



e-Domec: File and document management in the unit – for secretaries

CTO EDOMECE SECR



Training developed for the European Commission by
Accenture under the terms of a framework contract.

www.accenture.com



This training manual complies with EMAS rules.



Contents

INTRODUCTION: PRESENTATION OF COURSE OBJECTIVES	4
I. CONTEXT AND OBJECTIVES	5
1. Several objectives, a single policy	5
2. Legal foundations and obligations.....	6
2.1. Direct legal texts.....	6
2.2. Associated legal texts.....	7
3. The key actors in document and file management in the DG/Services.....	9
II. PRINCIPLES OF RECORDS MANAGEMENT	12
1. Document management operations	12
2. The records life cycle and the administrative cycle.....	12
III. DOCUMENT REGISTRATION	15
1. Why register ?	15
2. Analysis or identification of documents to be registered	15
2.1. Document form	16
2.2. Document origin	16
2.3. Verification of registration conditions	16
2.4. Protection of personal data.....	19
2.5. Classified documents and security markings	20
2.6. Role of the file manager	23
3. Registration.....	25
3.1. Metadata or descriptive data for a document to be registered	25
3.2. Attachment of the electronic version of the document.....	25
3.3. Registers and applications with equivalent effect	27
IV. FILING: FILES AND FILING PLAN	34
1. Why file?.....	34
2. Official file and working file	34
2.1. Definition of a file	34
2.2. Types of files.....	35
2.3. Lead Department responsibility.....	37
3. Creation of an official file	38
3.1. Creation of an official file.....	38
3.2. Proper file identification: action file and serial file	39
3.3. Attachment of files to the filing plan.....	40
3.3. The official file management tool: the file list	42
4. Filing documents	42
4.1. Choosing the correct file for filing	42
4.2. File consisting of documents registered in different applications	44
4.3. Role of file manager.....	44
V. MANAGEMENT OF CURRENT RECORDS	45
1. Electronic and/or paper retention ?.....	45
1.1. Validity of electronic documents	45
1.2. Management of a hybrid file (electronic and paper)	47
2. Retention sites for official paper files	48
2.1. Filing and storing	48
2.2. Unit storage plan	50
2.3. Organisation of documents in a file.....	50

2.4. Organisation of the unit shared drive	51
3. Access to attachments and files.....	51
3.1. Searching for documents/files in Ares	51
3.2. Consultation and borrowing of official paper files	52
4. Public access to documents.....	52
4.1. Basic rule	52
4.2. Exceptions.....	52
VI. CLOSURE AND RETENTION PROCEDURES	54
1. A fundamental action: closing files.....	54
1.1. Deadline for closure	54
1.2. Rules of closure	54
1.3. Date of closure	55
2. Retention procedures.....	57
2.1. Objectives	57
2.2. The Common Retention List	57
2.3. The archive schedule	59
3. Retention implementing rules	59
3.1. Calculating the ARP.....	59
3.2. Organisation of intermediate records	60
3.3. Review and transfer of files to the Historical Archives.....	60

INTRODUCTION: PRESENTATION OF COURSE OBJECTIVES

This manual is intended for participants in the training course entitled "e-Domec: File and document management in the unit – for secretaries".

The general objective of this training is for participants to know and be able to apply the recommended procedures for document registration and filing and the preservation of documents and files in their DG/Service.

The manual, which is issued to participants at the end of the course, summarises all the points addressed during the course, and should enable participants to find all the necessary information they may need in order to:

- understand the Commission's policy framework
- become familiar with the life cycle and administrative cycle of documents and files: from their creation/receipt to their transfer to the Historical Archives
- acquire a working method for mastering various management tools (list of files, filing plan, preservation plan,...)
- understand the basic obligations of file and document preservation.

For any further information, please contact your DMO (Document Management Officer¹) or your COFO (Training Coordinator)

¹ List: <http://www.cc.cec/home/dgserv/sg/edomec/index.cfm?lang=en&page=photosdmo>

I. CONTEXT AND OBJECTIVES

An institution such as the European Commission is both a producer and a user of information. In order to rationalise the production, retention and access to documents drawn up and received in the course of its activities, as from January 2002 the European Commission has established a records management policy: **e-Domec** (Electronic archiving and Document Management in the European Commission). This policy also applies to the Executive Agencies and the European External Action Service.

1. Several objectives, a single policy

Proper records management ensures that departments retain records of their activities in order to

- ensure they have robust, legally admissible evidence of their work;
- provide accountability and transparency for their actions and decisions;
- guarantee rapid and easy access to information; amongst other benefits, this means that decisions can be taken as rapidly as possible;
- reinforce security;
- improve the quality and continuity of public service;
- reduce administrative costs and save time.

e-Domec: Electronic archiving and Document Management in the European Commission.

This records management policy was formally launched by the Commission in January 2002, with the adoption of the basic normative framework establishing the rules and procedures of records management (Commission Decision 2002/47).

e-Domec is designed to ensure:

- preservation of the European Commission's institutional memory;
- an improvement in the quality of files within units;
- greater standardisation of procedures: rules and procedures common to all Directorates-General/Departments;
- monitoring and accountability to oversight bodies (IAS, OLAF, European Court of Auditors, European Parliament);
- transparency with regard to European citizens;
- the integration of ICT (Information and Communication Technology) and evolution towards the e-Commission with the introduction of electronic archiving.

2. Legal foundations and obligations

These texts may be consulted via the *e-Domec* Intranet website.

2.1. DIRECT LEGAL TEXTS

➤ 2.1.1. Fundamental decisions

◆ **Commission Decision 2002/47/EC, ECSC, Euratom**

Provisions concerning document management

- Art. 1: Definitions of documents and files
- Art. 2: Objectives of the document management system
- Art. 3: Presentation of document management operations: registration – filing – retention – transfer of files to the Historical Archives
- Art. 4: Registration
- Art. 5: Filing
- Art. 6: Retention
- Art. 7: Pre-selection and transfer to the Historical Archives
- Art. 8: Treatment of classified documents
- Art. 9: Role of the Document Management Centres
- Art. 10: Role of the Document Management Officer (DMO)
- Art. 11: Role of the Interdepartmental Group of DMOs
- Art. 12 – 15: Adoption and implementation of rules

◆ **Commission Decision 2004/563/EC, Euratom**

Provisions concerning electronic and digitised documents (DOCELEC)

➤ 2.1.2. Implementing rules for the founding texts

◆ **Implementing rules for Decision 2002/47/EC, ECSC, Euratom on document management and for Decision 2004/563/EC, Euratom on electronic and digitised documents: SEC(2009)1643**

- Chapter II.2 – Registration
- Chapter II.3 – Filing
- Chapter II.4 – Retention
- Chapter II.5 – Appraisal and transfer to the Historical Archives
- Chapter III – Electronic and digitised documents
- Annex 1 – List of metadata
- Annex 2 – Criteria to be respected by any registration system
- Annex 3 – Definition of key concepts relating to registration criteria
- Annex 4 – Structure of the Common Retention List
- Annex 5 – Exceptional rules applicable to the transfer of files
- Annex 6 – List of priority electronic procedures

◆ **Common Retention List (CRL): SEC (2007) 969-970**

Regulatory document that sets retention periods for the various types (also called "categories") of Commission files.

2.2. ASSOCIATED LEGAL TEXTS

➤ **Internal control standards for efficient management**

Of the 16 internal control standards, standard no. 11 refers directly to correct document management and five other standards have direct repercussions on obligations regarding document and file management in Directorates-General and departments:

- **n°6:** "Risk management process": risk management encompasses the protection of information.
- **n°8:** "Processes and procedures": drawing up adequate documentation on the operational and financial processes and procedures implemented by a DG, and on information systems. This documentation must be user-friendly, accessible and kept up to date.
- **n°9:** "Management supervision": Management at every level supervises the activities for which it is responsible and keeps track of the main problems identified. This managerial supervision covers matters of legality and regularity, as well as operational performance.

In particular, a unit manager must be able to guarantee that a reliable and comprehensive official file exists for every case on which her/his unit is Lead Department.

- **n°10:** "Business continuity": Appropriate provisions must be in place to ensure continuity of service in the event of a "normal" interruption of activity. This includes transmission files and backup systems for financial transactions and operational activities.
- **n°11:** "Document management": Appropriate procedures and processes must be in place to guarantee safe and effective document management, in particular to ensure that the necessary information can be readily found. This standard entails that any document meeting the conditions set out in the implementing rules must be registered, filed in an official file and retained for the period stipulated by the document management rules.

It is essential in particular to guarantee that all staff are familiar with registration, filing and retention procedures and apply them in practice in the Directorates-General and departments.

- **n°13:** "Accounting and financial reporting": Adequate checks and procedures are in place to guarantee that accounting data and related information used in the preparation of the organisation's annual accounts and financial statements is accurate, comprehensive and available in timely fashion. This implies an obligation for all staff concerned to keep accounting and financial documentation up to date and accessible.

➤ **Provisions on security**

Commission Decision 2001/844/EC, CECA, Euratom, dated 29 November 2001: Introduction of a global security system for all fields of Commission activity requiring a certain degree of confidentiality, and determination of the conditions applying to the management of classified EU information and to the declassification of documents.

➤ **Provisions on the protection of personal data**

Regulation (EC) n° 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data.

➤ Financial regulation

Regulation (EC, EURATOM) n° 1605/2002: basic precepts and rules governing the Community budget: budgetary and financial management, keeping and presentation of accounts, public procurement and the award of grants, liability of authorising officials, accounting officials and internal auditors, and arrangements for external control and the discharge procedure.

Regulation (EU, Euratom) no. 1081/2010 of the European Parliament and the Council of 24 November 2010 amending Council Regulation (EC, Euratom) no. 1605/2002 on the Financial Regulation applicable to the general budget of the European Communities, as regards the European External Action Service.

➤ Public access to documents

Rules setting out the general principles and limits governing exercise of the right of access to documents held by the Commission (drawn up or received by the Commission and in its possession):

- **Regulation (EC) n° 1049/2001** of the European Parliament and of the Council, regarding public access to European Parliament, Council and Commission documents.
- **Commission Decision 2006/291/EC, Euratom** on the re-use of Commission information.

➤ Opening of Historical Archives to the public

Regulation n°1700/2003 of the Council amending Regulation (EEC, Euratom) No 354/83 concerning the opening to the public of the Historical Archives of the European Economic Community and the European Atomic Energy Community.

Proposal for a Council Regulation amending Regulation (EEC/Euratom) No. 354/83, as regards the deposit of the historical archives of the institutions at the European University Institute in Florence.

➤ Code of good administrative behaviour

Principles on which relations between the public and the Commission must be founded: lawfulness, non-discrimination, proportionality of measures to the aim pursued, consistency in administrative behaviour.

- **Decision 2000/633/EC, CECA, Euratom**, of 17 October 2000: Code of good administrative behaviour for staff of the European Commission in their relations with the public.

➤ EMAS

The Eco-Management and Audit Scheme

- **Regulation (EC) n° 761/2001:** a Commission environmental management programme aimed at reducing consumption of resources and the generation of waste. Compliance with archiving rules can have significant environmental impacts.
- **Commission decision C(2009)6873** on the application by Commission services of the Community eco-management and audit scheme (EMAS).

Pursuant to these texts, all DGs and Departments (including Cabinets) must:

- **Register** all documents received or formally drawn up as part of their activities
 - *Decision 2002/47 – Article 4 of the annex*
 - *Implementing rules – SEC (2009) 1643: Chapter II.2 - Registration*
- Establish a **filing plan** and set up **files**
 - *Decision 2002/47 – Article 5 of the annex*
 - *Implementing rules – SEC (2009) 1643: Chapter II.3 - Filing*
- **Retain** the documents and official files that are related to their responsibilities
 - *Decision 2002/47 – Article 6 of the annex*
 - *Implementing rules – SEC (2009) 1643: Chapter II.4 - Retention*
 - *Common Retention List – SEC (2007) 969-970*
- **Appraise and transfer** their files to the Commission's Historical Archives as per the Common Retention List
 - *Decision 2002/47 – Article 7 of the annex*
 - *Regulation 1700/2003 – Article 7*
 - *Implementing rules – SEC (2009) 1643: Chapter II.5 – Appraisal and transfer to Historical Archives*

3. The key actors in document and file management in the DG/Services

Document management is part of daily work and concerns everyone in the Commission:

- the Commission as an institution;
- the Directorates-General;
- equivalent departments, Cabinets, Offices, Delegations, etc.

Every agent of the Commission is thus anxious to respect rules and procedures in administration of documents and, in particular, to organize and to preserve all the documents and the files for which he is responsible.

Executive agencies and EEAS (European External Action Service) also apply the e-Domec rules².

➤ **Role of DMOs (Document Management Officers)**

Article 10 Decision 2002/47

- **Mandatory:** 1 per Directorate-General/Department
- **Recommended:** 1 DMO and 1 Deputy DMO

The DMO's mission covers:

- the design and introduction of the records management and archiving system in the DG: adaptation of general rules to the specific characteristics of the DG;
- training, information and advice for DG departments and officials;

² Unless otherwise specified, the abbreviation "DG" in this manual covers all the departments mentioned above.

- verification of the proper application of rules and procedures;
- crosscutting coordination with the CADs and/or network of DMO correspondents in the DG;
- interdepartmental coordination with DMOs in other DG/Departments;
- management and updating of two instruments:
 - the DG filing plan: organisation of files according to the DG's activities;
 - the archive schedule for the DG's files: establishing the rules and retention periods for official files after their closure.

➤ **Role of the Document Management Centre (known under the French acronym: CAD) and equivalent services**

Article 9 Decision 2002/47

- Their mission is to
 - guarantee that documents received or drawn up by each DG or equivalent department are managed according to the rules;
 - manage, organise and retain documents;
 - guarantee archive availability when needed;
 - apply the common retention list;
 - preserve the authenticity of documents;
 - apply the "Code of good administrative behaviour" in records management

➤ **Role of the unit/department staff**

◆ **DMO correspondent in the Unit**

- Acts as the link between the unit and the DG Document Management Officer (DMO): participates regularly in correspondent network meetings (in certain DGs, the CAD is made up of the group of DMO correspondents);
- under the auspices of the head of unit and in concertation with the DMO, implements e-Domec rules on registration, filing, archiving, appraisal and transfer of files within the department (who does what in the unit);
- provides training, information and advice to unit officials, and to newcomers in particular, on records management;
- alerts the head of unit and/or DMO in the event of failure to apply e-Domec rules;
- manages the unit's list of official files: creation, management and closure of official files in Ares (via Nomcom3);
- manages the storage plan: organises the physical retention of official paper files to guarantee their protection;
- implements retention rules for closed files, in accordance with the archive schedule.

◆ **Document managers (Secretary function)**

- Apply the rules governing records management and archiving;
- Responsible for the registration, filing and retention of documents, regardless of medium, in the systems provided for, under the supervision of the DMO (Document Management Officer) or of the head of the Document Management Centre (CAD);
- File documents in files;
- Communicate the files and documents required for the work of the unit/department;

- Receive, retain and locate documents and files for ease of access by those concerned.

II. PRINCIPLES OF RECORDS MANAGEMENT

1. Document management operations

The document management system must make it possible to organise, retrieve, protect and retain documents recording the institution's activities.

In order for the records management system to meet these objectives, it is essential that:

- documents of importance to the Commission should be identifiable, understandable and secure: **registration**;
- documents can be linked to the context in which they were received or produced: **creation of files**;
- useful documents and files can be found easily: **filing** in official electronic files and possible **storing** in supplementary official paper files;
- files are retained in a reliable and continuous manner throughout their life cycle: **retention**;
- files with no further administrative use are eliminated or transferred to the Historical Archives in accordance with the **Common Retention List**.

2. The records life cycle and the administrative cycle

The **life cycle** of a document / file corresponds to the stages or periods in the life of the document / file from its "birth" (creation or receipt by the department) and throughout its administrative processing until it is transferred to the Historical Archives or destroyed in accordance with regulations.

The life cycle is divided into **3 stages**:

- **Current records or open files**: official files open and in use by the departments that produced them.
 - Official electronic files are managed by e-Domec compliant applications (the shared hard drive is only storage space, and has no probative value).
 - Official paper files are generally retained in the offices or in close proximity (e.g. archives storage rooms on each floor).
- **Intermediate records**: closed files which must continue to be retained for administrative or legal reasons (for inspection, for example). DGs retain these files, in accordance with their archive schedule, throughout their administrative retention period (ARP).
- **historical records**: closed files which, depending on the appraisal rules applicable, are transferred to the Commission's Historical Archives Service (HAS) and selected for permanent retention in view of their historic interest.

During the first two phases, the DG is responsible for the oversight of registration, filing and storage systems designed for easy search and rapid, efficient document retrieval when necessary.

⇒ In parallel to the life cycle, records also have a corresponding **administrative cycle** that covers the various stages of records management:

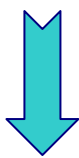
Life cycle		Administrative cycle
① Receipt/ creation of documents	⇒	<ul style="list-style-type: none"> - Analysis and registration: identification of the document and certification of its administrative value - Filing: association of the document with an official electronic file associated with a filing plan heading
② Current records = Open files	⇒	Active phase: <ul style="list-style-type: none"> - Retention and storage - Distribution and consultation - File closure
③ Intermediate records = Closed files	⇒	Semi-active phase <ul style="list-style-type: none"> - Retention and storage - Distribution and consultation Final phase: <ul style="list-style-type: none"> - Appraisal for destruction for files of no further value or transfer to Historical Archives for files with historical value.
④ Definitive archives		Files which, in accordance with the Commission's Common Retention List, are transferred to the Commission's Historical Archives and selected for permanent retention.

Document and file life cycle and administrative cycle

1. NEW CASE

- Creation of a new file
- Analysis and registration of the document
- Filing: Organisation of documents into files
- Storage/Consultation/Distribution

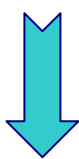
Constitution and use of CURRENT RECORDS:
Files used regularly in the management of current cases



2. END OF THE CASE

- Closing of files
- Retention of closed files during their ARP (Administrative Retention Period)

Management of INTERMEDIATE RECORDS:
Files closed but retained for administrative or legal reasons



3. END OF THE ARP

- Appraisal
 - Elimination
 - Transfer to the Historical Archives

Selection and transfer to DEFINITIVE ARCHIVES
Files with no further administrative value but retained definitively in view of their historical or political value

III. DOCUMENT REGISTRATION

1. Why register ?

Registration is the operation that attests to the administrative value of a document drawn up or received by a department as evidence of the activities, policies and decisions for which it is responsible.

Registration makes it possible to:

- identify the document with certainty,
- attest to the transmission and receipt of the document in accordance with established procedures,
- manage the document efficiently (assignment and follow-up) by guaranteeing its traceability throughout its life cycle,
- incorporate the document into the Commission archiving system: no modification or withdrawal possible without prior authorisation,
- quickly and easily retrieve useful information.

The document registration operation takes place in 4 stages:

1. Identification of documents to be registered: **analysis** phase;
2. Input of a document description sheet: **encoding** or input of **metadata**;

Metadata: data describing the context, content and structure of documents and their management over time.

3. Attachment of the document in electronic format to the description sheet;
4. Administrative follow-up: assignment, distribution, schedule, etc.

2. Analysis or identification of documents to be registered

"As soon as a document is received or formally drawn up within a department, in whatever medium, it shall be analysed with a view to determining what is to be done with it and thus whether or not it must be registered."

Source: C(2002) 99 final. Annex: Provisions on document management: Art. 4

Not all documents need to be registered: analysis of the content and context of a document received or drawn up is used to distinguish between:

- Documents that the department absolutely must retain because they contain important information, involve follow-up/action on the part of the Commission, have been endorsed and signed by the competent official and will form part of an official file.
- Documents that need not be retained and that are not subject to registration.

2.1. DOCUMENT FORM

Commission definition of a document

(Decision 2002/47/EC art. 1)

Any content drawn up or received by the Commission concerning a matter relating to the policies, activities and decisions falling under the institution's mandate and in the framework of its official tasks, in whatever medium (written on paper or stored in electronic form or as a sound, visual or audio-visual recording).

Whatever its form and medium, prior to registration the document must be checked for:

- **authenticity**: it is possible to identify without ambiguity the author, principal addressee, date of creation/issue/receipt/processing of information.
- **reliability**: the content may be considered as a complete and accurate representation of the operations, activities or facts attested, and may serve as a reference in subsequent operations, activities or facts.
- **integrity**: the information contained in the document and the relevant metadata are complete and correct (the document has undergone no formal modification).
- **exploitability**: location of the document (index number for a paper document or URL for an electronic document) and legibility over time.

2.2. DOCUMENT ORIGIN

A document may be:

- **A received document**: a document addressed formally to the entity concerned in the Commission.
- **A drawn up document**: a document designed and finalised within a distinct unit, regardless of its format and medium.

2.3. VERIFICATION OF REGISTRATION CONDITIONS

➤ 2.3.1. Documents to be registered

The identification of documents to be registered, or "**analysis**", consists of analysing both the **content** and the **context** of a document received or drawn up, in order to determine whether or not it should be officially registered.

- ⇒ Any document, regardless of medium, must be registered if it meets 3 conditions:
- ① Received or formally drawn up by a Commission department as part of its activities
- and
- ② **a)** Likely to involve action or follow-up, or to require a reply from the Commission or its departments
- or
- b)** establishes a commitment for the Commission or its departments
- and
- ③ Contains important information that is not short-lived
- ⇒ Documents drawn up to provide evidence of acts or intentions or to further understanding of the case should also be registered (for example: briefings).

VERIFICATION OF REGISTRATION CONDITIONS

① Was the document formally drawn up or received by a Commission department as part of its activities?

Documents received:

Check whether the document has been correctly received, i.e. is **available** to the department(s) to which it is addressed:

- document reaching the premises of the department
or
- document handed to the official competent to handle the case to which the document refers
or
- document handed to the official competent to receive and process incoming documents.

Documents drawn up:

Check whether the document has been subject to **formal transmission** by its author (person or entity formally responsible for the document content), i.e. if it was considered ready for transmission to its final addressee (individual, department or information system).

⇒ Registration is the final operation before sending on the document to its final addressee.

N.B.: A document ready for transmission is not necessarily the final version of the document; Significant drafts of a document may also be considered ready and be subject to registration.

And

② Does the document involve action, follow-up or reply, or is it binding upon the Commission or its departments?

Any document on a subject relating to the policies, activities or decisions of the Commission or its departments is binding upon the Commission.

And

③ Does the document contain important information that is not short-lived?

Any document that contains important information that is not short-lived must be registered. Information is considered unimportant and short-lived (i.e. useful for only a very short period of time):

- if the loss of the information involves no negative administrative or legal impact on the Commission,
- or if its value is clearly only temporary and destined to disappear shortly (in less than six weeks),
- or if its value is clearly ancillary (it is not the main information) or instrumental (it is only a means of implementing an action defined in another document).

Or

④ Has the document been drawn up as effective administrative or legal witness to acts, situations, intentions or events associated with the activities of the Commission and its departments?

Any document that meets these conditions **must** be registered by the department concerned.

⇒ For precise information on the documents that must be registered, contact the **DMO** (Document Management Officer), who is responsible for defining the practical procedures implemented by the DG in accordance with the regulatory texts.

➤ 2.3.2. Exceptions to the registration requirement

◆ General exceptions

Certain documents need not be registered, even if they meet all the required conditions, **as long as** other procedures guarantee results equivalent to those of registration:

- Documents distributed in multiple copies to Commission departments and checked by another responsible body (such as COM, SEC, C);
- Documents whose processing and retention are managed by a reliable procedure (MIPS or SYSPER2 applications, for example);
- Documents and communications exchanged between departments without specific formalities (e-mails exchanged informally and in good faith for comment and consultation between Commission departments).

◆ Registration and Code of good administrative behaviour

Recommendation on registration of replies to requests for information and exchanges of correspondence with the public pursuant to the code of good administrative behaviour

(Note to Document Management Officers – SG.B.3/MH D(2005)2687 – 17 March 2005)

Any exchange of correspondence with the public pursuant to the code of good administrative behaviour and which does not contain information that is important and not short-lived need not be registered in Ares. This applies particularly to requests for information of a general nature (request for information which, in reply, does not require examination of the particular case presented but can be answered by a simple form letter or referral to the Commission website).

In order to keep a trace of the request and justify the work performed, however, it is recommended that such requests and replies be simply saved (in a “Replies” file kept on an annual basis and eliminated after two years).

Example:

A 2010 file entitled "2010 requests for general information and replies" closed at the end of 2010 can thus be eliminated at the beginning of 2013.

➤ 2.3.3. Procedural constraints

◆ Public procurement procedures: registration of tenders

In files relating to public procurement procedures, tenders are important documents that have to be registered. But one has to take the procedural constraints into consideration:

- It is not allowed to open the tenders as they are received: they can therefore not be registered and scanned into ARES until after the opening of tenders meeting;
- The "record of opening of tenders" (standard form provided by DG BUDG), list of received tenders, their origin, date of submission and whether they are in order or not (tenders that are not in order are not opened. To guarantee the identification of the tenders, noting the moment when they were received and their follow-up suffices.
 - ⇒ It must be registered in ARES.

Also, the following procedure is recommended:

1. The registration of the "record of opening of tenders" can replace the individual registration of each tender.

It is up to the responsible authorising officer, or possibly the Director-General, to request, in addition, the registration of each individual tender.

2. Whether the tenders are registered individually or not, it is possible to digitize them, but not obligatory nor even recommended when the tenders consist of a substantial number of pages.

However, it is up to the responsible authorising officer to decide whether the tenders will only be kept in paper form or whether all tenders have to be scanned in their entirety or only the first page of each.

Copies of the tenders have to be destroyed after signing the contract: only the originals have to be preserved.

3. It is recommended to guarantee the confidentiality of the tenders until their destruction after the archiving period (5 years for rejected tenders, 10 years for the public procurement file containing the original winning tender) or until their transfer to the Historical Archives (a representative percentage of these files will be kept for historical purposes).
4. Regardless of the decisions taken, it is important that the departements know where the paper version of the tenders can be found, from the moment they are received and during their treatment, and then whether they are archived or destroyed.

2.4. PROTECTION OF PERSONAL DATA

Personal data is any information that makes it possible to identify a particular individual.

The protection of personal data is a primary requirement for the Commission. It applies equally to correspondence from citizens (unsolicited job applications, in particular) and to members of staff.

➤ 2.4.1. Administration of personal data

Personal data must be:

- administered equitably and in accordance with the law, for limited and clearly stated purposes,
- adequate and relevant,
- kept accurately and up to date,
- retained for as long as necessary,
- kept securely,
- protected from transfer to third parties without adequate precautions being taken.

The official responsible for data protection must be informed of the administration of personal data.

Recommendation on the registration of personal data

(Note to Document Management Officers – REG SG D(2005) D 1102 – 8 February 2005)

1) CVs and unsolicited job applications:

The HR DG operates an Internet portal entitled "EU CV on line"³ for the use of citizens wishing to submit unsolicited applications, including applications from winners of open competitions.

In addition, applicants should contact the DG Human Resources Department for information on the procedure to be followed for the DG in question.

2) Unit or DG/Department personnel files:

Official personnel files are managed exclusively by DG HR. Any other employee file, managed at unit level, can therefore only be a working file.

⇒ It is forbidden to:

- create an official file based on the name of a specific DG employee
- put names of individuals in the subject of the document.

⇒ It is essential to:

- consult the DMO on procedures to centralise these files by the HR unit and on destruction procedures (including for unsolicited job application files).

➤ **2.4.2 Exceptions to the transfer of personal data**

Exceptions to the transfer of personal data are made:

- with the agreement of the individual concerned,
- in the interests of the individual concerned,
- when legally necessary on the grounds of significant public interest,
- when the transfer emanates from a public register.

For any questions, please contact the DG DPC (Data Protection Controller)

2.5. CLASSIFIED DOCUMENTS AND SECURITY MARKINGS

Documents handled on a daily basis may be classified into five categories:

1. Unclassified documents accessible to the public
2. Unclassified documents not accessible to the public
3. Sensitive documents protected by a level of marking
4. Classified documents not subject to specific controls: documents classified Restreint UE
5. Classified documents.

➤ **2.5.1. Classified information**

◆ **The levels of classification**

Classification involves the allocation of a security level to a document whose unauthorised disclosure could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, whether such information/material originates within the EU or its Member States, or within non-member States or international organisations.

Four levels of classification exist, in descending order of importance:

³ http://ec.europa.eu/civil_service/job/cvonline/index_en.htm

- "TRES SECRET UE"/"EU TOP SECRET" documents: information and material whose unauthorised disclosure could cause **exceptionally grave** prejudice to the essential interests of the European Union or of one or more of its Member States.
- "SECRET UE" documents: information and material whose unauthorised disclosure could **seriously harm** the essential interests of the European Union or of one or more of its Member States.
- "CONFIDENTIEL UE" documents: information and material whose unauthorised disclosure could **harm** the essential interests of the European Union or of one or more of its Member States.
- "RESTREINT UE" documents: information and material whose unauthorised disclosure could **be disadvantageous** to the essential interests of the European Union or of one or more of its Member States.

Security markings are not a classification but a “handling instruction” indicating how the document so marked is to be treated. This has particular consequences on the visibility of the document (definition of the individuals or groups allowed access to the document).

The full list of security markings applicable is drawn up by the Security Directorate of DG HR⁴.

◆ Registration of classified documents

Classified documents are subject to special handling even within the Commission.

- **Documents classified as "TRES SECRET UE", "SECRET UE" and "CONFIDENTIEL UE"**: may not be registered in Ares, only in special registers.
- **"RESTREINT UE" documents**: must be registered in Ares, but without attaching the electronic version of the document.
 - The "Subject" field should show the title of the document, modified if necessary so it contains no reference to classified or protected information
 - A "Restreint UE" document should never be sent using Outlook (not even with SECEM) or any other equivalent electronic channels. If the document must be sent digitally, only the **RUE** (RESTREINT UE) IT system is allowed, which enables a predetermined group of users to create, archive and transmit "RESTREINT UE" documents .

For any questions, please contact the **LSO (Local Security Officer)** of your administrative unit.

➤ 2.5.2. Sensitive information

Sensitive information concerns all types of documents and information involving an element of confidentiality and thus requiring some form of protection, without coming under the formal classification system. This concerns information that must be protected for legal or contractual reasons.

The loss, misuse or disclosure of such information could be prejudicial to the interests of an individual (information of a private nature, medical information, information covered by medical confidentiality, disciplinary matters, etc.), to the commercial

⁴ Cf Security notice 1:

http://myintracomm.ec.europa.eu/corp/security/EN/RulesLegislationAgreements/securitynotices/Documents/sn_1_marking_en.pdf

interests of a company (competition, etc.), to the confidentiality of legal affairs, etc. but would cause **no harm** to the interests of the European Union or of one or more of the Member States.

◆ Sensitive information and security markings

Sensitive information must be indicated in Ares by the use of **security markings**:

- Documents with security markings must be registered in Ares **with the electronic version of the document attached** and selecting the appropriate marking. Depending on the marking used, it may be possible to indicate an expiry date.
N.B.: adding an expiry date is strongly recommended.
- Security markings are not a security classification but a "**handling instruction**". They are used either to supplement a classification level or to restrict access to or circulation of an unclassified document.
- The full list of security markings applicable is drawn up by the Security Directorate of the DG HR⁵.

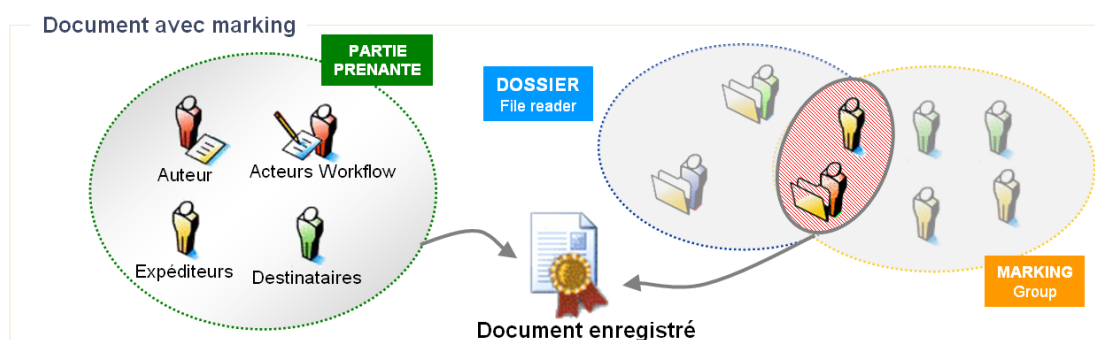
The use of a security marking has particular consequences on the visibility of the document (access is granted only to those members of staff with a "need to know" for the purposes of their work).

◆ Visibility of a document with security marking

The use of a security marking limits the document's visibility in Ares and NomCom at the time of its filing and the restricted visibility of a document with a security marking only affects the file readers:

- Prior to filing, documents – with or without a security marking – are accessible only to their stakeholders (creator, workflow actors, senders and recipients).
- After filing – for operational reasons – documents with a security marking continue to be accessible to the stakeholders even if they are not part of the user group associated with the security marking. File Reader access, however, is limited solely to members of the user group associated with the security marking.

⇒ As a result, a file may contain documents with limited access rights (with security marking) and documents with more open access (no security marking).



⁵ Cf security notice 1:

http://myintracomm.ec.europa.eu/corp/security/EN/RulesLegislationAgreements/securitynotices/Documents/sn_1_marking_en.pdf

2.6. ROLE OF THE FILE MANAGER

The file manager plays an essential role in ensuring compliance with registration requirements. The file manager must:

- transmit or indicate to the department/individual responsible for registration all documents to be registered
- remember to have “certifying” e-mails registered

Rules for the composition of “certifying” e-mails”:

E-mail is an increasingly important tool for swift, easy communication. It can be used to replace simple spoken communication or telephone calls (informal e-mail), but can also be used for formal written communication, both internal and external (certifying e-mail).

⇒ A certifying e-mail is a document that is binding upon the Commission (formally received or drawn up by a Commission department as part of its activities): as such, it must be registered.

As with any administrative document, there are certain basic principles of composition to be known and respected:

- 1) 1 single topic
- 2) 1 significant object
- 3) Clear identification of the author and signatory: use of a “signature block” or visiting card
- 4) Clear identification of the main addressee: full name and address in the address book or indication in the addressee message header (on the same principle as a printed letterhead)
- 5) Indication in the body of the message of the list of attachments (attachment name and document titles)
- 6) Indication, where necessary, of whether the paper document follows by post
- 7) Indication of the registration number in the object of the e-mail

Registration of an e-mail with attachment(s)

Any attached documents are also registered under the same registration number.

Registration of a series of e-mails:

In the case of a series of successive e-mails on the same subject, only the final e-mail can be registered, with no retroactive registration of preceding e-mails (each being not significant independent of the others). In this instance, the registration metadata are those of the final e-mail.

- Check regularly that the official file is complete

Useful hint:

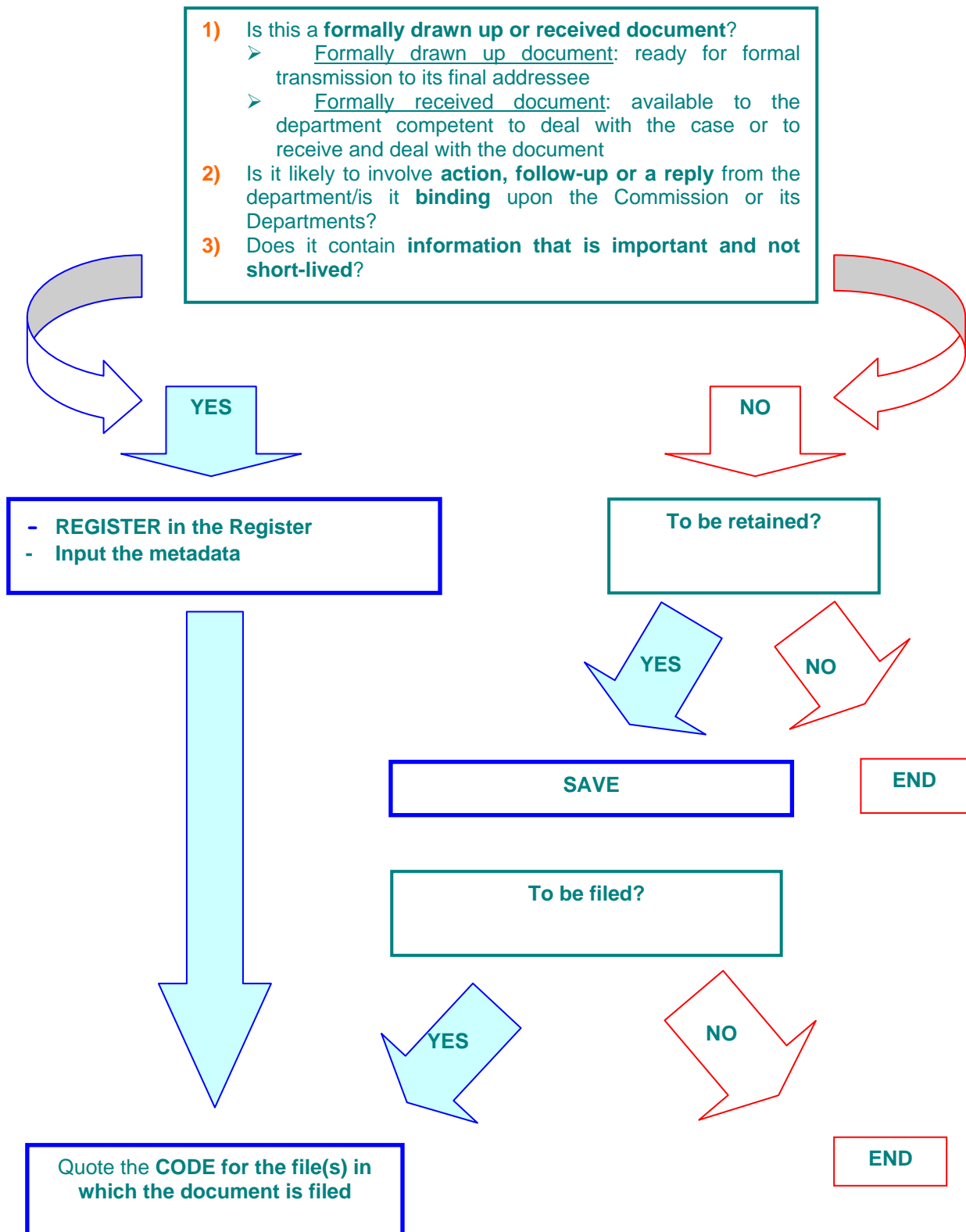
An official file must contain all documents that are binding upon the Commission or useful to its life and activities.

To check whether this is the case, ensure that all documents that may be useful in the event of:

- disputes
- audit
- transmission of the file

have been registered.

Document analysis and registration



3. Registration

3.1. METADATA OR DESCRIPTIVE DATA FOR A DOCUMENT TO BE REGISTERED

Registration is intended to provide for clear, definite identification of documents drawn up or received by the Commission or one of its departments, in such a way as to guarantee the traceability of the documents concerned throughout their life cycle.

Registration makes it possible to:

- identify the document with certainty
- attest to the document's:
 - origin: author, addressee, dates (of receipt, of sending or of integration into the system);
 - transmission by its author to an addressee;

In order to do so, descriptive information (known as "**metadata**") is included when the document is registered, in an operation known as **encoding**.

Identifying elements are indicated as needed, particularly as regards search for and use of documents. These elements must be as standardised as possible; it may be helpful to consult checklists and procedural manuals:

- ⇒ A document must be registered as soon as possible after it has been formally drawn up or received.
- ⇒ Correct input of metadata makes it easier to search for documents and to find supporting documents easily.

3.2. ATTACHMENT OF THE ELECTRONIC VERSION OF THE DOCUMENT

Except in specific cases (classified documents, documents with OLAF or COMP markings, documents that cannot be digitised), the electronic version of the document must be attached to the Ares registration sheet.

⇒ **In Ares:**

- Registration is only possible if the electronic version of the document is attached to the registration sheet. It is impossible to add an attachment after registration.
- Only translations of the document may be attached after registration.
- Each document attached must be identified by type: Cover note/Main document/Annex.

ARES workflow (e-signatory):

In Ares, it is possible to introduce a workflow procedure:

- 1st stage: saving a working document with attachment of the document in its native form and identification of addressees able to comment on/modify the document (e-signatory).
- 2nd stage: registration of the finalised and approved document with traceability of successive versions of the document.

Registration metadata in Ares

MINIMAL METADATA	COMMENTS
Document tab	
Mail type	<ul style="list-style-type: none"> ▪ Internal mail: correspondence sent or received within the Commission or between the Commission and an executive agency or the European External Action Service (EEAS) ▪ Incoming mail: correspondence from an external sender received by the Commission, an executive agency or the EEAS ▪ Outgoing mail: correspondence sent to an addressee external to the Commission, the executive agencies and the EEAS.
Document date	Date appearing in the text of the correspondence
Received Date (<i>sic</i>)	Date on which the document is received
Sent Date (<i>sic</i>)	Date on which the document is sent to its addressee
Encoding date	Date on which the document is encoded (generated by the system)
Title/Subject	Succinct description of the document's content giving an overall understanding of what it concerns without having to read it in detail.
Sent by	Author(s) or organisation(s) formally responsible for the content of the document. To be selected from the " <i>int</i> " or " <i>ext</i> " list depending on whether the sender is internal or external to the Commission
Recipient(s) / Distribution list	A distribution list (a predetermined group of people) can be used to complete the addressees line in an item of correspondence. This saves time by entering an entire group of recurrent addressees in a single action.
Security and Markings	<p>Level of sensitivity: Used in Ares to encode and process documents for which a security level is required. 3 possible levels:</p> <ul style="list-style-type: none"> - Normal (default option) - Handling restriction (security marking) - RESTREINT UE <p>Attachment of the document is mandatory for the first two levels (except for "OLAF" and "COMP" markings) and forbidden for "RESTREINT UE" documents.</p>

3.3. REGISTERS AND APPLICATIONS WITH EQUIVALENT EFFECT

The operation of registration is carried out in **registers**: databases containing the metadata of documents registered by the departments.

➤ 3.3.1. Registers

A register is an administrative instrument recording the receipt and sending of documents that are complete and correctly constituted in legal or administrative terms, and their proper transmission.

The register must contain the references of every formal document received and/or transmitted.

On distingue:

A distinction is made between:

- The **general register**: used for the registration of incoming, outgoing and internal correspondence and notes to the files (**Ares** at the Commission headquarters and **Delores** in the Delegations)
- **Specific registers**: used to register documents subject to specific procedures without having to re-encode them in the general register (guarantees equivalent to the general register: inclusion of minimal metadata, audit trail for modifications, security in the event of system failure).

/// Examples

- /// - **ABAC Contracts**: Management of contracts involving a financial commitment (invoice follow-up)
- /// - **Basil**: Management of parliamentary questions in Commission Departments and Cabinets and search engine on parliamentary questions
- /// - **CHAP**: Registration and management by the SG of correspondence involving complaints
- /// - **e-Greffe**: transmission and management of the Commission's decision-making procedures
- /// - **EU Pilot**: exchange of information with member States as part of checks on the application of Community law
- /// - **Gestdem**: workflow management for requests for access to European Commission documents (initial and confirmatory requests and resulting complaints to the Ombudsman)
- /// - **Tsar II** (Tracking Smart Assistance Request): management of briefings for Commissioners and Directors-General.

➔ Only the e-Domec (SG) team is authorised to determine whether an application may be recognised as a specific register⁶.

⁶ The complete list of e-Domec specific registers and applications can be consulted at:
http://myintracomm.ec.europa.eu/corp/sg/en/edomec/doc_management/Documents/compliance_en.pdf

➤ 3.3.2. Applications with effect equivalent to the register

This corresponds to applications that do not have all the characteristics of a register but that are sufficiently reliable to be used as such for the purposes of identification and filing.

Exemples

- **CIS-Net:** system for monitoring the official stages of transmission and processing of interdepartmental consultations (launch, contributions, replies, closing).
- **Vista:** An information system for internal use – managed by the Secretariat General – giving access to non-classified and non-marked Commission documents from 01/01/2010 on and to follow-up of progress on internal procedures.
SG VISTA can be used to consult Commission documents created prior to 01/01/2010, Council and European Parliament documents and inter-institutional procedures.
- **MIPS:** Logistics management for missions
- **Poetry:** Management of translation requests
- **Syslog:** Management of professional training programmes (creation of courses, enrolment, assessments, etc.), with filing in individual files (the file code is the employee number).
- **Sysper2:** information system for managing the Commission's human resources. Management of all aspects of career development, with filing in individual files (the file code is the employee number).
- **Webdor-Presto:** Webdor is an application for managing conference room bookings. It displays the list of bookings and details of each individual booking. Presto offers the same features for drinks orders.

Remark:

As part of the IT rationalisation process, a number of applications featuring a "Document Management" module are being integrated into the HAN (Hermes-Ares-NomCom) platform.

⇒ **A document must be registered once only, in the appropriate register.**

Interactions between Ares and the specific registers:

- **Interdepartmental consultations (CIS-Net):** The document launching an interdepartmental consultation is registered in Ares prior to the official launch in CIS-Net. The follow-up of interdepartmental consultations (replies from the DG consulted) must be carried out exclusively in CIS-Net (no supplementary registration of replies in Ares).
An official file must be created by the DG launching the CIS, noting under the "Comments" heading that the documents are managed in CIS-Net.
A DG consulted may use Ares to coordinate preparation of its reply and obtain line management approval, but this is not a substitute for the use of CIS-Net: the reply, approved at DG level, must be registered in CIS-Net.
- **Parliamentary questions (Basil):** Basil is the system used for dealing with a parliamentary question (assignment of a parliamentary question in order to register the reply in the same system).

In addition, a DG may use Ares to coordinate preparation of its reply and obtain line management approval, but this is not a substitute for the use of Basil: the reply, approved at DG level, must be registered in Basil.

➤ 3.2.3. Saving a document

A document that does not meet the conditions for official registration may be simply **saved**.

The aim is to notify the existence of a document in order to retrieve it easily: this simple notification is not a registration. It does, however, allow for documents to be filed in the files as supplementary information.

: Examples:

- : - **Ares: "Save"** function
- : - **CIRCABC:** An application used to create restricted access websites for communication between individuals inside and outside the Commission (collaborative workspace). CIRCABC includes calendar, chat, document publication and access management features. CIRCABC is not a register.

⇒ Using the "Save" function in Ares depends on procedures established in the DG or the Department:

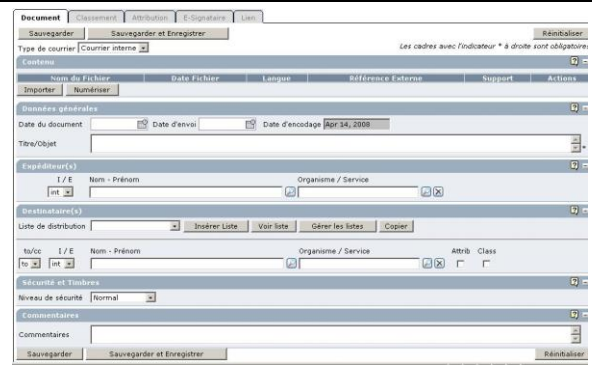
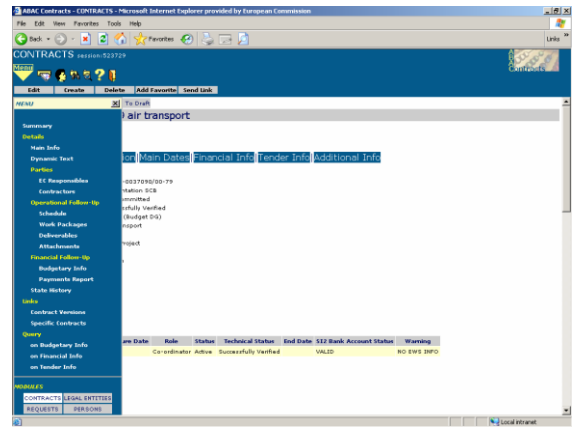
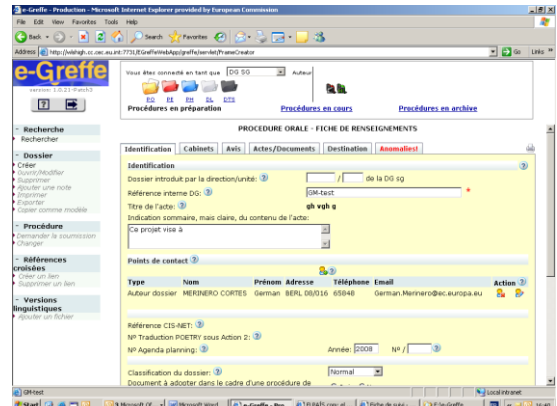
- transmission of a document for comment/modification and signature (workflow function with e-signatory),
- identification of information or working documents,
- notification of documents registered in specific registers, etc.

⇒ A document can be registered after it has been saved.

⇒ In ARES, a document that has been saved but not filed is automatically destroyed six months after the date of its creation (or the date of the last action on the file).

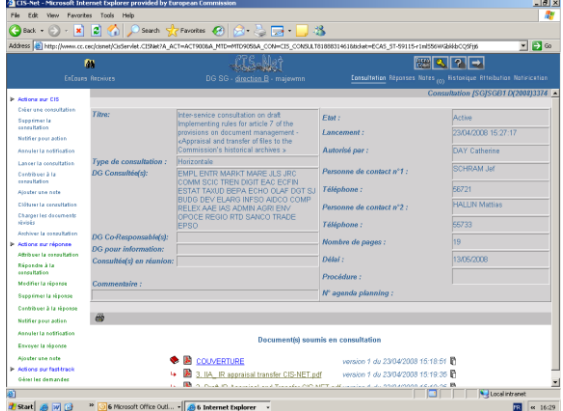
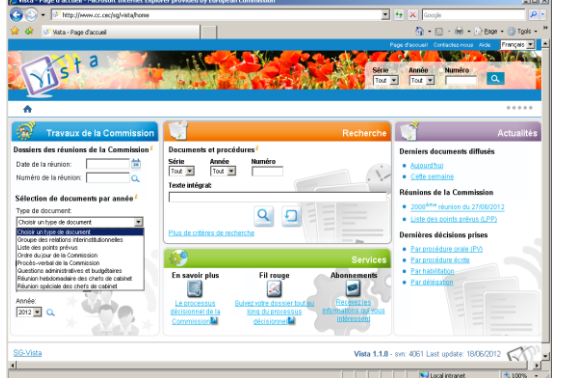
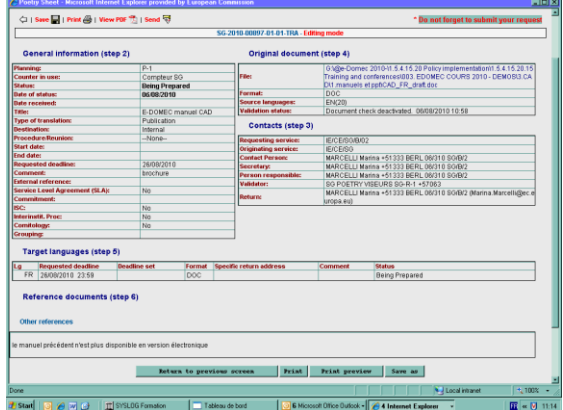
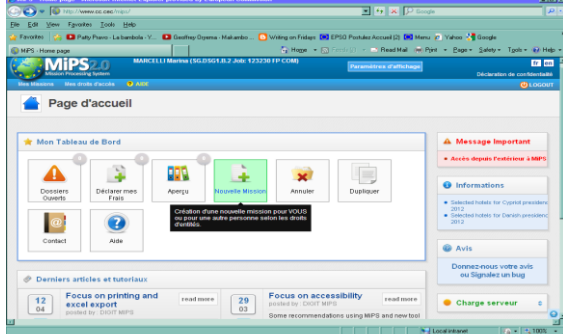
If the saved document is filed, it is not subject to the six-month limitation. Only when the file is closed will the system ask what is to be done with the saved documents: elimination or post facto "freezing" for the documents to be included in the closed file.

Registration: choose the right application ⁷

GENERAL REGISTER: used for the registration of incoming, outgoing and internal correspondence and notes to the file.		
Ares	General application for the management of files and documents	
SPECIFIC REGISTERS: any other register, constituted by a similar procedure, distinct from the general register, but offering equivalent guarantees (inclusion of minimal metadata, audit trail for modifications, security in the event of system failure).		
ABAC	Management of contracts involving a financial commitment	
e-Grefte	Management of written or oral electronic procedures	

⁷ The complete list of e-Domec compliant applications can be consulted at:
http://myintracomm.ec.europa.eu/corp/sg/en/edmec/doc_management/Documents/compliance_en.pdf

APPLICATION WITH EFFECT EQUIVALENT TO THE REGISTER: applications that do not have all the characteristics of a register but are sufficiently reliable to be used as such for the purposes of identification and filing.

<p>CIS-Net</p>	<p>Management of interdepartmental consultations, used for monitoring the official stages (launch, contributions, replies, closing).</p>	
<p>Vista</p>	<p>Information system for internal use, managed by the Secretariat-General, giving access to non-classified and non-marked Commission documents, used to follow the progress of internal procedures.</p>	
<p>Poetry</p>	<p>Management of translation requests</p>	
<p>Mips</p>	<p>Logistics follow-up for missions with filing in individual files (the file code is the employee number).</p>	

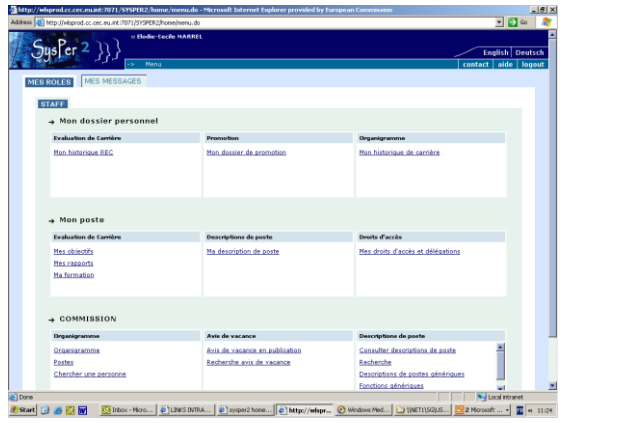
Syslog

Management of professional training programmes (creation of courses, enrolment, assessments, etc.), with filing in individual files (the file code is the employee number).



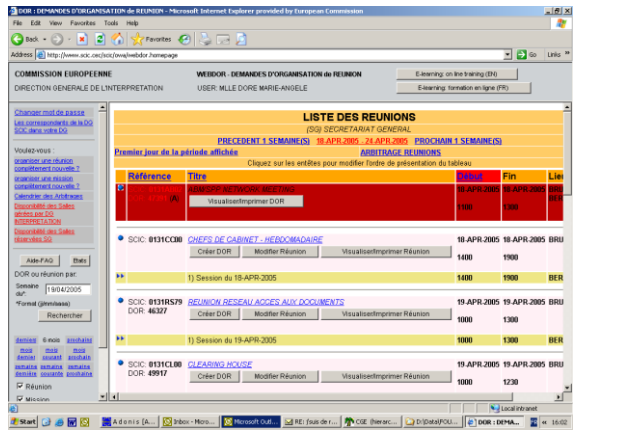
Sysper2

Information system for managing the Commission's human resources. Management of all aspects of career development, with filing in individual files (the file code is the employee number).



Webdor-Presto

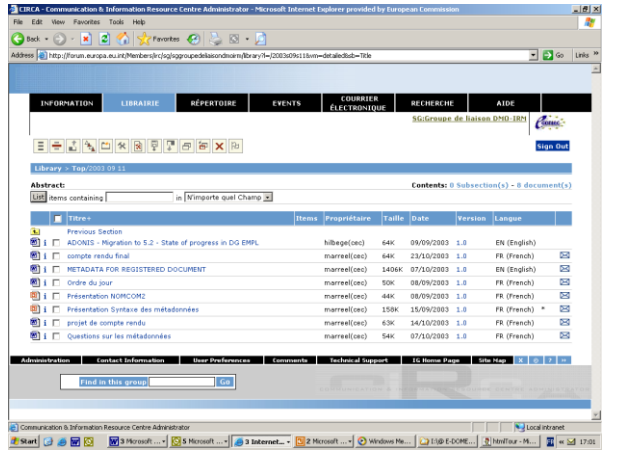
Webdor is an application for managing conference room bookings. It displays the list of bookings and details of each individual booking. Presto offers the same features for drinks orders.



Outil d'échange

CIRCABC

Application used to create restricted access websites for communication between individuals inside and outside the Commission (collaborative workspace). CIRCABC includes calendar, chat, document publication and access management features. CIRCABC cannot be used to register documents.



Summary table of register and repository for information applications

Application	General register (1)	Specific register (2)	Process with equivalent effect ⁽³⁾	Save function (4)	Filing	Attachment of electronic document
ARES	X			X	X	X
Sybil		X			X	X
ABAC		X			X	X
Basil		X			X	X
CHAP		X			X	X
Delores	X				X	X
e-Grefe		X				X
Gestdem		X				X
Cis-Net			X			X
Vista			X			X
Mips			X	X	X	X
Poetry			X			X
Syslog			X		X	X
Sysper2			X		X	X
Webdor-presto			X			X

- (1) **General register:** used for the registration of incoming, outgoing and internal correspondence and notes to the file.
- (2) **Specific register:** used to register documents subject to specific procedures without having to re-encode them in the general register (guarantees equivalent to the general register: inclusion of minimal metadata, audit trail for modifications, security in the event of system failure).
- (3) **Application with equivalent effect:** applications that do not have all the characteristics of a register but that are sufficiently reliable to be used as such for the purposes of identification and filing.
- (4) **Save:** notification of the existence of a document (repository for information).

IV. FILING: FILES AND FILING PLAN

1. Why file?

Principle of filing:

- ✓ Documents are drawn up or received as part of a **case**.
- ✓ To simplify the management and retrieval of all documents relating to a particular case, they must be associated within a single **file** to which a unique identification code is assigned.
- ✓ In order to simplify the retrieval of electronic files, they are allocated to an appropriate heading of the **filing plan**.
- ⇒ For each case dealt with by a Lead Department, there must be a complete and reliable official file.
- ⇒ Every document registered must be filed in an official file.
- ⇒ **The real working instrument is the file.**

Files that are properly managed, complete and reliable can be used to:

- retrieve useful information rapidly
- rationalise tasks
- support collaborative work
- ensure accountability
- facilitate mobility

2. Official file and working file

2.1. DEFINITION OF A FILE

Definition of a file:

Core around which the documents are organised in line with the institution's activities, for reasons of evidence, justification or information and to guarantee efficient working. The group of documents making up the file is organised in such a way as to form a coherent and relevant unit in terms of the activities conducted by the Commission and/or its departments.

Source: SEC(2009)1643: Implementing rules on document management and on electronic and digitised documents.

- ⇒ A case is a set of administrative actions carried out as part of a determined procedure (with a **beginning** and an **end**).
- ⇒ The file serves as justification, proof or information on a case. Its proper management is a guarantee of efficient and relevant work.
- ⇒ The file is thus a set of documents relating to a particular case and organised consistently. The aim is to be able to find all the documents relating to a case as quickly and easily as possible.

2.2. TYPES OF FILES

➤ 2.2.1. Official file and working file

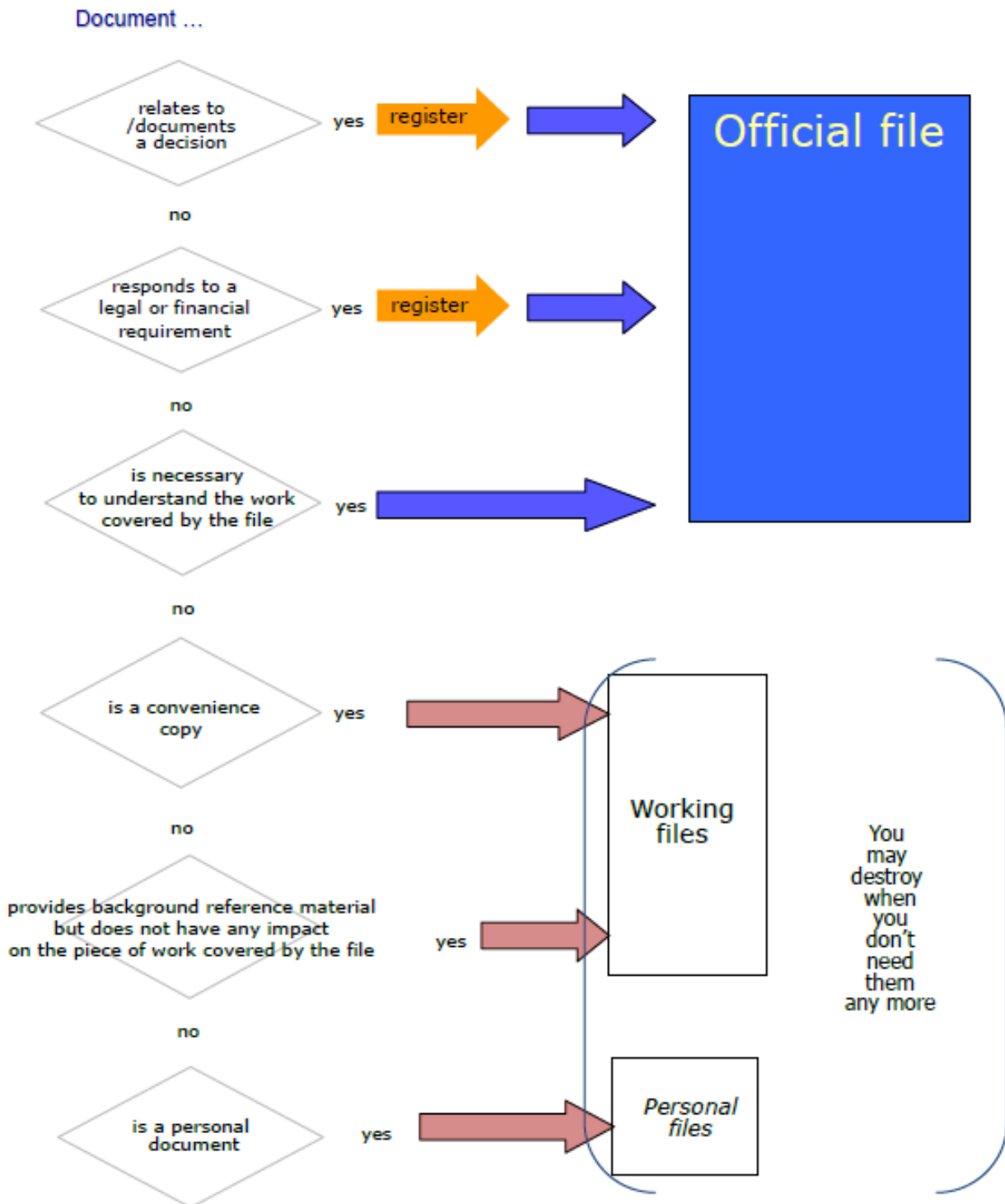
There are two types of files managed during the everyday follow-up of cases:

- **Official file:** a single file managed by the Lead Department responsible for the file and containing all the supporting documents relating to a case.
 - ⇒ Each official file must be complete: it must contain at least all the officially registered documents relating to a case, and any other document useful in handling the case.
 - ⇒ It constitutes evidence and must be retained.
 - ⇒ It must be subject to inspection and audit.
 - ⇒ It will be checked prior to closure and then, at the end of the administrative retention period, will be transferred, if appropriate, to the Historical Archives for retention and public consultation.
- **Working file (or information file):** file created for working purposes, with content determined by the officials responsible for compiling it. It is used to retain documents that have not been registered but that have some short-term usage. They may include: copies of documents, non-finalised versions of documents, documents not subject to registration requirements (collections of notes, technical reference material, copies of articles, telephone call logs, non-certifying e-mails, drafts, etc.)
 - ⇒ working files have no legal value.
 - ⇒ they might be destroyed at any time without the loss of essential information.
 - ⇒ they will be eliminated on closure of the file and excluded from the intermediate records.

Only official files are subject to e-Domec obligations and internal control standard n°11.

- ⇒ **Official files that are complete and reliable give a guarantee of:**
 - increased efficiency within the unit by making it possible to retrieve all documents relating to a particular case quickly and easily by putting them into context.
 - proper management of cases for the purposes of accountability.
 - business continuity in the event of staff mobility: consulting the file makes it clear what has been done and what is still to be done.
- ⇒ **Every document registered must be filed in an official file.**

Official file and working file



➤ 2.2.2. Value of official files

The official file provides justification, proof or information on a case. If correctly managed, it guarantees the effectiveness and relevance of work done.

⇒ For each case, at least one official file must be created by the Lead Department (or several official files if several departments share responsibility for different aspects of a single case).

⇒ The official file is characterised by the value of its functional, operational, legal information etc. and not by the type of document it contains or how it is organised.

Example:

⚡ An "Order Forms" file or a Chrono file (in which documents are simply organised in chronological order) cannot be an official file.

⇒ The official file follows the pace of development of the case: it is created when the case commences and closed when the case comes to an end.

Special exception: "Personnel management and human resources" files

The DG HR has sole authority to manage and retain the official files of Commission employees. Additionally, the DG Human Resources Department manages the official files relating to the DG's specific personnel management policy:

⇒ In the DGs, a personnel management file cannot have the name of a particular employee (no file named "John SMITH" can be held, for example).

⇒ Any "Personnel Management" files that may be held by units for the everyday management of human resources must therefore be considered as working files:

- These files must nonetheless be kept securely.
- They can not be transferred to the Historical Archives.
- When the file is due for elimination, the DMO must be consulted on the procedure for centralisation of files by the HR Department and on the procedures for destruction (including files containing unsolicited applications).

2.3. LEAD DEPARTMENT RESPONSIBILITY

For each file, there is a "**Lead Department**" ("Chef de file") in which a member of staff designated as "**file manager**" is responsible for the day-to-day management of the file.

The Lead Department is responsible for the case, even if other units may be involved in ancillary tasks or providing assistance.

The responsibility for creation and retention of the file relating to a case lies with the Lead Department.

⇒ The Lead Department is responsible for:

- **Creating** a new file when a case is opened.
- **Managing** the file: the Lead Department on the case is responsible for filing each registered document in the corresponding official file.
- **Closing** the file on conclusion of the case.

- **Retaining** the file during the Administrative Retention Period (ARP) or storing it in the DG Central Archives (depending on the internal organisation as regards the retention of intermediate records).
- Collaborating with the DMO on the first **review of files** and their **possible transfer to the Historical Archives**.

⇒ Each official file must be complete at all times and must be available for inspection and audit.

3. Creation of an official file

A new file must be created when a new case starts or when a registered document has no link to a current case and therefore cannot be filed in an existing file.

3.1. CREATION OF AN OFFICIAL FILE

A new file must be created whenever a new case is opened i.e. when a registered document is not linked to a current case and therefore cannot be filed in a current file. We advise against creating a new file before having at least one document to file (too many created files remain empty), except in the case of serial files.

A new official file must be created in **Ares**. The creation of a file involves filling out descriptive information (metadata) about the file

- 1) Filing plan heading for attachment to the filing plan
- 2) File code: generated automatically by NomCom (year of the file's creation + 2 letters + 4 digits)
- 3) Specific file code: freely chosen internal management code. This code may be chosen by the DG or department based on its own file identification system.
- 4) Lead department: administrative entity (= department) responsible for the file
- 5) File manager: person in the department responsible for following up the file
- 6) Category: choice of retention list category (CRL/SRL) from the categories associated with the filing plan heading
- 7) Title: must be clear and meaningful and in either French or English
- 8) Limited: to be used if the file is not available for consultation by the entire organisation to which the user belongs (i.e. the DG; the executive agency, cabinet or EEAS).
- 9) Security: determination of access rights = roles in relation to the file (Editor(s), User(s), Reader(s)).
- 10) Date created: date the file/subfile was created
- 11) Date activated: date on which the file status changed to "active"
- 12) Closing date (once the case is closed): date on which the file/sub-file status changes to "closed"
- 13) Status: 4 possible options:
 - active (new documents can be added to the file)
 - closed (no new documents can be added to the file)
 - transferred (to Historical Archives)
 - destroyed (by the DG or Historical Archives)
- 14) Comments: comments on the file's contents.

N.B.: Minimum information required to create a file: file plan heading, file title, Lead Department

⇒ To facilitate the creation and the management of files, it is recommended, whenever possible, to create « master files » indicating the checklist of the mandatory documents in the file (e.g. for call for tender procedures, research projects , budgets, ...)

3.2. PROPER FILE IDENTIFICATION: ACTION FILE AND SERIAL FILE

Files may be of two types:

1 - Action files arise from one-off or unique cases, the duration of which is not known in advance but for which the procedural action that will make it possible to close the case is clearly determined.

⚡ Examples of such actions:

- ⚡ Monitoring a research project
- ⚡ Call for tender procedure

⇒ Creation of an **action file** (or case): concerns a specific case, beginning and ending at a precise and clearly identifiable moment.

⚡ Examples of scopes:

- ⚡ Monitoring a research project: completed when the final report is presented and the final payment is made
- ⚡ Call for tender procedure: completed once the successful bidder has been chosen

⇒ **Action file title:** Compose a title that is explicit, as regards both the subject of the file and the action required on that subject.

⚡ Examples of action file titles:

- ⚡ Development of the manual on filing documents and files at the Commission"
- ⚡ Adoption of legislation on the validity of electronic documents"

2 - Serial files arise from work of a repetitive nature, the duration of which is generally linked to a calendar or budget year and which always proceeds in the same way.

⚡ Examples of recurrent works:

- ⚡ AMP (Annual Management Plan): a new AMP must be drawn up every year
- ⚡ Determination of a training programme: linked to a budget year

⇒ Creation of a **serial file**: repetitive in nature and must be open to specific identification to simplify the operations of closure and duplication of the structure for the next serial file.

⇒ **Serial file title:** facilitate the distinction between action file and serial file by indicating the date (period covered) in the title of serial files.

⚡ Examples:

- ⚡ IT budget **2012** ⇒ Serial file
- ⚡ Annual Management Plan **2012** ⇒ Serial file

⇒ Check with the DMO if the DG has any specific rules applicable to file titles. If not, create a naming charter for the unit's standard files.

3.3. ATTACHMENT OF FILES TO THE FILING PLAN

The **filing plan** provides for the intellectual organisation of the official files of the Commission, the executive agencies and the EEAS on the basis of their activities, so that the files can be easily retrieved. It is a hierarchical and logical structure in the form of a tree structure by theme:

- composed of a fixed number of headings relating to the activities and missions of the Commission, the EAs and the EEAS
- consisting of a hierarchy of several levels, from the most general to the most specific,
- identified by a title and a numeric code,

The filing plan consists of:

- the **common nomenclature: the first levels** are defined by the Secretariat-General.
- the **specific levels**: each Commission DG and department, EA and the EEAS must have a filing plan that represents their activities and is linked to the common nomenclature.

First level of the Common Nomenclature:

01. Institution – Commission
02. Future of the Union and institutional questions
03. The Community economic and social area
04. Citizenship and quality of life
05. International relations
06. Financing of community activities and the management of financial resources
07. Community law
08. Press, communication and publications
09. Policy strategy and coordination per DG
10. Administration
12. External Action – Common foreign and security policy
15. Activities of the delegations and offices of the European Union in third countries and to international organisations

The purpose of the filing plan is:

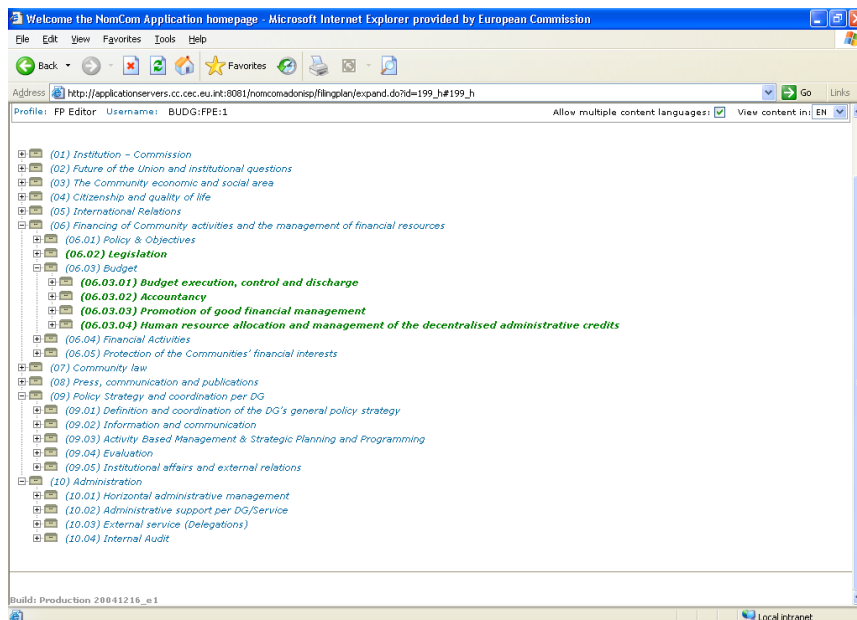
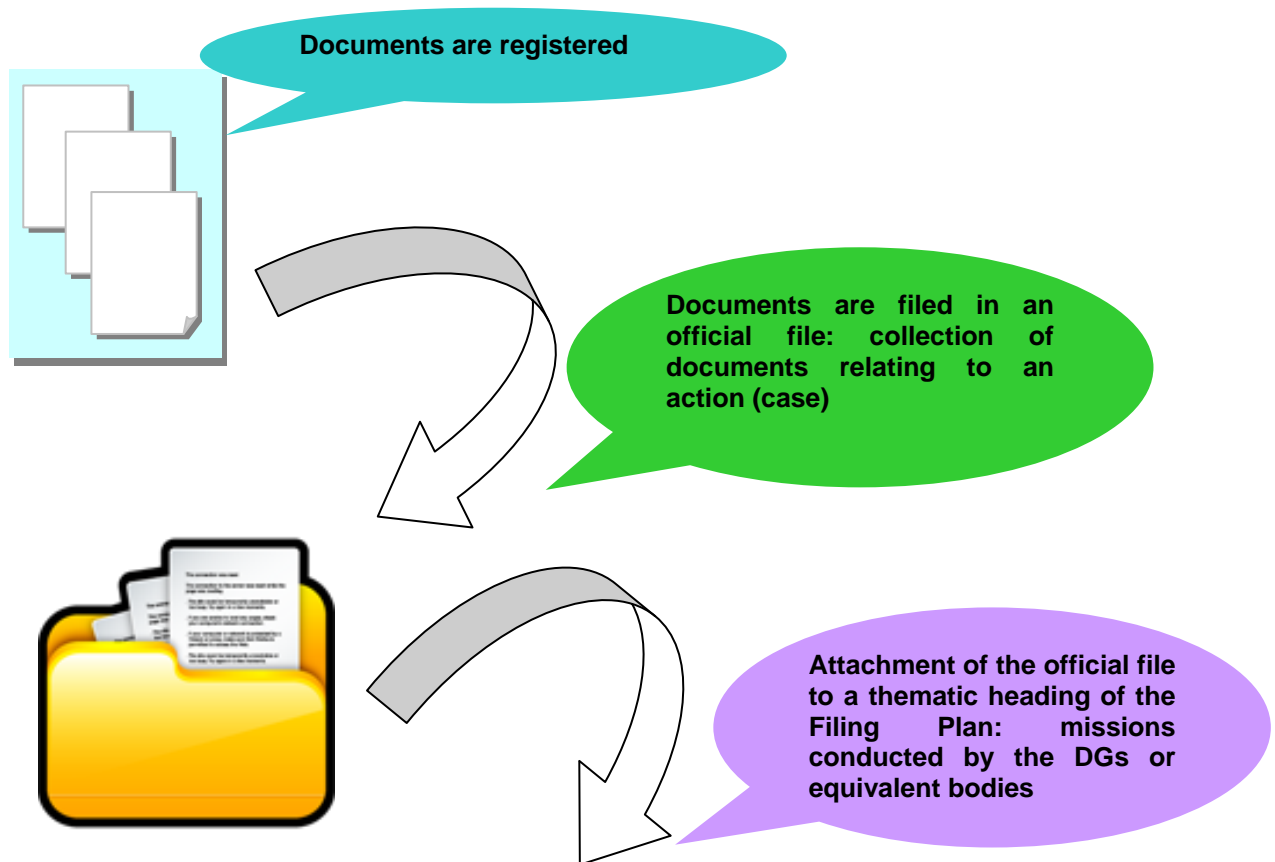
- to give a global overview of all the activities of each department;
- to ensure consistency of filing systems: uniform identification of files handled by teams;
- to structure the constitution of files and facilitate the filing of documents in files in a logical manner;
- to facilitate searches for files and documents;
- to improve the quality and continuity of file follow-up, especially in the event of a change of Lead Department or assignment of the case.

All official records must be attached to the filing plan.

- ⇒ They are filed under the appropriate heading of the filing plan: last level heading of the filing plan specific to a DG

⇒ **This operation is done one single time, when creating the record.**

Headings, files and documents



⇒ **A document is never filed directly in a heading of the filing plan but always in a file and the file is attached to a final-level heading in the filing plan.**

3.3. THE OFFICIAL FILE MANAGEMENT TOOL: THE FILE LIST

The file list is managed via Ares. It contains the descriptions of each official file and is an everyday working tool that can be used to:

- draw up an inventory of the official files managed by the Commission;
- identify the Lead Department (chef de file) for each case;
- file documents in their corresponding file;
- enable searches for and access to files and documents;
- determine the retention period for each file;
- facilitate transfer to the Historical Archives.

4. Filing documents

Every registered document must be filed in an official file.

A document that has not been registered may also be filed in an official file. This may apply in particular to documents that have simply been saved (Ares), but which are useful to an understanding of the case: simple working documents, documents registered in specific registers and flagged to make them easier to find, etc.

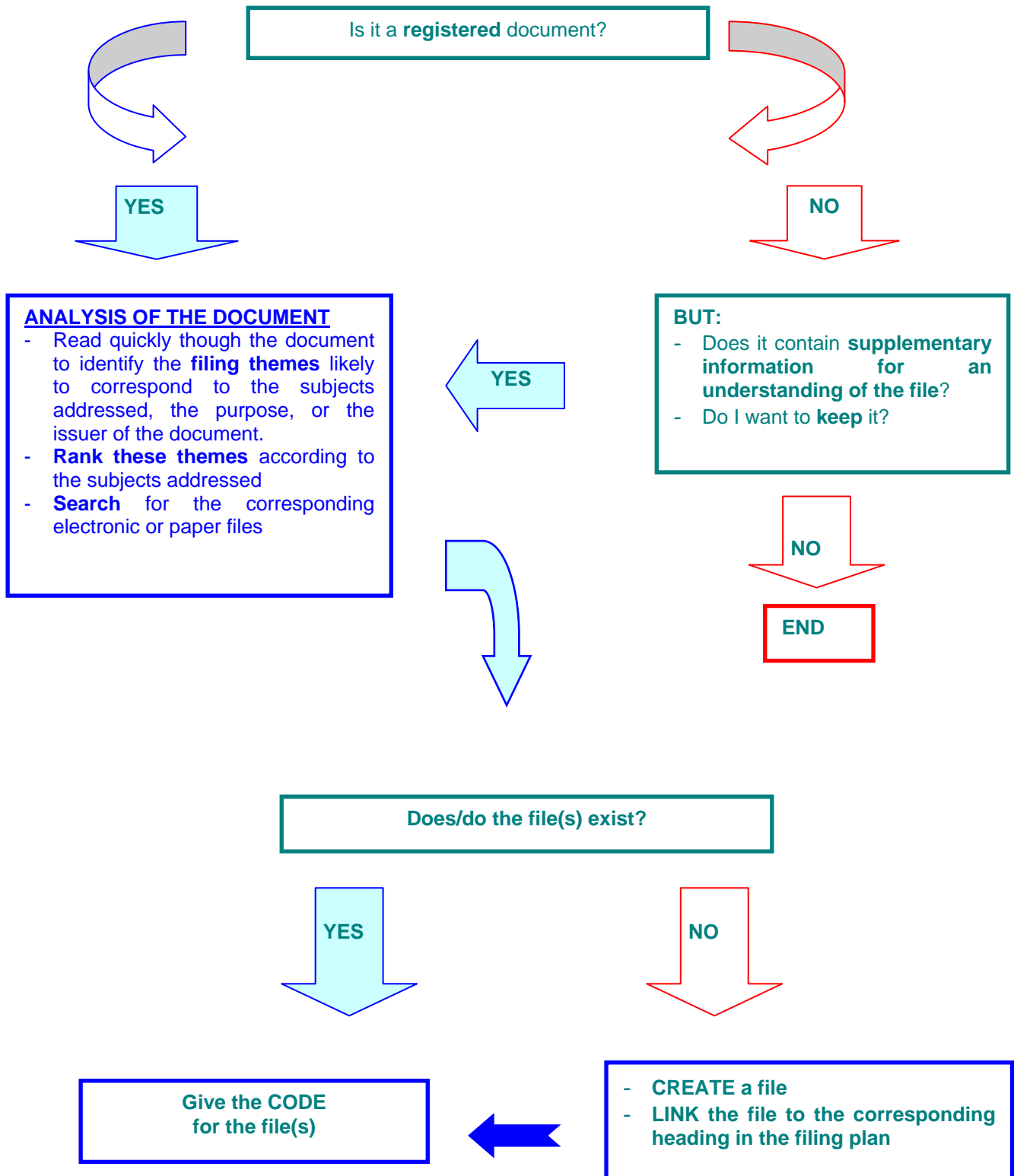
4.1. CHOOSING THE CORRECT FILE FOR FILING

Before filing a document in a file, an analysis must be carried out to determine which is the appropriate file.

The analysis may be conducted as follows:

STAGES		DESCRIPTION
1	Define the filing themes of the document	Read quickly through the document to identify the filing plan themes likely to correspond to the subjects addressed, the purpose, or the issuer of the document.
2	Rank these themes according to the subjects addressed	Depending on the subjects addressed, select the main theme that characterises the document.
3	Search for the corresponding electronic or paper file(s)	A document may be filed in several files when the information in the document relates to several cases.
4	File the document	Indicate the code of the electronic file(s) in the encoding sheet
5	Store the document (original documents, classified documents, documents that cannot be digitised, etc.)	Note the file code on the paper document and store the document in the corresponding paper file.

Analysis of a document to be filed



- ⇒ **The choice of file for filing is fundamental:** filing a document in a file automatically assigns to it all the rules and procedures associated with that file:
- Retention period,
 - Authorisations for consultation,
 - Rules of elimination, etc.

4.2. FILE CONSISTING OF DOCUMENTS REGISTERED IN DIFFERENT APPLICATIONS

If a file consists of documents registered and kept in different registers (Ares, Cisnet, Sybil, Abac ...), it is important to both facilitate access to information and respect the rule of the single registration of any official document.

- ⇒ At present, documents can only be filed in official electronic files in Ares. An indication must therefore be given in the file description in NomCom that the file contains documents registered in other applications ("Preservation" tab: Media + list the applications concerned)
- ⇒ Additional suggestion: create a working document that you save and file in the file, listing all the documents and the applications in which they are registered.

4.3. ROLE OF FILE MANAGER

Filing, like registration, comes under the administrative responsibility of the Lead Department.

The file manager plays an essential role:

- ensuring that every registered document relating to the case for which he is responsible is filed in the correct file
 - indicating to the person in charge of the filing operation in which file the document should be filed
- ⇒ A procedure must be established in the unit to define who files, and how; in practice, the file manager must pass the information on the file to be filed to the person responsible for filing in Ares.
- ⇒ To facilitate filing, it is possible to create in Ares a list of **favourite files**: add / delete your favourite files depending on the on-going business.

V. MANAGEMENT OF CURRENT RECORDS

It is important that files be properly retained and preserved, whatever the medium (electronic and/or physical), throughout their life cycle. Each Directorate-General or equivalent department therefore assumes responsibility for the retention of files relating to its sphere of responsibility.

1. Electronic and/or paper retention ?

Documents that have been registered and filed must be available in electronic format: in born-digital or digitised format.

⇒ In Ares, it is impossible to register a document without having attached the electronic version (except for "RESTREINT UE" documents or those with an "OLAF" or "COMP" marking).

It is essential to be familiar with the principles of validity of electronic documents in order to determine whether retention in electronic format is sufficient, or if the original also needs to be retained in paper form.

1.1. VALIDITY OF ELECTRONIC DOCUMENTS

The implementing rules relating to electronic and digitised documents (SEC(2009)1643, chapter III) specify an initial, non-exhaustive list of types of documents that may be retained exclusively in electronic form and do not require a signed original.

⇒ This list will evolve as the use of electronic signatures develops.

➤ 1.1.1. Principles of validity

An electronic records management system must offer the same guarantees, in terms of security and access, as those provided for the document management of physical (particularly paper-based) documents.

In evaluating the validity of electronic documents at the Commission, the following must be taken into account:

- **Circles of parties to electronic exchanges of documents:**
 - **Circle 1:** internal circle made up exclusively of the Commission and its Directorates-General and equivalent departments, which exchange electronically among themselves drawn up or received documents. The electronic identification of parties is performed by the ECAS system (or any other equivalent certified system).
 - **Circle 2:** circle made up of the Commission and partner administrations (other institutions, member States, national public administrations, entities with which the Commission has regular dealings), which electronically exchange documents subject to mutual legal and IT standards.
 - **Circle 3:** open circle made up of the Commission and organisations, non-member States, commercial businesses, legal entities and citizens, which exchange documents via Internet or Extranet networks. An external person may be identified by the use of a simple electronic signature or by an authentication function of the IT application used, or continued exchanges.

- **Origin of electronic documents:**
 - **“Born-digital” electronic documents:** drawn up or received in electronic format. Only “born-digital” electronic documents may be signed with an electronic signature.
 - **Digitised documents:** all documents drawn up or received in paper form and registered must be digitised (subject to format or security constraints).

➤ 1.1.2. Born-digital” electronic documents “⁸

◆ Documents requiring a signed original

Only a small proportion of Commission documents require a signature as a substantial formality in order to be valid.

⇒ Types of electronic documents for which signature is a substantial formality:

- Documents drawn up by the Commission: minutes and acts to be authenticated pursuant to articles 11 and 17 of the Commission’s Rules of procedure,
- Documents received by the Commission: tenders under public procurement procedures, grant agreements or decisions, declarations of expenditure, annual accounts, etc.

◆ Documents not requiring a signed original

These include the majority of administrative documents drawn up by the Commission. It must, however, be possible to duly identify the person from whom the document emanates and guarantee the integrity of the document’s content and metadata. The requirements depend on the circle concerned and the level of formalism required by the field of activity or the procedure under way.

⇒ Examples of documents drawn up by the Commission not requiring a signed original:

- Internal administrative procedures: relations between the administration and its officials, etc.
- Documents relating to the internal or inter-institutional legislative process: preparatory documents, notes, studies and reports to evaluate the content or consequences of legislation.
- Information on calls for tender or calls for proposals
- Documents relating to the internal operation of a Directorate-General or a department: minutes of meetings, etc.
- Documents of an administrative, financial or budget discipline nature, for external communication.

⇒ Examples of documents received by the Commission not requiring a signed original:

- Exchanges of information with member States and other institutions and bodies under Community policies.

⁸ Paperless Commission in the financial domain – handwritten signature or not (FR only):
http://myintracomm.ec.europa.eu/corp/sg/en/edomec/doc_management/Documents/paperless_signat_nov2011.pdf

- Requests by citizens for access to documents;
- Complaints about breaches of Community law;
- Submission of applications.
- Supporting documents for the submission of grant applications.
- Statistical and financial data.

➤ 1.1.3. Digitised documents

Registered documents in a non-electronic medium must be digitised in a format which offers guarantees of permanence, legibility over time and ease of access such as PDF or PDF/A (PDF for archives) or TIFF.

The department carrying out the digitisation must put in place quality control to check that the scanned document corresponds to the original. As a precaution, the original version of all digitised documents must be kept for a period of at least six months so that the necessary checks and corrections can be carried out.

⇒ Retention of the original paper document

The digitisation tools currently in use at the Commission do not make it possible to certify that a scanned document corresponds to its original. In the case of documents for which signature is a substantial formality, the original must be retained in an official paper file.

- Examples:
- Contracts
 - Invoices
 - Expense claims

1.2. MANAGEMENT OF A HYBRID FILE (ELECTRONIC AND PAPER)

A hybrid file is a file made up of electronic documents that have been registered and are available via the official electronic file and paper documents paper stored in a supplementary official paper file.

In a certain number of cases, retention of registered documents in their physical medium of origin remains mandatory:

- documents for which only the paper original has evidential value: documents required for control or audit purposes.
 - documents partially digitised or not digitised and not attached to the Ares sheet:
 - classified documents
 - documents on media or in formats that cannot be digitised,
 - voluminous documents of which only the first page has been scanned
- documents that have not had the quality of their digitisation checked.

These documents must be stored in an official paper file supplementary to the official electronic file.

Two possible instances:

- Either the official file is made up of both electronic documents and original documents that must be in paper form: documents stored in a paper file noted in the electronic file description sheet with reference to the location of the paper file.
- Or the official file is exclusively in paper form: creation of a description sheet in the list of official files with reference to the location of the paper file.

- ⇒ To guarantee that the electronic file and paper file correspond:
- note the existence of the paper file under the “Comment” heading of the file description sheet.
 - on the paper file label, note at the very least the same title and code as the electronic file, the date of creation and the Lead Department.
 - identify the official nature of the file by a clear reference or a colour code (e.g. a coloured sticker).

Practical tip:

To guarantee that the official paper file will be identified in the same way as the official electronic file, the simplest solution is for this file to be created by the DMO correspondent at the same time as the electronic file and handed directly to the file manager if (s)he retains the paper file in her/his office.

2. Retention sites for official paper files

2.1. FILING AND STORING

A distinction is made between:

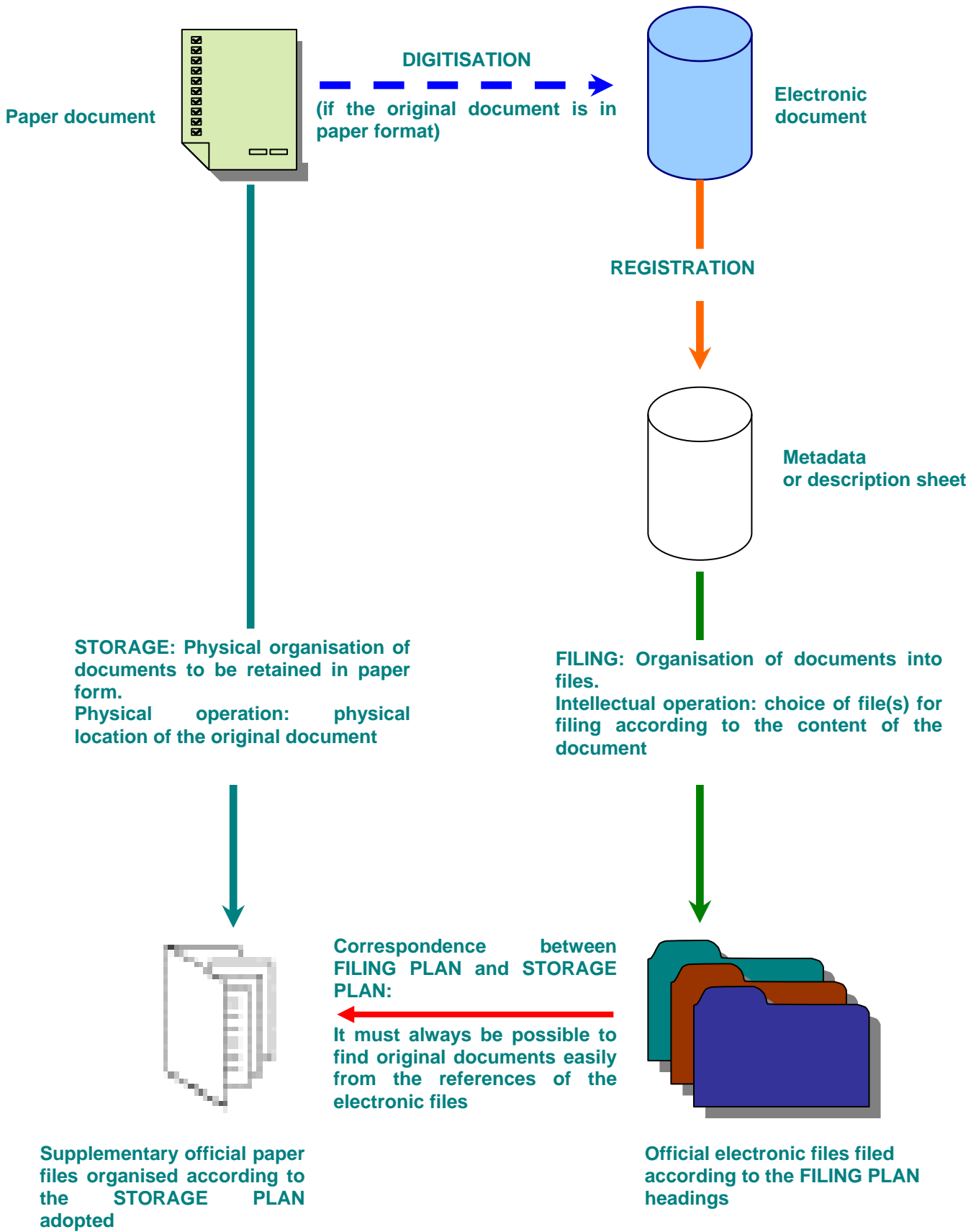
- **Filing:** an **intellectual** operation of assigning a filing code to documents = association of a document with one or more files.
- **Storing:** a **physical** operation of storing documents in a file, whether in paper form (storage in files and cabinets) or in IT form (storage on shared discs, in databases, on a web server, etc.).

Each DG or department is responsible for ensuring the physical protection of the files within its sphere of responsibility until their transfer to the Historical Archives Service.

Official paper files may be retained in different locations during their life cycle.

LIFE CYCLE	FREQUENCY OF CONSULTATION	STORAGE LOCATION
Current records Files corresponding to current cases	Consulted very frequently (e.g. daily, weekly).	Department files: official files are held centrally in the department or in the file manager’s office
Intermediate records Closed files retained for legal or administrative inspections	Consulted less frequently (e.g. monthly)	DG central archives repository or specific locations in Lead Departments.
Definitive archives Closed files retained to constitute the institution’s collective memory	Consulted occasionally	Historical Archives: archives are retained in repositories managed by the Historical Archives Service.

Filing and storage of documents



2.2. UNIT STORAGE PLAN

The storage plan is a practical instrument that defines:

- the allocation of responsibilities for the physical preservation of files
- the exact location of all official files in the DG: the level of location detail in the storage plan is defined by the Lead Department and/or the DMO
- the form of storage adopted according to the type of file (alphabetic, numerical, chronological, by subject, etc.).

N.B.: The storage plan, like the filing plan, applies to all documents in paper and/or electronic form. It is the responsibility of units, as regards current and intermediate records, except for those DGs with a Central Archives service responsible for the intermediate records.

Recommendations:

- To guarantee secure conditions for the retention of official paper files, these should be held in a location central to the unit or DG. In which case, file managers should keep only working files and/or copies of original files in their office, as necessary.
- If the original files are held in the unit, a common **storage plan** for the unit should be adopted, indicating the precise location of files.

2.3. ORGANISATION OF DOCUMENTS IN A FILE

Within their electronic file, the documents may be organised:

- either directly at file level;
- or into sub-files.

Within their paper file, the documents may be organised:

- by chronological order of arrival.
- by subject or procedure: filing according to the purpose of the document according to a predetermined hierarchy that is reflected in the organisation of the file: division of the subject into sub-themes represented by sub-files.
- by alphabetic order of authors or of title (not recommended in most instances).
- in numerical order: assigned a number at the time of registration (not recommended in most instances).

☞ The logic of document organisation must always be easy for anyone who is not the file manager to understand.

Storage of documents filed in several files:

If a document must be kept on paper and it is filed in several files, the original must be stored in the paper file with the longest retention period under the rules of the Retention List.

The other files contain only a copy of the document with a reference to the location of the original.

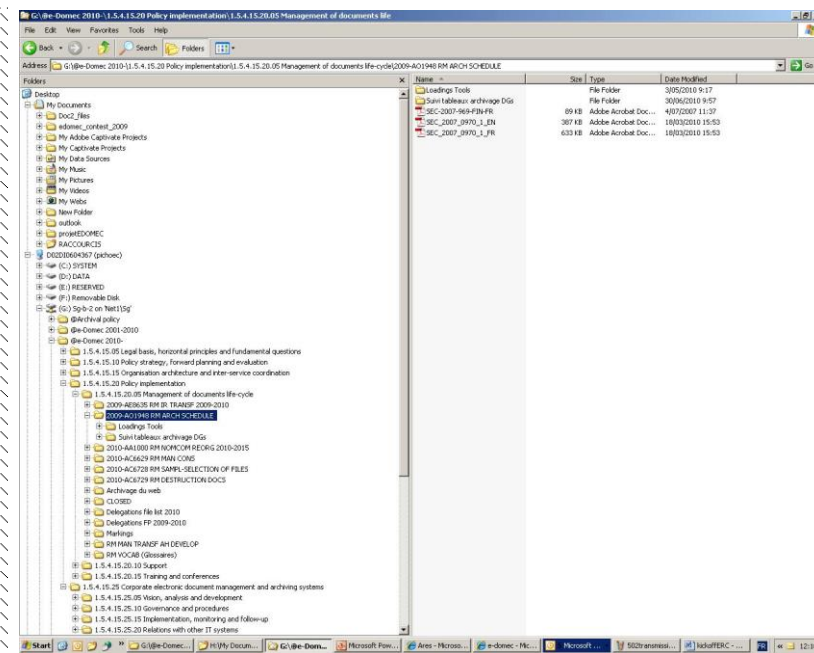
2.4. ORGANISATION OF THE UNIT SHARED DRIVE

The unit common hard drive or shared hard drive is merely a working area in which a set of information in electronic format can be centrally stored and shared.

⇒ The fact of storing documents on the unit shared drive in no way affects the fundamental obligation to register the document.

For ease of use, the shared drive should be organised in accordance with a simplified filing plan, to ensure that information is organised in one way only.

- ✓ **Example:**
- ✓ Tree structure of a common hard drive organised according to a simplified filing plan:



3. Access to attachments and files

Different search possibilities are offered to facilitate as far as possible the search for description sheets and hence access to documents.

Access to electronic files and documents is controlled by IT systems and applications.

3.1. SEARCHING FOR DOCUMENTS/FILES IN ARES

A number of different search possibilities are offered in **Ares** to facilitate, as far as possible, the search for documents, files or tasks.

- **Document search:**
 - **Full text search:** performs a search of both the metadata describing the attached electronic files and of their content (search engine function also available as a search box on each screen).
 - **Search criteria:** used to combine several search criteria at the level of Documents, Filing, Assignments, Attachments, Security.
 - It is also possible to combine a full text search and a search by criteria.

- **File search:** may be conducted by means of a simple search or by browsing the filing plan.

3.2. CONSULTATION AND BORROWING OF OFFICIAL PAPER FILES

Precise rules must be laid down:

- Those responsible for the file must ensure that:
 - the requester is authorised to consult the file
 - confidentiality standards are met
 - appropriate measures are taken for the physical protection of the material
- Traceable information on the borrowing or consultation of the file must be kept, indicating:
 - File code
 - Number of physical items and description
 - Requester's name, job, department, telephone number, etc.
 - Date of internal consultation or borrowing
 - Borrowing period or return date
- Internal borrowings must be monitored, including checks on:
 - Date of return of borrowed files
 - Check of the physical condition of the file at the end of the internal consultation or borrowing period

Practical tip:

If the official paper files are kept in the file managers' office, it may help to keep trace of file borrowing by attaching a paper sheet to the filing cabinets so that each borrower can identify him/herself, indicate which file has been borrowed and when it is due for return.

4. Public access to documents

4.1. BASIC RULE

Registering a document does not mean that it automatically becomes public and while any document that may potentially be retained by the Commission may, in principle, be consulted by any citizen (see Article 255 of the Treaty of Amsterdam and Decision 001/937), this is subject to a request for access to the document to be duly examined by the competent departments of the Commission.

4.2. EXCEPTIONS

Certain documents may be withheld from public access on the basis of specific exceptions, in instances where disclosure could be prejudicial to:

- public interest (public security, defence, military affairs, international relations, or the policies of the Community or one of its members)
- the commercial interests of an individual or organisation, legal action, legal counsel, or inspections, investigations and audits
- the Commission's decision-making processes, in instances where a decision has not yet been taken or when opinions are given for internal purposes or

- as part of preliminary deliberations or for consultations within the Commission

VI. CLOSURE AND RETENTION PROCEDURES

The rules of file retention are intended to guarantee:

- the protection of files over time: determination of retention periods,
- the clear definition of roles and responsibilities in terms of retention,
- the definition of strict procedures for the elimination of documents or files.
- the physical protection of files: rational management of physical and/or electronic storage areas.

1. A fundamental action: closing files

Every official file must be closed. As soon as a file is created, it should already be clear what procedural act will be required to consider that the case is completed and to close the corresponding file.

The value of a file varies according to its age. There are two distinct phases in the use of a single file.

- **Current files** containing documents consulted daily or frequently (= **current records**).

The physical responsibility for retention of the file lies with the Lead Department.

- **Closed files** corresponding to completed cases but that need to be retained for administrative or legal reasons (= **intermediate records**).

⇒ The physical responsibility for retention of the file lies with the Lead Department or with the DG's Central Archives, depending on how the DG is organised.

Closure is a fundamental operation:

- Closure implies a verification of the file: certification by the Lead Department that the case has been correctly dealt with and that, as a result, the file is complete.
- A closed file can no longer be modified: no documents can be removed from it or new documents filed on it (apart from certain exceptions).
- The retention period determined by the **Common Retention List (CRL)** and the **Specific Retention List (SRL)** runs from the date of closure of the file.

1.1. DEADLINE FOR CLOSURE

The closure of a file must take place once all actions triggered by the case are completed and when no further document needs to be created or added to the file.

Recommendation:

In practice, a file should not be closed as soon as a case is completed, but only after a minimum period of six months to be sure that all relevant documents have been correctly processed.

⇒ Check the file list, at least on an annual basis, to close files corresponding to completed cases and organise their transfer to intermediate records.

1.2. RULES OF CLOSURE

A file must be checked before it is closed, since a file retained for the long term without any preliminary review or reorganisation can result in extended information search time.

This operation must be carried out by the Lead Department (chef de file). It is essential, in that it focuses on the content of the file and will not be repeated at a later date.

Before any file is closed, therefore, it is essential to:

- Check that all the important documents have indeed been registered and filed in the file. If necessary, there is still time to add omitted important documents by registering one or more "Notes to the file" in Ares, containing the missing document(s).
- Weed the file: remove information and working documents of no further use. For the electronic file, this involves analysing and possibly deleting any documents that have simply been saved, and not registered (by unfiled them from the file in Ares).
- Complete the file metadata if necessary: indicate in particular the retention media and their physical location (storage area for paper files, IT applications for hybrid electronic files), the CRL/SRL category.
- Consolidate the file: unite the different parts of a single file dealt with by different units (for cases dealt with by an operational unit and a financial unit, for example).
- Process classified documents: check the documents and declassify if necessary.

Special case:

- **File made up of sub-files:** remember to close each sub-file as each aspect of the case is completed.
Remember to close the file itself when all the sub-files it contains are closed.

Recommendation:

For hybrid files (electronic and paper), not only must the electronic file be closed in Ares (Adonis for oldest files) but the paper file must also be closed

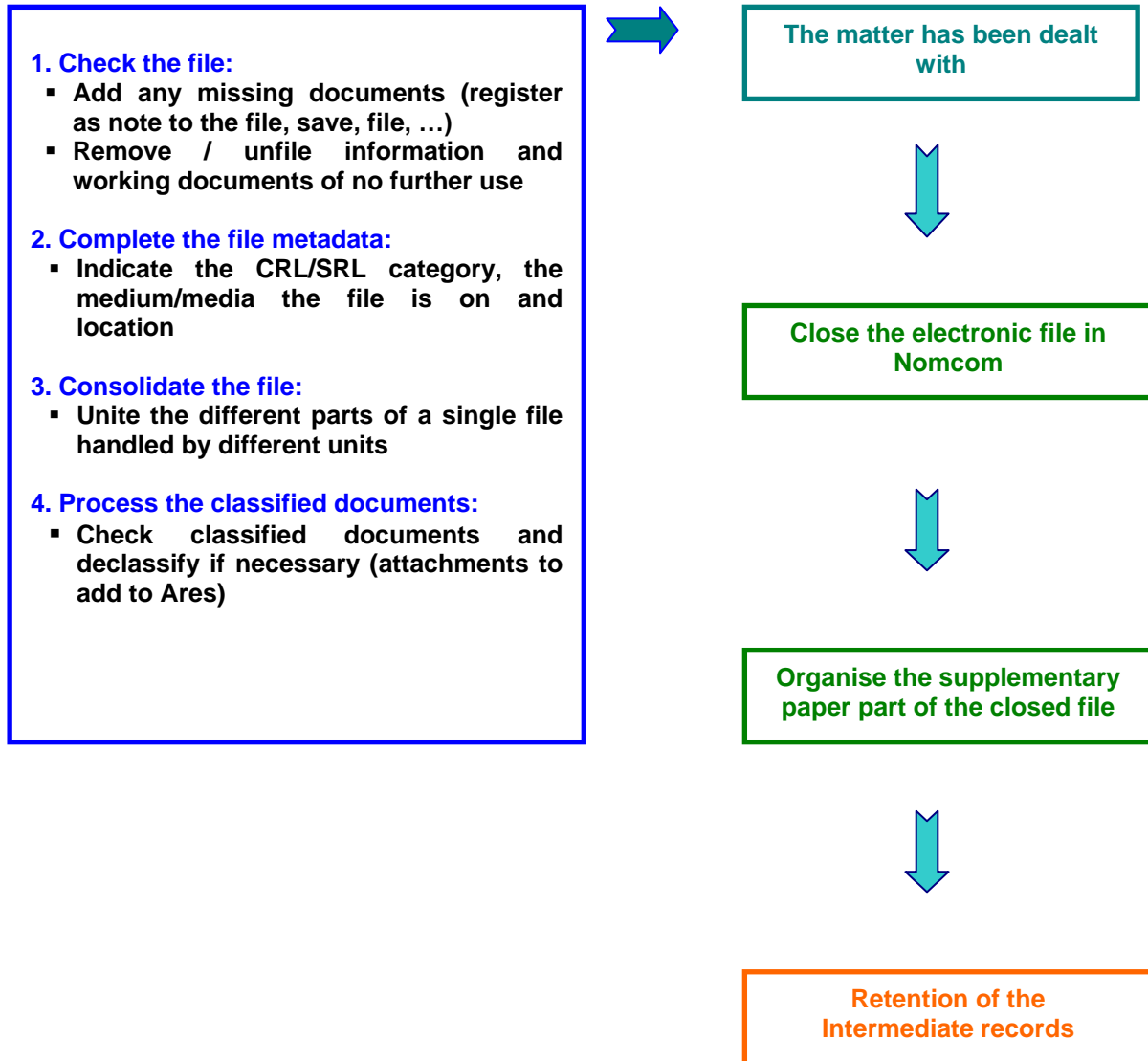
- **Electronic file:** close the file in via Nomcom3 for Ares (or in Adonis for oldest files)
- **Supplementary paper file:** Facilitate the identification of closed paper files by stamping the paper file and using a labelling system in a different colour.

1.3. DATE OF CLOSURE

Irrespective of the moment the file is closed, the "closure date" will be the date of the most recent document filed in the file.

If a file is reopened for the filing of new documents, the closure date will change only if the new documents filed carry a more recent date.

Operations to be carried out in order to close a file



2. Retention procedures

2.1. OBJECTIVES

Archives are all those documents, regardless of their form and physical medium, registered and kept in files, which the European Commission must retain either for a limited period or permanently.

Files created and held by the Commission must be subject to regular appraisal in order to:

- eliminate records of no further value;
- transfer to the Historical Archives Service only the categories of files for which this is foreseen in the Common Retention List (CRL) or Specific Retention List (SRL);
- guarantee adequate retention in the Historical Archives of records of permanent value.

To do so requires the ability to:

- determine the file retention period;
- identify responsibilities for the retention, review and elimination of archive files;
- identify closed files for transfer to the Historical Archives or to be destroyed in accordance with the Common Retention List;
- proceed to the elimination of certain documents as part of an administrative elimination procedure (laid down by the CRL in these particular instances);
- ensure rational management of paper and electronic storage infrastructure and areas.

Precise details of retention periods for particular archive series and the administrative practices to be followed can be found in the DG's archive schedule.

2.2. THE COMMON RETENTION LIST

➤ 2.2.1. Objectives of the CRL

The **Common Retention List (CRL)** is a regulatory instrument defining the period and conditions for retention of the Commission's official files.

The CRL:

- identifies the different types of file created and held by the DG/ Departments;
- determines the retention period for each type of file in the light of its administrative usefulness to departments, of legal obligations and of its potential historical value;
- determines the ARP (Administrative Retention Period) for each type of file, i.e. the number of years the file must be retained by the DG/Department. The retention period runs from the date of closure of the file;
- indicates the post-ARP action to be carried out by the DG/ Department at the end of the file's ARP: transfer to the Historical Archives, sampling/selection, elimination;
- determines the ultimate fate of files transferred to the Historical Archives: permanent retention or second review by the Historical Archives Service.

The Common Retention List was adopted and published by Secretariat-General in July 2007 (SEC(2007) 970):

- Its application by all Directorates-General and equivalent departments is **mandatory** for all files created under the e-Domec rules, irrespective of their medium (paper, electronic or hybrid).
- It may be applied by the DG/Department, on a voluntary basis, to closed files not constituted under e-Domec rules.
- It may be supplemented by **Specific Retention Lists (SRL)** at DG/Department level for series of files specific to the DG/Department and not covered by the CRL. In this instance, the SRL must have been adopted within six months of publication of the CRL.

N.B.: only the PMO has a Specific Retention List.

➤ 2.2.2. Structure of the CRL

The Common Retention List is presented in the form of a management table indicating the metadata for retention by major type of file.

- 1) **File Types:** The types of files make it possible to identify files relating to the same type of actions, questions or procedures. They are divided into 12 main types subdivided into sub-types:
 - Institutional and governance questions
 - Strategy and coordination
 - Commission decision-making
 - EU financial system & Budget
 - Policy development
 - Implementation of policies and legislation
 - Programmes, projects and grants
 - International activities and enlargement
 - Transparency, information, communication and relations with citizens
 - Monitoring the application of Community law
 - Legal proceedings
 - Administration
- 2) **Description:** General description of file content: introductory comments on the kind of files concerned by each type of file.
- 3) **ARP (Administrative Retention Period)** = period (number of years) during which the DG/Department is required to retain a file in the light of its administrative usefulness, of any associated legal obligations and of its potential historical value.
The ARP runs from the date of closure of file.
- 4) **Post-ARP Action or First Review** = action to be carried out by the DG on expiry of the ARP:
 - **THA:** Transfer to the Commission's Historical Archives Service.
 - **SAM/SEL** = Sampling and/or Selection
 - **Sampling:** Method of appraisal whereby, on the basis of objective criteria, a representative portion of files for retention is chosen from a body of files too large to be retained in its entirety.
 - **Selection:** Appraisal of a body of files for elimination in order to retain certain files on the basis of subjective criteria (importance, media impact).
 - **EL** = Elimination: physical destruction of files
- 5) **Action Following Transfer to the Historical Archives:**
 - **PP** = Permanent preservation

- **2nd REVIEW:** A second appraisal, carried out by the Historical Archives Service, of the historical value of files to decide whether they should be permanently retained or eliminated.
- 6) **Lead Department for Preservation:** Indication of the DG or DGs using this type of file and responsible for their retention.
 - 7) **Observations:** Elements to be taken into consideration by the DG as regards file retention.

⇒ The retention period of a file is determined by:

- its Administrative Retention Period (ARP): the period of its retention in intermediate records by the DG
- the action applicable at the end of the ARP (post-ARP action or first review)
- if necessary, the action applicable after transfer to the Historical Archives Service (post-THA action).

2.3. THE ARCHIVE SCHEDULE

The archive schedule is an administrative document that governs the practical implementation of file retention in the DGs.

The schedule is drawn up by the DG DMO in collaboration with the Lead Departments, and sets out actions to be taken and responsibilities for the retention and elimination of official files in accordance with the Common Retention List.

The archive schedule must therefore give indications regarding:

- The correspondence between the filing plan headings to which the files are attached and the CRL/SRL categories. The aim is that when a new file is created, its long-term retention attributes should be automatically assigned in accordance with the attachment heading in the filing plan.
- A note on retention setting out:
 - Internal procedures regarding file retention, those responsible for file retention and their responsibilities.
 - The location of files and their medium of retention (electronic and/or paper);
 - The minimal file content;
 - Any rules regarding the elimination of documents;
 - Factors that may give rise to the reopening of a closed file (OLAF investigation, case brought before the Court of Justice, complaints to the Ombudsman, etc.).

3. Retention implementing rules

3.1. CALCULATING THE ARP

The ARP runs from the date of closure of the file, i.e. from the date of the most recent document in the file (most recent registration or save date).

☞ If the file has not been properly closed, a forced closure will be carried out using as the date of closure the date of the most recent document in the file.

Recommendation:

- To guarantee secure conditions for retention of closed official paper files, these should be kept centrally at DG level.
- If closed files are not located in a central archive attached to the DG's Archives service, the Lead Department remains responsible for their retention during their ARP.

3.2. ORGANISATION OF INTERMEDIATE RECORDS

If intermediate records are retained centrally by the DG, closed files must be transferred from the Lead Department to the DG's Central Archives Department.

If there is no Central Archives Department, the Lead Department must guarantee the retention of the closed file throughout its ARP (Administrative Retention Period).

- ⇒ Consult the DMO on the procedure applied within the DG for the retention of intermediate records.

3.3. REVIEW AND TRANSFER OF FILES TO THE HISTORICAL ARCHIVES

➤ 3.3.1. Review operations

The rules for the review and transfer of files to the Historical Archives are intended to:

- guarantee the long-term retention of the European Commission's archives;
- facilitate access to the Historical Archives;
- enable the Historical Archives of the European Commission to be opened to the public after 30 years.

DGs are under obligation, at least once a year, to identify those files whose ARP (Administrative Retention Period) has expired and to implement the post-ARP action laid down in the DG's archive schedule:

- Transfer to the Historical Archives Service of the Commission,
- Sampling/Selection
- Elimination

This operation, known as the **first review**, must be carried out by the originating Directorates-General/Departments under the responsibility of the DG/Department's DMO.

Files not associated with a retention list, i.e. files created before the introduction of the e-Domec rules, will be reviewed no later than 15 years from file closure. In these instances, the Historical Archives Service will assist departments in determining which files, if any, may be transferred. Prior approval from the Historical Archives Service is required before any transfer can be made.

For files transferred to the Historical Archives, the CRL/SRL may stipulate a **second review** to identify, no later than 25 years after their closure, files that will be retained definitively (Historical Archives) or eliminated, possibly after sampling or selection.

This second review, based on the historical value of the files, is carried out by the Historical Archives Service in cooperation with the originating department or its successor.

➤ **3.3.2. Rules of transfer to the Historical Archives**

A transfer of files to the Historical Archives must follow three principles:

- Physical transfer of the records
- Preservation of the metadata associated with the records
- Following of correct procedures for the transfer

⇒ **The Historical Archives Service, in collaboration with the Secretariat-General, has produced a "Guide to transfers to the Historical Archives".**

