.4.1. Basic features.....	6
1.4.2. Assignment of a unique identifier	7
1.4.3. Audit trails	7
1.5. Documents created automatically.....	7
1.6. Registration.....	7
1.7. Rules and procedures with equivalent effect to capture and registration	8
1.8. Provisional registration procedure.....	8
2. FILING.....	9
2.1. Purpose and aims of filing	9
2.2. Commission filing plan	9
2.3. Principles of the filing plan	10
2.4. Creating and managing files	11
2.4.1. Lead unit (unité chef de file)	11
2.4.2. File	11
2.4.3. File list	11
3. VALIDITY AND ADMISSIBILITY CRITERIA OF DOCUMENTS	12
3.1. Parties involved in electronic exchanges of documents	12
3.2. Identification of a member of staff	12
3.3. Identification of an external person	13
3.4. Reliability of the Commission's production context.....	13
3.5. Reliability of a third party's production context	13
3.6. Guarantee of integrity of document content and metadata, and their preservation	14
4. VALIDITY AND ADMISSIBILITY OF DIGITISED CONTENT	14
4.1. General principles.....	14
4.2. Formats	14

4.3.	Quality control.....	14
4.4.	Retention of original content.....	15
4.5.	Documentation of the digitisation procedure	15
5.	ELECTRONIC SIGNATURES	15
5.1.	Management of documents with electronic signatures	16
5.2.	Documents not requiring a handwritten or qualified electronic signature	16
6.	VALIDITY OF ELECTRONIC PROCEDURES.....	17
6.1.	Protection of content and stages of the procedure against alteration	17
6.2.	Priority use of the workflow system for structured transmissions	18
7.	DATA AND INFORMATION WITHIN THE COMMISSION	19
8.	INFORMATION SECURITY	19
	CHAPTER II PRESERVATION AND HISTORICAL ARCHIVES.....	20
9.	PRESERVATION	20
9.1.	Organisation and responsibility.....	20
9.1.1.	Lead department (département chef de file).....	20
9.1.2.	Preservation responsibility of Commission departments	21
9.2.	Preservation over time.....	21
9.3.	Preservation of metadata	22
10.	STORAGE.....	22
10.1.	Responsibility.....	22
10.2.	Official electronic repositories	22
10.2.1.	Architecture	23
10.2.2.	Functionalities	23
10.2.3.	Preservation of electronic signatures.....	24
10.3.	Physical storage areas.....	24
11.	RETENTION, TRANSFER AND ELIMINATION	25
11.1.	Common Commission-level retention list.....	25
11.2.	Specific retention list.....	26
11.3.	Administrative elimination procedures for records.....	26
11.4.	Administrative retention period (ARP)	26
11.5.	Appraisal and transfer to the historical archives	27
11.5.1.	Purpose and aims	27

11.5.2. Principles governing appraisal and transfer of files to the Commission's historical archives	27
11.6. Rules governing the appraisal of files	28
11.6.1. First review	28
11.6.2. Second review	28
11.7. Rules governing sampling and selection	29
11.8. Rules governing the elimination of files	30
11.9. Rules governing the transfer of files	31
11.10. Transfer and elimination metadata	31
11.11. Responsibilities concerning files and records transferred to the Commission's historical archives	31
11.12. Processing of records and archives created before the implementation of Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom	32
12. COMMISSION'S HISTORICAL ARCHIVES SERVICE	32
13. DEPOSIT OF THE COMMISSION'S HISTORICAL ARCHIVES AT THE EUROPEAN UNIVERSITY INSTITUTE (EUI)	33
13.1. Deposit	33
13.2. Public access	33
CHAPTER III GOVERNANCE AND IMPLEMENTATION	34
14. COORDINATION AND MONITORING BY THE SECRETARIAT-GENERAL	34
14.1. Capture of information	34
14.2. Filing and management of files	34
14.3. Preservation of files	34
14.4. Appraisal and transfer of files to the Commission's historical archives	35
15. DOCUMENT MANAGEMENT OFFICERS	35
15.1. Implementation in Commission departments	35
15.2. Document management officers	35
15.3. Professional competences of records management and archives staff	36
16. PREVIOUS ACTS	37

Scope

These implementing rules, adopted pursuant to Article 22 of Commission Decision C(2020) 4482, concern:

- a) the capture of information (Articles 4 and 6 of the Decision);
- b) the digitisation of analogue information (Article 5);
- c) the registration of records (Article 7);
- d) the filing plan and filing (Article 8);
- e) the legal effects of electronic signatures, seals, time stamps and registered delivery services, and criteria for the validity and admissibility of documents and procedures (Articles 10 and 11);
- f) the provision of data and information within the Commission (Article 12);
- g) information security and protection (Article 13);
- h) the storage and preservation of records (Article 14);
- i) the retention, elimination and transfer of files to the Commission's Historical Archives Service (Article 15);
- j) the Commission's Historical Archives Service (Article 16);
- k) the processing of personal data contained in the Commission's historical archives (Article 17);
- l) the deposit of the Commission's historical archives at the European University Institute (Article 18);
- m) governance at Commission level (Article 19); and
- n) the network of document management officers (Article 20).

Chapter I

Records management

1. CAPTURE

1.1. What to capture

Information that is considered useful for understanding a case or activity, or that could be of interest to other Commission colleagues or departments¹ (whether at the time of creation or later) will need to be captured.

1.2. Purpose of capture

The purpose of capturing information as a record is to:

- a) consider the information as held by the Commission;
- b) identify the record in question with certainty and in such a way that it cannot be altered at any point in its lifecycle;
- c) be able to make the information available to other colleagues or departments, either now or in the future.

Information that does not fulfil the conditions for capture is not considered part of the Commission's documentary resources².

1.3. A two-stage process

Capture comprises two distinct operations to be performed at the same time:

- a) saving the metadata of the record in the records management system concerned, to ensure that the record is properly described for administrative, legal and archival purposes; and
- b) linking the record to its metadata in a permanent and non-modifiable manner, so that an individual or department can identify the record beyond any doubt in the future.

1.4. Minimum criteria to be fulfilled by all capture systems

1.4.1. Basic features

The system must save the captured metadata and preserve the link between the original record and its metadata for as long as the record is retained.

The system must facilitate:

- a) assignment of the record to a given individual, department or IT system for action, follow-up, information or preservation; and
- b) the traceability of the record throughout its lifecycle.

¹ In this document, the term 'Commission departments' refers to the Commission's directorates-general and equivalent departments.

² 'Documentary resources' means all records, files and metadata created, received, captured, filed and preserved by the Commission.

At the request of the record's originator or on their own initiative, document management officers or other authorised members of staff may modify a record's metadata where they are inaccurate or incomplete. Such changes must be documented in a way that shows:

- who requested them;
- who made them;
- when they were made; and
- the original metadata.

This information must be retained for as long as the record to which it pertains is retained.

1.4.2. Assignment of a unique identifier

Where a new record is created in or captured by a records management system, the system must associate it with a unique identifier that allows users and systems to retrieve, refer to and use the record.

As a minimum, that identifier must contain the year in which the capture was performed and a number that is reset to zero on 1 January of each year³. This numerical series is unique to each general or specific register kept by each Commission department and must offer the best possible guarantees of consistency and continuity in numbering. Alongside the numerical series, alphanumeric identifiers may also be used to provide additional information on the register used or on the type of entry.

1.4.3. Audit trails

All capture systems must provide specific audit trails. These must be designed to preserve essential metadata relating to the actions performed on the record over time.

1.5. Documents created automatically

Documents that are created automatically by an IT system and meet the conditions for capture are subject to the same analysis as other records at the stage of the configuration of the IT system that creates them. The purpose of this is to determine how formal the records should be, their layout, how their content is to be formulated and how they are to be managed.

1.6. Registration

Registration is the main type of capture. It is subject to more stringent rules.

Records created to provide evidence of decisions, situations, intentions or events linked with the activities of the Commission or its departments must be registered in an official register, unless they are governed by rules or procedures with equivalent effect.

³ This does not apply to the minutes of meetings of the College.

Information as described in Article 7 of the Decision that is received by a Commission department in the course of its activities is subject to registration.

The purpose of registering a record created or received by the Commission is to:

- a) certify that the record (provided that it fulfils the Commission's established or generally recognised minimum requirements⁴) has been sent by an author to an addressee on a given date, as incoming or outgoing mail, or has been incorporated into one of the Commission's official repositories; and
- b) facilitate the creation of registers containing references to records registered by Commission departments and designed to meet the Commission's needs and its legal obligations regarding public access to documents⁵.

All official registers are linked to one or more official electronic repositories of records. The Secretariat-General assigns the official status to electronic registers and repositories.

Records are registered within 48 hours of being received or finalised and, if applicable, signed.

A registered record may be removed from the records management system only by the document management officer or other member of staff responsible for the register and only if it was registered in error.

1.7. Rules and procedures with equivalent effect to capture and registration

Departure from the capture or registration rules is possible for certain records⁶ where the procedures to which they are subject guarantee equivalent results. In particular, the procedures must be reliable and stable, and it must be possible to verify their correct and consistent application.

1.8. Provisional registration procedure

Each Commission department must adopt appropriate procedures for provisional registration, so that it can meet any obligation to transmit a record if, for technical reasons (e.g. prolonged power or computer failure), the registration system is unavailable and registration of the record cannot be postponed.

⁴ All Commission documents must be checked for compliance with established procedures and forms. Documents from other institutions or third parties are presumed to comply with established procedures and forms unless there is an obvious error.

⁵ Under Article 11 of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

⁶ e.g. mission orders and translation requests.

2. FILING

Captured records (whether registered or not) are organised in files. A single official file must be established for each matter falling within the remit of a given department. Each official file must be completed with records created or received in connection with the matter; these must reflect departments' activities in the case in question.

Commission departments must add file-level metadata that are reliable and sustainable and can be used to carry out operations arising from legal obligations⁷.

2.1. Purpose and aims of filing

The purpose of filing is to:

- a) incorporate all records received or created into the Commission's documentary resources; and
- b) organise records according to their original relationships with one another and with the activities that led to their existence, thereby reflecting the circumstances in which they were created and their significance in the development of the case.

The aims of filing are to:

- a) interpret and use records in the context in which they were created, so that they provide a full account of the administration's activities and serve as proof of the work it has carried out;
- b) facilitate targeted searching by making the file and constituent records more traceable throughout their lifecycle;
- c) improve the quality and continuity of administration, especially where another member of staff takes charge of the case and/or it is taken over by a different department; and
- d) assign the record its retention period and disposal action (elimination or transfer to Commission's historical archives), according to the retention category of the file (see point 11.1).

2.2. Commission filing plan

A filing plan is drawn up at Commission level. Its consistency is guaranteed by a common methodology and terminology based on common principles at central and local levels.

The department concerned is responsible for creating a file and linking it to a heading in the filing plan, in accordance with its own internal arrangements.

The aim of the filing plan is to:

- a) provide an overview of the Commission's documentary resources;

⁷ Under Regulation (EC) No 1049/2001 and Council Regulation (EEC, Euratom) No 354/83 of 1 February 1983 concerning the opening to the public of the historical archives of the European Economic Community and the European Atomic Energy Community (OJ L 43, 15.2.1983, p. 1).

- b) ensure the consistency of the Commission's filing systems across all common sectors of activity; and
- c) make it easier to find files and records by means of the metadata added to the filing plan headings and files.

2.3. Principles of the filing plan

The filing plan depends on the mission of the Commission in general and the tasks, functions and activities of individual departments in particular. It is therefore adjusted in line with relevant fundamental changes in EU law.

The filing plan takes the form of a tree structure, with headings that represent the activities carried out by the Commission departments in the exercise of their mandates⁸. The headings are identified by a clear, succinct title and a code.

The filing plan is divided into levels as follows:

- a) the common file classification for the first levels of the tree structure are defined by the Secretariat-General; and
- b) subsequent (specific) levels are defined by the departments, which bear full responsibility for them, particularly as regards the drawing-up, management and upkeep of the headings relating to their areas of activity.

The departments 'own' the headings they create. Departments that share the management of certain activities can nevertheless decide to create common headings and, if necessary, call on the Secretariat-General to assist with coordination.

The means and tools exist to ensure that the filing plan has:

- the flexibility needed to reflect how the functions and activities of the Commission and the departments evolve over time; and
- the stability, in terms of independence in relation to departments' organisation charts, that is essential to its operation.

A change of Commission or the reorganisation of a department will not affect the stability of the filing plan. However, if they involve the setting of a new mission or the assignment of new functions, the filing plan must be adapted accordingly and if a mission or function is abandoned, the relevant headings must no longer be used.

The filing plan must be completed and adapted, if necessary, in the light of the results of a detailed functional analysis, based on the procedures, working methods and rules in force, and on the documentary needs and operating procedures of the authors of the records.

⁸ In consultation with the departments responsible for keeping files, the Secretariat-General may develop other ways of aggregating records, linking information and defining the organisation of files.

2.4. Creating and managing files

2.4.1. Lead unit (unité chef de file)

At any given moment in the course of a case, one unit is always lead unit within the Commission department.

The lead unit is in charge of the case, but other units may be involved in performing related tasks or providing *ad hoc* assistance.

The lead unit is responsible for assigning every record to the appropriate file — either directly or by delegation as part of a procedure specific to the Commission department.

The lead unit must ensure that the logical coherence of the file is maintained, even if the case is dealt with in conjunction with several entities within the Commission department or across the Commission.

2.4.2. File

The lead unit opens the file at the start of the case, which is when the file's metadata must be encoded.

The lead unit must close the file when all actions stemming from the case have been concluded and no further record has to be created or modified. The closure date⁹ is the date of the most recent record added to the file. When a file is closed, it is no longer possible to add records. However, the metadata remain editable and filed records can still be consulted (depending on conditions of access).

Every registered record must be kept permanently in a file, unless the retention rules prescribe an administrative elimination procedure for records.

Other records may be included in the file to help clarify how a case was handled. If not removed before the file is closed¹⁰, these records become a permanent part of the file at the moment of closure and may then no longer be changed or removed from the file.

Each file reflects how a case has been handled in the Commission department concerned. This means that there may be several files for a given case.

A single 'file' may comprise a 'parent' file and several sub-files.

2.4.3. File list

The file list is a records management tool designed to:

- a) list the files created and held by the Commission;
- b) describe the files created under headings of the filing plan; and

⁹ Not to be confused with the material closing date, i.e. the date on which the file is closed in the system.

¹⁰ In particular, captured records containing personal data should be considered for removal before the file is closed.

- c) provide the Commission and its departments with a tool for retrieving and accessing the files.

The file list must contain the metadata for each file.

3. VALIDITY AND ADMISSIBILITY CRITERIA OF DOCUMENTS

3.1. Parties involved in electronic exchanges of documents

The parties involved in electronic exchanges of documents fall into one of the following circles:

- a) **circle 1** – the inner circle, comprising the Commission and its departments, which exchange documents electronically among themselves;
- b) **circle 2** – a semi-open circle comprising, on the one hand, the Commission and its departments and, on the other hand, partner administrations (other EU institutions, Member States, national public administrations and duly identified bodies with which the Commission has regular transactions), which exchange documents electronically via networks and mutually agreed procedures; and
- c) **circle 3** – an entirely open circle comprising, on the one hand, the Commission and its departments and, on the other hand, any external natural or legal person¹¹, who exchange documents through networks such as the internet or electronic mail.

3.2. Identification of a member of staff

The members of staff from whom documents originate may identify themselves by:

- a) signing the document with an electronic signature;
- b) signing the document by hand;
- c) sending the document, or authorising another colleague to send it, from their Commission email address; or
- d) sending the document, or authorising another colleague to send it, via an IT system to which access has been provided by means of EU Login¹² or an equivalent access system.

If no signature is required, the name of the member of staff from whom the document originates may be omitted from the text if:

- the name is clearly mentioned in the metadata of the corresponding electronic record; and
- either the capacity in which that person is acting is explicitly stated in the text of the document; or
- the team, unit or department to which that person belongs is explicitly stated in the text of the document.

¹¹ e.g. organisations, non-EU countries, commercial businesses, corporate bodies, recipients of Commission payments who are not members of its staff, and members of the public.

¹² EU Login is a user authentication service used by staff members to access particular IT applications.

3.3. Identification of an external person

The requirements of the system making it possible to identify the person from whom the document originates depend on the circle concerned and the degree of formality required for the subject area or the stage of the procedure. The guarantees of clear identification must be more stringent if the document is to have legal effect and less stringent if it is just an exchange of information.

Individuals belonging to circle 1 are identified electronically by means of EU Login or an equivalent system¹³. The Directorate-General for Informatics (DIGIT) is responsible for operating and maintaining the identification system¹⁴.

In circle 2, any document is admitted; parties involved in electronic exchanges must be identified by a mutually accepted system.

In circle 3, an external person may, as appropriate, be identified by:

- a) a simple electronic signature, unless the clear and unambiguous identification of the author and/or addressee is required, e.g. for reasons of confidentiality linked to the content of the document to be transmitted;
- b) the authentication function installed for a Commission application which complies with the principles of these implementing rules; or
- c) successive acceptance of exchanges of documents by senders and recipients.

In circle 3, any analogue document sent by an external physical or legal person is admitted on the assumption that the declared sender is the actual sender. A document cannot be admitted where, following an assessment of its form and content, reasonable doubts arise as to whether the external person is really its author.

The Commission does not admit anonymous incoming documents, unless it assesses that the information they contain is relevant for the institution and the document is to be captured.

3.4. Reliability of the Commission's production context

The Commission creates documents in accordance with common and specific rules, and the formal requirements set out in Article 4(2) of the Decision.

3.5. Reliability of a third party's production context

The Commission assesses whether the form and content of incoming documents tally with the purported identity of the author. If they match the context in which the document appears to have been produced and there is

¹³ For transmission of documents by email, the secure electronic mail (SECEM) system guarantees identification of the sender.

¹⁴ Exceptions may apply for systems dealing with classified information.

no reasonable doubt as to the document's authenticity and integrity, the Commission deems the document to be reliable and admissible.

The Commission admits documents in any media, including copies of originals, unless a Commission rule or an EU or national legal provision requires a specific medium or format.

3.6. Guarantee of integrity of document content and metadata, and their preservation

The required guarantee of integrity of the content of the document, its metadata and the method used to provide this guarantee are directly proportional to the degree of formality required by the type of exchange concerned.

Whatever the circle of parties involved and the system used for the exchange of documents, the content received is assumed to be equivalent to the content sent unless proven otherwise.

Paper documents drawn up by the Commission are considered intact if no alterations are found. In the event of damage caused by difficulties with preservation, documents are considered valid if their essential parts are still readable by any means and by collating with the corresponding digitised version.

4. VALIDITY AND ADMISSIBILITY OF DIGITISED CONTENT

4.1. General principles

The Commission systematically digitises all analogue documents to be added to its documentary resources.

Electronic renditions resulting from digitisation procedures and added to the Commission's documentary resources replace the initial content and form on which they are based (without prejudice to point 4.4).

4.2. Formats

Documents are digitised in a format that guarantees permanence, integrity and readability over time, and facilitates access to the information they contain.

Where possible, the format chosen for Commission documents is enriched by optical character recognition (OCR) that leaves the image intact but facilitates full text searches.

4.3. Quality control

The team responsible for digitisation in each Commission department establishes checks to provide reasonable assurance that the electronic rendition tallies with the original.

Quality control takes place at two levels:

- a) automatic quality control provided by the combined digitisation/OCR system – in the event of errors relating to metadata, duplications, etc., the system automatically sends an error message to the digitisation department, which duly corrects them; and
- b) manual quality control to verify that all content has been digitised correctly (all pages are included, the order of the pages has not been reversed, there are no errors, etc.).

The stringency of quality controls is directly proportional to the value of the electronic renditions or the length of time for which they are to be retained.

Notwithstanding the rules on the elimination of originals, all records are kept in their original medium for 6 months as a precaution. During this time, any errors reported are immediately corrected.

Where digitised content is corrupted due to preservation issues, it is considered valid if its essential parts are still readable by any means and by comparison with the corresponding original, if still available.

4.4. Retention of original content

If the original is a paper document for which one or more signatures are a substantial formality, it is preserved and subsequently transferred or eliminated in accordance with the retention rules¹⁵.

4.5. Documentation of the digitisation procedure

In all cases, the digitisation procedure must document:

- a) the scope;
- b) the procedural framework;
- c) the validation of results; and
- d) the elimination of the original medium.

All documentation relating to digitisation operations must be kept permanently.

5. ELECTRONIC SIGNATURES

The use of electronic signatures within the Commission does not affect the rules under which the signatory is, or is not, empowered to take decisions binding the Commission.

While only a small proportion of Commission documents require a signature as a substantial formality in order to be valid in accordance with EU or national law, an advanced or qualified electronic signature may be required, in particular for electronic exchanges within circle 3, where individuals must be clearly and unambiguously identified.

¹⁵ See Chapter II.

5.1. Management of documents with electronic signatures

For documents created by the Commission, secure electronic signature creation devices¹⁶ must use appropriate technical and procedural means to ensure that:

- a) the electronic signature creation data occur only once and reasonable guarantees exist that they will remain secret;
- b) there are reasonable guarantees that the electronic signature creation data used cannot be derived data and the signature is protected against forgery by the most advanced technology available; and
- c) the electronic signature creation data used can be reliably protected by the legitimate signatory against use by others.

In addition, secure electronic signature creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to signature.

For documents received by the Commission, DIGIT, assisted by the Security Directorate of the Directorate-General for Human Resources and Security (DG HR), makes available to the other departments the infrastructure and software required to read and technically validate advanced and qualified electronic signatures in accordance with generally accepted standards.

5.2. Documents not requiring a handwritten or qualified electronic signature

Documents **created** by the Commission that do not require a handwritten or qualified electronic signature relate mostly to administrative procedures, whether purely internal (e.g. relations between the Commission administration and its officials) or external (relations between the Commission and the other EU institutions, agencies and other bodies, Member States, firms or members of the public).

They include, inter alia¹⁷:

- a) documents created by the Commission that relate to the internal¹⁸ or interinstitutional¹⁹ legislative process. These include draft legislation, notes, studies and other reports assessing the content or consequences of legislation to be proposed, and preparatory documents such as green papers, white papers and communications;
- b) contracts or grant agreements exchanged, sent or notified through an electronic exchange system having equivalent legal effect to handwritten signatures²⁰;

¹⁶ See Regulation (EU) No 910/2014 (Articles 3 and 29-31, and Annex II).

¹⁷ The following list is non-exhaustive.

¹⁸ Excluding the authentication of acts, as provided for in the Commission's rules of procedure.

¹⁹ Transmission of such documents can nevertheless require an electronic signature as proof of their origin and to show that their integrity is preserved during transmission.

²⁰ See Article 148 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union (OJ L 193, 30.7.2018, p. 1).

- c) certain documents relating to the management of contracts and grants, such as information on calls for tenders (e.g. technical specifications) or calls for proposals (e.g. guidelines for applicants), reports of opening and evaluation committees;
- d) documents created by the Commission having legal effect in internal administrative procedures (e.g. application of the Staff Regulations);
- e) documents relating to the purely internal operation of a Commission department (e.g. minutes of meetings); and
- f) documents of a financial nature or concerning budgetary discipline, created by the Commission and intended for the other institutions, the Member States or external bodies acting under EU policies.

Documents **received** by the Commission that do not require a handwritten or qualified electronic signature relate mostly to administrative procedures and come from EU institutions and bodies, Member States, firms or members of the public. In particular, these consist of mail from outside, where national or EU legislation or administrative practice do not require a signed original.

They include, inter alia²¹:

- g) exchanges of information with Member States and other EU institutions, agencies and other bodies under EU policies;
- h) requests for access to documents made by members of the public;
- i) complaints about infringements of EU law;
- j) applications to take part in competitions or selection procedures, or unsolicited applications;
- k) supporting documents accompanying grant applications and, where appropriate, the application form itself, following a call for proposals under a framework programme; and
- l) statistical and financial data required under EU legislation, in particular those relating to common policies and their management, control or financing.

6. VALIDITY OF ELECTRONIC PROCEDURES

Within the Commission, IT solutions for managing specific procedures use EU Login or an equivalent system for the electronic identification of persons authorised to be involved in the procedure.

These information systems manage procedures in domains such as human resources, the policy and legislation lifecycle, programme management, procurement and grant management, case management and administrative procedures. They can involve circle 1, 2 or 3 exchanges.

6.1. Protection of content and stages of the procedure against alteration

To enable checks that the content of records and the stages in the procedure have not been altered, IT systems managing Commission procedures must:

²¹ The following list is non-exhaustive.

- a) provide effective measures to control rights of access, to prevent any access, elimination, alteration or illegal, malicious and unauthorised moving of records, files, metadata and stages in the procedure;
- b) be equipped with systems of protection against threats such as virus attacks, hacking, theft, fire, excessive temperature and water damage;
- c) prevent any unauthorised change and incorporate integrity mechanisms to check that a record has not changed over time;
- d) keep an audit trail for each essential stage of the procedure;
- e) save stored data in a safe environment, possibly in multiple copies and at different locations;
- f) provide reliable format conversion and migration procedures to guarantee the readability and accessibility of records throughout their retention period; and
- g) provide sufficiently detailed functional and technical documentation on the operation and characteristics of the system, accessible at all times by the organisational entities responsible for the functional and technical specifications²². This documentation must be kept up to date and, in the event of a change in the departments concerned, sent directly to the new lead departments responsible for the functional or technical aspects.

IT systems managing procedures in which the Commission and other bodies or organisations are involved and whose conditions and technical guarantees are determined by agreement must offer *mutatis mutandis* guarantees equivalent to the IT systems managing procedures specific to the Commission.

6.2. Priority use of the workflow system for structured transmissions

Commission departments must put in place workflow management systems where possible. These may take the following forms:

- a) information systems supporting automation of a process, in whole or part, during which electronic documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules (e.g. controlled access to documents and records)²³; and
- b) electronic sequential validation chain²⁴ enabling any person with the necessary access rights to modify, validate, sign or send back the records to be signed.

²² Organisational entities responsible for the functional and/or technical specifications are departments that are project owners of IT systems (e.g. Secretariat-General or DGs), DIGIT, the Security Directorate of DG HR, and DGs' document management officers and IT departments (information resource managers and their teams).

²³ See ISO 12651-2:2014.

²⁴ Commonly called 'e-signatory' at the Commission.

7. DATA AND INFORMATION WITHIN THE COMMISSION

Data and information must be available and shared as widely as possible within the Commission, in order to:

- a) facilitate the use of collaborative working methods;
- b) facilitate search and reuse of data and information; and
- c) promote synergies and efficiencies in the use of resources.

Commission departments may limit information sharing on certain files in the short, medium or long term, depending on the sensitivity of the subject and the cases being dealt with.

The main reasons to limit access to data and information relate to information security, data protection and sectoral confidentiality, e.g. due to competition issues, investigations and commercial interests.

Effective systems and tools must be used to facilitate the search for data and information across official electronic repositories.

In the interest of information sharing, departments must ensure that their files are as visible and as widely accessible as is consistent with the sensitivity of their content.

8. INFORMATION SECURITY

The IT systems, networks and means of transmission used to integrate records into the Commission's documentary resources must be checked, either by the Security Directorate of DG HR itself or under its control, for compliance with the legislation or rules governing security, personal data protection, IT system security and management of access rights.

Records containing sensitive non-classified information are subject to the Decision and these implementing rules. They are also subject to specific drafting, marking, capturing and other processing provisions, in accordance with the rules on information security²⁵.

Classified records are processed in accordance with the Decision and these implementing rules, while taking account of specific processing requirements under the rules on information security²⁶.

In addition, the Commission will implement these provisions in the procedures used to manage records and archives and in the configuration and adaptation of the IT systems used for this purpose.

Each department owning an IT system is responsible for the security of the system in its entirety.

²⁵ Mainly, Commission Decision (EU, Euratom) 2015/443 on security in the Commission (OJ L 72, 17.3.2015, pp. 41-52), Commission Decision (EU, Euratom) 2015/444 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, pp. 53-88), Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the Commission (OJ L 6, 11.1.2017, pp. 40-51), Security Notice C(2019) 1903 on information assessment and classification and Security Notice C(2019) 1904 for marking and handling of sensitive non-classified information.

²⁶ See previous footnote.

Chapter II

Preservation and historical archives

9. PRESERVATION

Preservation encompasses all techniques and practices used to ensure the integrity and readability of records and files over time, so that they can be accessed for as long as necessary, whatever their medium. This involves:

- a) establishing how preservation is organised and where responsibility for preservation lies within the Commission and its departments;
- b) preservation over time, in accordance with the provisions of the applicable retention list; and
- c) preserving capture and filing metadata, and any other relevant metadata accompanying the records and files throughout their lifecycle.

9.1. Organisation and responsibility

Each department must ensure the protection of the records and files for which it is responsible and their short- and medium-term accessibility²⁷, until these responsibilities are transferred to the Commission's Historical Archives Service²⁸ or the files are eliminated.

9.1.1. Lead department (département chef de file)

Throughout their lifecycle, records and files fall under the responsibility of a clearly identified lead department. This responsibility usually follows the normal lifecycle of the file in the documentary resources of the Commission department concerned. Depending on the Commission department's organisation (centralised, decentralised or mixed), the lead department will be responsible for the preservation of the files in its possession, including storage and transmission, in cooperation with the Commission department's document management officer and document management team or archives service.

The transfer or cessation of a lead department's activities may result in one of the following scenarios:

- a) an activity is transferred between units or Commission departments – responsibility for the records and files is transferred to the new lead department(s);
- b) the Commission is no longer responsible for the activity – all files relating to the activity are closed and the Commission department that produced the records and files remains responsible for them until they are transferred to the Historical Archives Service or eliminated;

²⁷ i.e. accessibility throughout the administrative retention period as set out in the common retention list or, where applicable, specific retention lists.

²⁸ From the date of such transfer, the Historical Archives Service is responsible for the physical protection of these archives. However, any other activity relating to a transferred record or file under 30 years old that forms part of the transferred archives remains the responsibility of the Commission department.

- c) the creator of the files is a temporary body – if this body ceases to exist and no Commission department takes over the activity²⁹, the temporary body closes and transfers the files to the Commission’s Historical Archives Service, which then assumes responsibility for their preservation and deals with any request for consultation or access; and
- d) the creator of the records and files is a Commission department that ceases to exist – if no other department takes over the activity³⁰, it closes all files associated with the activity and transfers them to the Historical Archives Service, which then assumes responsibility for their preservation and deals with any requests for consultation or access.

In all of the above scenarios, the new lead department for preservation must preserve the records and files in accordance with the Commission’s retention lists.

Any change in lead department must be documented.

9.1.2. Preservation responsibility of Commission departments

Document management officers are responsible for implementing the preservation rules. They must ensure that, whatever the medium:

- a) current records and files are available to the staff dealing with the case;
- b) the lead department for the records and files is known and is aware of its responsibilities;
- c) current and intermediate records and files are kept in the appropriate storage infrastructure and are inventoried; and
- d) the nature and location of intermediate records and archives are known.

Any creation, modification or migration of the systems, means and location of the archives is documented and carried out in agreement with the document management officer of the Commission department concerned and in compliance with the rules in force.

9.2. Preservation over time

Once captured, records are preserved in their original and/or a permanent format.

As soon as a record becomes part of an official electronic repository, any change is identified by means of an audit trail.

²⁹ If another Commission department takes over the activity in question, it becomes lead department for preservation (cf. point (a)).

³⁰ If another department takes over the activity in question, it becomes lead department for preservation (cf. point (a)).

Depending on the period for which records and files are to be retained and without compromising their authenticity or integrity, their medium or format may be changed to guarantee that they remain accessible and legible over time in line with the principles of the Commission's digital preservation strategy.

9.3. Preservation of metadata

All metadata accompanying a record or file throughout its lifecycle must be preserved³¹.

These are supplemented by preservation metadata, which are added by the lead department or by the official electronic repository.

10. STORAGE

Appropriate storage infrastructure must be provided to meet any preservation requirements. It must be suitable in the light of the types of record and file it needs to accommodate and the length of time these need to be preserved.

10.1. Responsibility

Each Commission department must take the necessary measures to ensure it has adequate space, equipment and infrastructure for its current and intermediate records and files, whatever their format or medium.

The departments responsible for establishing and maintaining registers in a given domain and for the accompanying official electronic repositories must ensure the protection and accessibility of electronic records and files managed therein. They must also ensure that the repositories comply with the Commission's provisions on the security of information systems and the provisions on electronic records and digitised documents, and their implementing rules.

10.2. Official electronic repositories

The Commission's electronic and digitised records and files are preserved in official electronic repositories throughout their lifecycle.

Any IT system that creates or receives records intended to form part of the Commission's documentary resources must be designed so as to ensure that records are captured, filed and preserved in an official electronic repository, in accordance with the procedures laid down by the Secretariat-General and any specific indications provided case by case.

If records are signed electronically, the electronic signatures and the digital certificates which were used to produce them must also be integrated into the related official electronic repository.

³¹ A list of the minimally required metadata for each phase of the lifecycle is provided by the Secretariat-General.

10.2.1. Architecture

Records are to be captured in a common official electronic repository or a specific official electronic repository that has received the prior approval of the Secretariat-General.

The architecture of the official electronic repositories takes account of the fact that there are different requirements for short- and medium-term readability, accessibility and preservation (current and intermediate records and files) and long-term readability, accessibility and preservation (definitive or historical archives).

The two types of common official electronic repository are:

- a) an official electronic repository for current and intermediate records and files – capturing electronic and digitised documents, together with all relevant metadata; and
- b) an official electronic repository for definitive or historical archives³².

10.2.2. Functionalities

Official electronic repositories must feature the following minimum functionalities:

- a) capture and filing of records in accordance with the applicable rules;
- b) preservation of records and files, all relevant metadata and the stages of the procedure in accordance with the rules on preservation and their implementing rules;
- c) migration of format(s) and/or computer environment(s) at sufficiently frequent intervals to guarantee the readability, accessibility and preservation of records and files throughout their retention period;
- d) management of linguistic and historical versions of the same record;
- e) a time stamp certifying the deposit of the record and its metadata on a given date, and the renewal of this time stamp at suitable intervals depending on security risks;
- f) disablement of the possibility of altering records bearing an electronic signature;
- g) access management and control based on the predefined rights of users and departments that own records and files and on the degree of accessibility to the records and files themselves;
- h) elimination of files, records and their metadata that are to be eliminated once their retention period expires and preservation of an audit trail of such eliminations;
- i) efficient search tools enabling files, records and metadata to be easily retrieved;

³² Long-term digital preservation needs to take account of the impact of changing technologies and changing audiences. Arrangements for this repository must therefore provide for monitored and documented preservation actions, such as adding technical metadata, using checksums and executing format conversion, to ensure that the digital records remain readable.

- j) a reporting function making it possible to produce reports on the basis of predefined criteria, with facilities for sorting and the possibility of saving, exporting or printing these reports;
- k) material protection of the official electronic repository against any risk of damage, loss or alteration of its integrity (measures to protect against virus and cyber-attacks and any other non-authorised access); and
- l) regular backups and the availability of a site mirroring the entire structure and content of the official electronic repository that is ready to take over if an emergency plan has to be activated.

DIGIT is responsible for operating and maintaining the common official electronic repositories in agreement with the Secretariat-General.

10.2.3. Preservation of electronic signatures

At the time of integration into the official electronic repository, the electronic signature is preserved in its original format throughout the period of short- and medium-term readability, accessibility and preservation of the record to which it relates.

Beyond that period³³, the function of the electronic signature is guaranteed in the official electronic repository by means of a digital fingerprint, even if the electronic signature itself is no longer readable, accessible or preserved.

For each record bearing an electronic signature, the official electronic repository generates a time stamp and automatically associates it with the record. This time stamp serves as proof of the date on which the record was entered into the system and certifies that the electronic signature, its key, algorithm and digital fingerprint were valid at that time.

10.3. Physical storage areas

Analogue records and files must be kept in physical storage areas that guarantee adequate physical protection and meet the following minimum requirements:

- a) a suitable location that is well designed, constructed and maintained;
- b) the possibility to control environmental conditions and protection against excessive light, dust, dirt, damp, heat, pests and mould;
- c) suitable storage facilities for records with different requirements, including shelving for boxes and cabinets or drawers for maps and plans;
- d) protection from unauthorised access; and
- e) protection from damage and disaster, including incompatible or hazardous activities and circumstances.

³³ If the ARP does not apply, 15 years at most.

If any of the above conditions cannot be met, the department responsible must contact the competent department for infrastructure and logistics so that appropriate steps can be taken.

Where more stringent requirements apply, e.g. for multimedia archives, the department responsible should review the situation jointly with the Secretariat-General, DIGIT and the competent Commission departments, so that appropriate technical and organisational steps can be taken.

11. RETENTION, TRANSFER AND ELIMINATION

11.1. Common Commission-level retention list

The common retention list (CRL)³⁴ is a regulatory instrument that sets the retention period for the different types of Commission file. Structured as a retention schedule, it provides preservation information for each type of file.

The Secretariat-General draws up and updates the CRL in close cooperation with all Commission departments.

The CRL takes account of the organisational context and the Commission's legal obligations. It aims to:

- a) identify the file types created and held by departments in the course of their activities, in order to ensure that the corresponding files are properly preserved;
- b) lay down the retention period for each type of file, taking into account its administrative usefulness, any statutory and legal obligations, and its potential historical value.

The retention period for each type of file is determined by:

- its administrative retention period (ARP);
- the action to be taken at the end of the ARP (post-ARP action or first review); and
- where applicable, the action to be taken after transfer to the historical archives.

The CRL sets these three parameters for each type of file;

- c) establish the administrative elimination procedures that departments must apply to certain types of file;
- d) set out the action to be taken by departments on the various types of file once the ARP has expired; and
- e) determine what action should be taken by the Historical Archives Service on the various types of file received.

Three post-ARP actions are possible: elimination, transfer to the historical archives and sampling or selection. For transferred files, two post-transfer actions are possible: permanent preservation and second review.

³⁴ SEC(2019) 900/2.

Commission departments must apply the CRL to all files created in accordance with these implementing rules, except the types of file for which a specific retention list (SRL) has been drawn up.

The CRL may have to be reviewed as a result of the adoption or amendment of legal bases, European Data Protection Supervisor (EDPS) opinions or Legal Service opinions imposing retention periods for certain types of file.

The Secretariat-General will have to submit any review of the CRL to the EDPS in accordance with Article 41(1) of Regulation (EU) No 2018/1725³⁵.

11.2. Specific retention list

Where Commission departments have specific types of file that do not concern another department and are not included in the CRL, they have to draw up a specific retention list (SRL).

The CRL rules apply *mutatis mutandis* to SRLs.

Before being adopted and implemented in the department in question, SRLs must have the approval of the Secretariat-General, the Legal Service and the Historical Archives Service. Since retention rules concern personal data, SRLs must be submitted to the EDPS under Article 41(1) of Regulation (EU) No 2018/1725.

11.3. Administrative elimination procedures for records

Administrative elimination procedures for records require departments to eliminate certain records or information from files for well-defined reasons before the end of the ARP.

The Commission's retention lists must refer to administrative elimination procedures applicable to certain types of file.

The elimination of records entails their physical destruction.

The elimination processes must be documented. This documentation must be preserved permanently.

11.4. Administrative retention period (ARP)

Commission departments preserve their records before closing the files concerned and during the ARP laid down by the applicable retention list. Only records that are part of files for which an administrative elimination procedure for records applies may be eliminated before the end of the files' ARP.

Where all or part of a closed file is needed in the event of litigation, an investigation or a complaint to the Ombudsman, any post-ARP action is

³⁵ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

suspended until the case has been dealt with. Once this suspension ('legal hold') is lifted, the post-ARP action can be carried out.

11.5. Appraisal and transfer to the historical archives

11.5.1. Purpose and aims

The purpose of the rules on the appraisal and transfer of files to the Commission's historical archives is to:

- a) guarantee the long-term preservation of archives that have legal or administrative value;
- b) facilitate access to such archives for anyone entitled to have access; and
- c) guarantee that the historical archives of the European Commission can be opened to the public after 30 years³⁶.

The aims of the rules are to:

- a) establish procedures for the appraisal of the Commission's files in accordance with the applicable retention lists;
- b) establish procedures for the elimination of files; and
- c) set out the responsibilities of the Commission departments and of the Historical Archives Service with a view to guaranteeing the medium- and long-term accessibility and preservation of the archives.

11.5.2. Principles governing appraisal and transfer of files to the Commission's historical archives

- a) Retention periods must take account of the obligation to transfer records no later than 15 years after the date on which they were created³⁷.
- b) Commission departments must review their files in the light of the applicable retention list with a view to eliminating them or transferring them to the historical archives. At the end of their ARPs, all files that need to be permanently preserved must be transferred to the Historical Archives Service.
- c) Within each department, the document management officer is responsible, under the authority of the director-general or head of department, for the first review of files³⁸ and for their transfer to the historical archives. The Historical Archives Service may refuse such transfers if these rules and the applicable retention list have not been correctly applied. It must inform the department concerned of the reasons for such refusal.

³⁶ In accordance with Regulation (EEC, Euratom) No 354/83.

³⁷ See Article 7 of Regulation (EEC, Euratom) No 354/83.

³⁸ This includes post-ARP actions such as sampling/selection and elimination. In many cases, operational units must be involved in reviewing files. The roles of the document management officer and of the operational units depend on the internal organisation of the department concerned. In any case, the document management officer must ensure that the first review of files complies with these provisions.

- d) At the time of first review, departments must check for external circumstances that could justify exemption from an elimination prescribed by the retention list³⁹. They must document any such exemption and submit it to the Secretariat-General for agreement.
- e) Compelling reasons must be provided to justify any exemption from the obligation to transfer files. The department's document management officer must submit these reasons to the Secretariat-General and the Historical Archives Service for agreement. Such exemptions will not affect the opening of the historical archives to the public after 30 years.
- f) To guarantee processing in compliance with the obligation to open the historical archives to the public, records and files containing sensitive information⁴⁰ must be clearly identified when they are transferred to the historical archives. Transferring departments must cooperate with the Historical Archives Service to review such sensitive information no later than 25 years after the closure of the files concerned, with a view to determining whether the files concerned can be opened to the public.
- g) Records and files not identified as containing classified or sensitive information will be opened to the public no later than 30 years after their creation.

11.6. Rules governing the appraisal of files

The appraisal of files consists of a first and a second review. A first review is applicable to all files at the end of their ARP. If the retention list provides for a second review, it must take place no later than 25 years after the files are closed.

11.6.1. First review

On the basis of the applicable retention list, Commission departments undertake, at least once a year, a first review of files that have reached the end of the ARP.

To this end, departments consider the file type and the date on which the file was closed. In accordance with the applicable retention list, the first review results in either the elimination of the files or transfer to the historical archives, where applicable after sampling or selection.

11.6.2. Second review

Files transferred to the historical archives after first review are:

- permanently preserved; or
- reviewed for a second time, where:

³⁹ Such circumstances could include the uncovering of past maladministration, an extraordinary public interest in the information or in the records concerned, or other factors that could make it necessary to preserve the files, at least temporarily.

⁴⁰ Within the meaning of Article 2(1), (2) and (3) of Regulation (EEC, Euratom) No 354/83.

- a second review is provided for in the applicable retention list; or
- the files are not subject to a retention list.

The second review is performed no later than 25 years after the closure of the files and results (depending on their historical value) in:

- their elimination; or
- their permanent preservation, where applicable after sampling or selection.

11.7. Rules governing sampling and selection

Sampling and selection are procedures that involve choosing a number of files for preservation from among a larger body of files. The files that are not preserved are eliminated.

The rules on sampling and selection apply to both the first and the second review.

In the case of **sampling**, files are chosen for preservation on the basis of an automated or random procedure with a view to keeping a proportion that is representative of the whole.

In the case of **selection**, files are chosen for preservation on the basis of subjective criteria. The files are not necessarily representative of the larger body from which they were selected.

Each sampling/selecting procedure must be fully documented. The documentation must include at least the following:

- a) the justification and purpose of sampling/selection;
- b) a list of files undergoing sampling/selection, including an indication of:
 - the relevant retention list category;
 - the files chosen for preservation; and
 - the files chosen for elimination; and
- (c) the criteria applied and the reasons for them.

Where files are sampled/selected at first review, the documentation is produced by the originating department or its successor. Files selected for elimination are eliminated in accordance with point 11.8. Files selected for preservation are transferred to the historical archives in accordance with point 11.9, together with the file lists and the accompanying documentation.

Where files are sampled/selected at second review, the Historical Archives Service produces and preserves a list of files chosen or selected for permanent preservation, a list of eliminated files and the accompanying documentation. Copies of these lists and documentation are sent to the originating department or its successor.

11.8. Rules governing the elimination of files

Elimination entails the physical destruction of files in accordance with the applicable retention list at first review or where elimination is the result of second review or of sampling/selection.

Files must be eliminated in accordance with the applicable security provisions.

Elimination includes the physical destruction of storage media⁴¹ and the erasure and overwriting of all known instances of the material to be eliminated, to ensure that the information is permanently and irrevocably eliminated.

Where the elimination of files involves the physical destruction of paper or other material support, the department and the Historical Archives Service will need to apply the recycling and destruction standards in force at the Commission at the time of destruction.

Elimination must be properly documented. Such documentation must include:

- a) the justification for elimination;
- b) the list of eliminated files, including their relevant metadata;
- c) the Commission department and the staff responsible for the decision to eliminate the files;
- d) where physical destruction of storage media occurs:
 - the department and staff responsible; and
 - the conditions under which elimination took place, including the date and method of destruction.

Where files are eliminated after first review, the department responsible produces lists of eliminated files and the accompanying documentation, which it sends to the Historical Archives Service for permanent preservation.

Elimination of information classified as CONFIDENTIEL UE/EU CONFIDENTIAL or above is done in accordance with the information security provisions.

Where files are eliminated after second review, the Historical Archives Service produces and preserves lists of eliminated files and the accompanying documentation. Copies of these lists and documentation are sent to the originating department or its successor.

Where the Historical Archives Service reviews transferred files that are not subject to a retention list, it must first submit the lists of files proposed for elimination to the originating department or its successor for approval.

⁴¹ Storage media include paper, tapes, hard drives and any other physical material with recorded data.

11.9. Rules governing the transfer of files

Commission departments must cooperate with the Historical Archives Service when preparing transfers. After the Historical Archives Service has accepted, the document management officer can transfer the files and records to the historical archives.

All transferred files must be accompanied by a transfer form and include the metadata required for the appropriate reception and processing of the files by the Historical Archives Service. The transfer form must be signed by the document management officer acting under the authority of their director-general or head of department and countersigned by the Historical Archives Service.

Departments should transfer records containing classified information only after declassification. However, they must transfer the metadata of records containing RESTREINT UE/EU RESTRICTED information at the end of the ARP of the files in which they are kept.

Files for which the metadata are not fully available must nevertheless be reviewed and transferred.

Responsibility for the content of files is transferred to the Historical Archives Service after a maximum of 30 years⁴².

11.10. Transfer and elimination metadata

Following first review, in addition to the acquired metadata⁴³, transfer metadata must be added to all transferred archives.

Where records and files are eliminated in the original official electronic repository, their metadata are sent to the official electronic file repository for definitive or historical archives as evidence of their elimination.

Following first or second review, elimination metadata must be preserved permanently in the references of eliminated files.

11.11. Responsibilities concerning files and records transferred to the Commission's historical archives

Each Commission department must:

- a) if requested, help the Historical Archives Service to assess the historical value of transferred files during second review;
- b) regularly review classified RESTREINT UE/EU RESTRICTED information and cooperate with the Historical Archives Service to review sensitive non-classified information⁴⁴, with a view to declassification or ascertaining whether the exceptions for sensitive records continue to apply;

⁴² Under Regulation (EEC, Euratom) No 354/83.

⁴³ This concerns capture, registration, filing and preservation metadata, and metadata for electronic and digitised records.

⁴⁴ Within the meaning of Article 2(1), (2) and (3) of Regulation (EEC, Euratom) No 354/83.

- c) continue to process all access requests from other EU institutions, agencies and other bodies until the archives have been opened to the public; and
- d) continue to process public access requests in accordance with Regulation (EC) No 1049/2001 until the archives have been opened to the public.

11.12. Processing of records and archives created before the implementation of Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom

These implementing rules can also be applied to records, files and archives created before the implementation of Decision 2002/47/EC, ECSC, Euratom and Decision 2004/563/EC, Euratom.

Commission departments may apply different rules after consulting the Secretariat-General and, as regards activities after the end of the ARP, with the agreement of the Historical Archives Service.

12. COMMISSION'S HISTORICAL ARCHIVES SERVICE

The Historical Archives Service is responsible for:

- a) examining requests for transfer to the Commission's historical archives, advising departments on their quality and accepting those that comply with the obligations set out in the Decision and these implementing rules;
- b) ingesting transferred files and related records into the Commission's analogue and electronic repositories;
- c) providing archival descriptions of files and archives in accordance with recognised international standards;
- d) ensuring the physical protection and integrity of all transferred archives in accordance with the above rules;
- e) ensuring the preservation and integrity of the file metadata provided by transferring departments;
- f) managing the repositories for the long-term preservation of the archives;
- g) making records and files available, upon request, to the departments;
- h) forwarding requests for access to documents and files from other parties to the originating department or its successor for action;
- i) processing, in accordance with Regulation (EC) No 1049/2001, all requests for public access to documents that have been transferred to the historical archives but not yet opened to the public, in cases where the department no longer exists and a successor department cannot be identified⁴⁵;
- j) establishing general criteria for the second review of files;

⁴⁵ e.g. requests for public access to documents from a former task force set up by the President to deal with particular matters or from a former cabinet. In such cases, the Historical Archives Service must consult the department that is currently responsible for the policy area concerned.

- k) conducting, where applicable, the second review of files, either asking for the cooperation of the originating department or its successor or at least informing the latter before eliminating any files;
- l) reviewing records containing classified and sensitive non-classified information, where applicable in cooperation with the departments concerned or their successors, with a view to their declassification or determining whether exceptions for sensitive records continue to apply. Such a review must take place no later than 25 years after the closure of the files concerned and, where necessary, at least once every 5 years thereafter; and
- m) ensuring that the Commission's historical archives are open to the public after 30 years in accordance with Council Regulation (EEC, Euratom) No 354/83 and that, as far as possible, they are made available by electronic means.

13. DEPOSIT OF THE COMMISSION'S HISTORICAL ARCHIVES AT THE EUROPEAN UNIVERSITY INSTITUTE (EUI)

13.1. Deposit

- a) The historical archives that have been opened to the public are to be deposited at the Historical Archives of the European Union at the EUI in accordance with the annex to Regulation (EEC, Euratom) No 354/83. Deposits must take place at least once a year.
- b) The Commission must provide descriptions of the deposited archives. These descriptions must be in line with recognised archival standards and accompanied by an overview, e.g. transfer lists, of the deposited material.
- c) The Commission must provide for the transport of the non-digital archives to the EUI and bear any associated insurance costs.

13.2. Public access

- a) The Commission must cooperate with the EUI as the primary point of public access to its historical archives. In addition, it may, where necessary, also provide direct access to its own historical archives.
- b) The Commission must cooperate with the EUI where possible to promote access to its own historical archives and to the related guides and inventories via the Archives Portal Europe.

Chapter III

Governance and implementation

14. COORDINATION AND MONITORING BY THE SECRETARIAT-GENERAL

The Secretariat-General is responsible for coordinating records and archives management and Commission departments' compliance with the common standards on:

- a) the capture of information, including the registration of records;
- b) the filing and management of files;
- c) the preservation of files; and
- d) the appraisal and transfer of files to the Commission's historical archives.

Directors-general and heads of department must inform the Secretariat-General of all agreements⁴⁶ they conclude with external bodies in their area of competence and of the validation procedure for quality control (see point 4.3), in view of possible harmonisation on the basis of the most effective criteria.

14.1. Capture of information

On the basis of criteria established in cooperation with DIGIT, the Secretariat-General must check that the IT systems used by departments that create or receive information to be captured comply with the Decision and these implementing rules.

14.2. Filing and management of files

The Secretariat-General is to:

- a) update the common nomenclature applicable to all departments;
- b) monitor the terminology used in the common nomenclature and its links with the filing plan headings that fall under the exclusive responsibility of the departments;
- c) provide and maintain the IT application for managing the Commission's electronic filing plan, including the file list management module; and
- d) monitor departments' implementation of the rules on filing and the management of files.

14.3. Preservation of files

The Secretariat-General is to:

- a) regularly update the CRL in accordance with upcoming administrative needs or change of working methods, in close cooperation with the departments; and
- b) provide a suggested methodology for compiling SRLs.

⁴⁶ Within the meaning of Article 2 of the Decision.

The Secretariat-General must be informed at once of any irregular destruction of archives or any serious infringement of the preservation rules.

14.4. Appraisal and transfer of files to the Commission's historical archives

The Secretariat-General is to:

- a) in close cooperation with the Historical Archives Service and the Commission departments, take steps to ensure that procedures and instructions are consistent;
- b) in close cooperation with the Historical Archives Service and the network of document management officers, establish general criteria for the first review of files; and
- c) deploy IT tools for the appraisal, transfer and management of archives, in close cooperation with DIGIT and the Historical Archives Service.

15. DOCUMENT MANAGEMENT OFFICERS

15.1. Implementation in Commission departments

Commission departments are responsible for implementing the Decision on records management and archives. Each director-general or head of department must take the necessary steps to ensure that the data, information, records, archives, procedures and electronic systems for which their department is responsible fulfil the requirements of this Decision and these implementing rules.

For this purpose, departments must provide the necessary IT infrastructure, IT systems, networks, means of transmission, suitable storage areas for electronic and paper media, and the necessary resources for the elimination of archives.

15.2. Document management officers

Each director-general or head of department must ensure that the document management officer of their department has the requisite professional qualifications to carry out the relevant tasks in this field.

Departments must consult the Secretariat-General when appointing their document management officer.

The document management officer is responsible for:

- a) identifying the types of record and file specific to the areas of activity of their department;
- b) establishing and updating the inventory of specific databases and IT systems managing information to be captured in one of the official repositories and informing the Secretariat-General of any new entry to check the compliance of its activity with the Decision and these implementing rules;

- c) maintaining and updating the parts of the filing plan relating to their department and ensuring compliance with the rules on filing;
- d) keeping up to date the list of all open and closed files with information on their media, storage, location, retention period, post-ARP action and internal procedures and actions to implement the preservation rules, including reference to the stakeholders involved and their responsibilities;
- e) establishing, implementing and updating the rules and procedures specific to their department that, notwithstanding the Decision and these implementing rules, are used to manage records and files and to monitor their application;
- f) monitoring the drafting of metadata for records and files and the inventory of the department's archives so as to ensure the ongoing smooth operation of the procedures for access to records, transfers to the historical archives and opening archives to the public;
- g) ensuring within their department that staff responsible for implementing, checking and monitoring the rules for managing records and archives set out in the Decision and these implementing rules receive adequate training;
- h) ensuring that all staff in their department are aware of their responsibilities as regards records and archives management, as set out in the Decision and these implementing rules, and that they follow training that enables them to fulfil these responsibilities;
- i) coordinating, within the meaning of Article 20 of the Decision, the document management team(s) that have been created to assist the document management officer and other staff in the department;
- j) maintaining relations with the Secretariat-General, the Historical Archives Service, DIGIT and any other department that may be involved in the performance of their duties;
- k) helping to uphold the 'need to know' principle and to conduct security risk assessments for records and files;
- l) reporting security and information security incidents to their department's local informatics security officer and local security officer; and
- m) reporting to the data protection coordinator of their department any cases of (potential) personal data breaches that have come to their attention.

15.3. Professional competences of records management and archives staff

The Secretariat-General ensures that document management officers and other specialised records management and archives staff have the competences and professional skills to carry out their tasks.

To this end, it will need to develop and maintain a competence framework, which will be the basis for the recruitment and professional development of such staff.

The Secretariat-General will need to cooperate with DG HR to provide in-house training, so as to maintain and improve the professional skills and competences of such staff. Training in records and archives management must also be made available to all staff to improve general awareness and knowledge of the relevant procedures and tools.

16. PREVIOUS ACTS

The rules implementing Decision 2002/47/EC, ECSC, Euratom⁴⁷ and Decision 2004/563/EC, Euratom⁴⁸ (as adopted on 30 November 2009⁴⁹) no longer have effect.

⁴⁷ Commission Decision 2002/47/EC, ECSC, Euratom of 23 January 2002 amending its Rules of Procedure (OJ L 21, 24.1.2002, p. 23).

⁴⁸ Commission Decision 2004/563/EC, Euratom of 7 July 2004 amending its Rules of Procedure (OJ L 251, 27.7.2004, p. 9).

⁴⁹ SEC(2009) 1643.