Emily O'Reilly

European Ombudsman

Decision of the European Ombudsman on Records Management

This Decision contains the European Ombudsman's records management principles, rules and policies. Further implementing rules are laid down in thematically organised Annexes, which form part of this Decision.

The Decision seeks to align the Office's records management to the best practices of other EU institutions and to international records management standards. It does so whilst introducing solutions specific to the organisation of the Office.

Article 1: Records management systems

1.1 **Scope**

This Decision applies to the Office's two main records management systems; the general records management system (Advanced Reports System or Ares) and the complaints management system (CMSEO). The Office uses other corporate or internal tools, for example for the management of HR and financial procedures. These tools are each equipped with their own records management system and are therefore not covered by this decision.

1.2 CMSEO

CMSEO records information and documents related to case handling and inquiries. It contains a working area, an archive, a workflow feature, remote access and reporting features.

1.3 ARES

Ares records information and documents relating to the non-case handling or inquiries activities of the Ombudsman's Office.

ARES contains a general filing plan, a common retention list, assignment and workflow features, remote access, capacity for integration with other IT systems, and reporting features.

1.4 Processing of records and language

As far as legally and practically possible, the Office's records and their processing shall be electronic. This includes the final archiving for historical purposes.

The working language applicable to records management - including meta-data and titles of files and records - is for practical purposes English.

Article 2: Documents - definition

A 'document'[1] in the present Decision refers to the following:

(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audio -visual recording) concerning a matter relating to the policies, activities and decisions falling within the European Ombudsman's sphere of responsibility;

(b) the reference to "content" above includes content produced by the Ombudsman or any member of staff in her/his professional capacity, through Office or non-Office devices, or through online communication tools, including social media.

Article 3: Obligation to register, and related measures

3.1 The act of registration implies (a) separate recording of specific individual documents or (b) the inclusion of documents in registered files, or equivalent, that are managed through dedicated records management tools.

The registration rules below do not apply to the private spaces of staff and the separate spaces of the Staff Committee (cf articles 4 and 5 below).

3.2 All final versions of documents produced in the course of the European Ombudsman's performance of the core activity of investigating possible instances of maladministration, and policy documents related thereto, shall be registered.

3.3 All incoming and outgoing paper correspondence shall be registered, subject to the following exceptions:

a) The incoming correspondence has been identified, by designated responsible staff, as clearly being of an abusive nature.

b) The incoming correspondence has been identified, by designated responsible staff, as clearly being for information only, including of a promotional nature, and not requiring any action by the Office.

3.4 All incoming and outgoing electronic correspondence (email, sms, instant messaging or similar and social media) shall be registered, subject to any of the following exceptions:

a) Where access to the electronic correspondence by other colleagues is not necessary in order to ensure completion of the work process in question (no business continuity need);

b) Where the electronic correspondence would not be needed for the purposes of regulatory or other checks by EU control bodies in the event that a check on the particular work were to be undertaken (no accountability need);

c) Where the electronic correspondence is part of inter-institutional processes where the lead institution is responsible to manage the related records;

d) Where the electronic correspondence is with other public bodies of the European Union, relates to a very short-lived work process (measured in weeks), and would be subject to no retention period at the end of that process (proportionality).

[1] The definition of document is that set out in Article 3(a) of Regulation (EC) No. 1049/2001.

3.5 E-mail correspondence that must be registered, and which occurs through functional e-mail accounts (non-personal e-mail accounts to which one or more services have full access), may be subject to conversation/batch based registration if this does not involve a postponement of the registration of more than four weeks.

3.6 Electronic correspondence that form part of the routine activities related to contacts with the media may be left unregistered.

3.7 All final versions of administrative documents that are necessary for the Office's day-to-day functioning shall be registered.

3.8 The systematic use of individual document storage spaces, notably in Windows Explorer, in e-mail systems or on other devices, shall as far as possible be avoided.

3.9 The Office shall, at all levels, introduce day-to-day practices that from the outset facilitate a high standard of substantive and procedural compliance with the principles and rules of transparency and data protection. It shall moreover introduce practices that allow for a high standard of re-use of the documents and their related data.

Article 4: Private and personal spaces for staff

4.1 The Office provides clearly defined private spaces for staff members in their Outlook account and staff can create folders which they mark as private in Windows Explorer. Content which is legitimately held in these private spaces shall not be considered to be held by the European Ombudsman for the purpose of implementing legislation on access to documents, data protection, archiving, or other related legislation or rules.

4.2 A legitimate personal interest may further exist in relation to past work and communications that the staff member in question expects may be important background material for their annual staff assessment exercise. Similarly, staff members' communications with the Office's Staff Committee, the ethics correspondents or similar communications (such as with a trade union), may legitimately be held in the private spaces.

4.3 In order for content to be held legitimately in private spaces, the content must be such that no other colleagues could possibly have a present or future need to access it for the purpose of carrying out their professional duties.

Further, the content may not be such that its storage or future processing could possibly infringe on any other individual's right to protection of their personal data.

4.4 In addition to obviously private content, certain Office related content may legitimately be considered to be personal although not private, for example, notes or personal thoughts on draft documents or other matters.

4.5 The European Ombudsman cannot provide any guarantees as to the accessibility of the content of private or personal spaces in relation to criminal, fraud or other investigations carried out by responsible bodies. Neither can the Office guarantee that a Court will accept that the content of such spaces does not constitute documents held by the Office for the purposes of the EU's legislation related to public or privileged access to documents.

4.6 Staff leaving the Office upon termination of their duties shall delete all private and personal content held on Office devices.

Article 5: Separate spaces for the Staff Committee

5.1 The Office provides clearly defined spaces for the Staff Committee in its Outlook account and in Windows Explorer respectively. Content which is legitimately held on

Office or non-Offices devices shall not be considered to be held by the European Ombudsman for the purpose of legislation on access to documents, data protection, archiving, or other related legislation or rules.

5.2 Staff who communicate with the Staff Committee on sensitive matters have a legitimate expectation that such matters are not accessed by, or disclosed to, anyone in the Office without their express and informed consent. The Staff Committee itself has a corresponding legitimate interest in being able to discuss sensitive staff matters in confidence.

5.3 Therefore, as an exception to the general rule, records related to the work of the Staff Committee cannot be subject to the general right of immediate access that is otherwise held by the management, the Data Protection Officer and/or any other person/function in the Office that holds such general rights of access to documents internally.

5.4 The Staff Committee, being an organ provided for in the Staff Regulations, fulfils a number of tasks of a formal nature, and its activities are reflected in the Office's filing plan. At the same time, with a view to ensuring and promoting transparency, the Staff Committee therefore will ensure regular formal registration of documents that are not covered by any staff member's legitimate expectation of confidentiality.

5.5 The European Ombudsman cannot provide any guarantees as to the accessibility of the content of the Staff Committee spaces in relation to criminal and/or fraud investigations. Neither can the Office guarantee that a Court will accept that the content of such spaces does not constitute documents held by the Office under the EU's legislation for the purposes of public or privileged access to documents.

Article 6: Retention of documents and data

6.1 Records retention periods are managed through the rules laid down in this Decision and the 'Common Retention List' annexed to this Decision. The use of a 'Common Retention List' reflects standard international practice and facilitates the full or partial automation of the management of retention periods.

6.2 Retention periods cover two main time related issues: 'Administrative retention periods' and indefinite archiving.

The administrative retention period reflects the period during which the Office can reasonably anticipate that it, or other persons or bodies, may need to consult the documents. The indefinite archiving refers to the permanent archiving of documents for the purpose of long-term accountability, transparency and historical recording of the Office's activities.

6.3 The retention periods referred to in the ‘Common Retention List’ and in this Article shall apply retroactively.

6.4 The Office's retention of documents and data shall to the maximum extent possible reflect the established and evolving rules and best practices that EU institutions apply by way of good practice or on the basis of inter-institutional agreements.

6.5 Documents related to staff, finance and communications/media shall be covered by the retention periods that are common to the EU institutions' relevant practices.

6.6 The final versions of documents relating to policy and strategy shall, subject to any special provisions including provisions for the protection of personal data, be kept indefinitely.

6.7 Complaint related documents, including records of internal discussions but excluding confidential information[2], shall be subject to the following retention periods:

a) two years where the case was outside the Ombudsman's mandate;

b) ten years where the case was within the Ombudsman's mandate (this includes complaints in which the Ombudsman opened an inquiry and complaints in which the Ombudsman did not open an inquiry either because they were inadmissible or for lack of grounds).

6.8 Complaint related documents containing confidential information, obtained from an institution or a Member State during an inquiry, and declared to contain confidential information shall be retained only for so long as the inquiry is ongoing including any period of time for dealing with a request for review.

6.9 Complaint related documents containing information provided by a complainant which the Office itself has classified as confidential, or containing information which a complainant has identified to be confidential, shall be retained only for so long as the inquiry is ongoing including any period of time for dealing with a request for review, subject to the exceptions at 6.10 and 6.11.

6.10 In exceptional cases, documents referred to at 6.9 shall be retained for a period of 10 years where:

(a) it is clear that the information in question is, or may well be, important for an understanding of the case in the future, including circumstances in which the case has precedence or training value;

(b) retention of the document is likely to serve historical or public interests; or

(c) retention of the document may be relevant in the context of actual or possible future formal procedures, including audits or court proceedings.

6.11 Documents referred to at 6.7(b) or 6.9 that relate to complaints which are of significant public importance or which are otherwise considered major cases shall be anonymised and archived indefinitely for historical purposes.

6.12 The decisions and actions in relation to the handling of confidential documents (removal, retention and archiving) shall be duly recorded on the case file.

6.13 Ad hoc removal/deletion of documents and related data shall be authorised only by the Secretary-General on proposal by the responsible Director in consultation with the Office's Document Management Officer.

6.14 For the sake of completeness, in accordance with the Ombudsman's Decision of 30/03/2021 laying down the security rules and procedures for access to EU classified information by the European Ombudsman in the context of inquiries, the Ombudsman does not hold any EU classified information (EUCI) and thus this type of information is not subject to the Office's retention policy.

Article 7: electronic collaborative, individual and online tools

7.1 All Office related content produced or received through e -mails, mobile devices, social media, websites, collaborative websites, or similar tools, is a 'document' and in

[2] 'Confidential information' does not refer to EUCI but to information that is treated confidentially by the Ombudsman due to its sensitive or confidential nature and/or at the request of the complainant, institution or Member State that provided it.

principle subject to the applicable rules in the Ombudsman's Decision on Records Management. Official communications handled on a personal device shall be copied to an official Office file. The related practical arrangements are set out in a dedicated annex to the present Decision.

7.2 In the context of requests for public access to documents, a data protection check, audits, or any other similar information needs related to regulatory rules of the European Union or any of its Member States, any person working, or having worked, for the Office may be asked to verify whether his/he r (a) mobile device(s), (b) e-mail accounts, or any other equivalent tool, contains documents relevant to the subject matter in question that have not been registered.

7.3 In relation to public websites, the Office shall, as far as appropriate, ensure coherence with the practices agreed at the European Union's Inter -institutional Editorial Committee.

Article 8: Public Register

The Ombudsman implements, for its organisation, the principle of online public registers through publication of core business documents on its online cases section, through direct and full publication of all documents adopted in relation to strategy, policy and high-level management, and through the publication of its document filing plan.

Article 9: Document Management Officer

A member of staff shall be assigned the role of the Office's Document Management Officer (DMO), which will be reflected in that person's job description. The Office may also assign the role of Deputy DMO to another staff member. The Document Management Officer shall ensure the implementation of the present decision and the related rules and principles, provide records management training to the Office's staff, and make proposals for improvement to the Office's records management practices.

Article 10: Transparency Officer

The Ombudsman shall appoint a Transparency Officer for a renewable 2-year term. The Ombudsman may also appoint a deputy Transparency Officer. The Transparency Officer(s) shall centrally handle initial requests for public access to documents, and shall promote best record management practices that allow for an efficient handling of such requests.

Article 11: Security

11.1 The handling of EUCI is regulated by the Decision of the European Ombudsman of 30/03/2021 laying down the security rules and procedures for access to EU classified information by the European Ombudsman in the context of inquiries.

11.2 The Office shall issue and keep up-to-date guidelines for dealing with, and protecting, information received during the inquiry process that is not EUCI but that the Office considers confidential.

11.3 In relation to ICT, the work of the Office is technologically integrated into, or carried out through, ICT systems of other institutions, notably the European Parliament. The Ombudsman and all staff shall respect the related security rules and guidelines.

11.4 All members of staff shall sign a declaration to the effect that they have read and understood the security rules and guidelines.

Article 12: Entry into force

12.1 When this Decision enters into force, the following annexes shall enter into force also:

a. Common Retention List

b. Annex on internal access to documents

c. Annex on draft documents

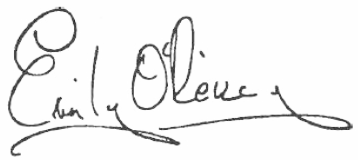
d. Annex on recording of electronic communications

12.2 This decision enters into force on the day of its adoption and repeals the previous decision on records management of 6/9/2017 (Ares(2017)4342927).

11.3 Guidelines or instructions to facilitate the implementation of specific provisions of this decision may be adopted by the Secretary-General or the responsible Directors.

11.4 The Common Retention List may be amended when needed by a separate decision of the European Ombudsman.

Strasbourg, 28/06/2022



Emily O'Reilly

European Ombudsman

ANNEXES to the Records Management Decision

Annex a - Common Retention list (separate excel file)

Annex b - Internal access to documents

The Office operates with a high level of internal transparency. It is not generally necessary to demonstrate a necessity to access internal documents. Members and staff have access to documents of the Office, unless there are specific reasons to limit or prevent such access.

A basic guiding rule shall be that, if the documents concerned would be subject to disclosure following a request for public access to documents, the documents shall normally be considered accessible to all members of staff.

The rules applying to specific fields of activity are the following:

Human resources management

All documents for human resources management in relation to current, former and potential staff, are covered by a presumption of confidentiality. They are strictly covered by access on a need-to-know basis, in particular to protect personal data.

Finance management

Documents related to ad hoc procedures related to contracts shall be covered by a presumption of confidentiality. They are strictly covered by access on a need-to-know basis.

Case management

The 'file' of a case is the compilation of final recorded documents in the 'Archive' area of the Office's current case management system, and for previous systems in the equivalent of that area, with the exception of “outside mandate” cases for which the file comprises, for reasons of simplification, notes in the Case Form and correspondence that is processed and stored through the use of e-mail integration tools in the system.

As a rule, the case files are accessible to all staff involved in case handling, including staff involved in strategy, policy, communication and outreach.

By way of exception to the above rule, confidential documents may be registered as internally confidential, and accessible on a need -to-know basis only. The same exception may be applied to documents disclosing the personal data of complainants or of third parties, or disclosing other particularly sensitive material. In such instances, because of the

sensitivity of the data or material, and/or because of the requirements of risk management, access may be restricted on a need-to-know basis only.

The drafts circulated between the case handlers and their superiors, and which are located in the 'Working Area' of the Office's Case Management System, shall be accessible on a need to know basis, which in the first place involves staff with the role of approving draft texts.

Annex c - Draft documents

Administrative documents:

Draft versions of any document in the area of administration may be produced and kept for as long as the setting or matter is open. When the setting or matter is closed or completed, drafts shall normally be destroyed.

The drafts submitted by staff to the Ombudsman for her/his signature, and which concern strategy and policy, shall be registered and kept indefinitely. They shall be fully accessible internally, and disclosed in case of external requests for access.

Complaint-related documents:

Draft versions of any document related to case handling shall be saved in the Working Area of CMSEO and shall be retained for either two or ten years depending on whether they relate to outside mandate or within mandate complaints (subject to provisions in relation to the retention, removal and archiving of confidential documents cf Article 6.9 - 6.11).

Performance assessments:

Draft performance assessments may be kept by staff in their private space(s), if the draft has an actual or potential relevance to the assessment of their own performance or conduct.

Draft assessments may be kept by management staff if the drafts in question have an actual or potential relevance to its assessment of staff. Once the procedure related to that assessment has been finalised (including reviews as the case may be), the drafts shall be destroyed.

Other:

Other specific drafts may be kept by decision of the Ombudsman or of the Secretary-General, if s/he deems the documents to be of significant long -term value, of academic interest, necessary to protect essential interests of the Office or the European Union, or if the content of the draft in question is likely to be of significant use to the Office's future work.

Annex d - Recording of electronic communications

In principle, staff should avoid using text messaging, instant messaging or similar tools (for example WhatsApp or Cisco Jabber chat) for substantive work communications.

This said, and in the absence of other technological means, all Office related content produced or received through mobile devices, social media, websites, collaborative websites, or similar tools, if not already registered (where necessary) in the general records management system, shall be registered (where they meet the registration criteria) in the following manner:

1. A screenshot of the content should be taken (including, in the context of a text or other form of instant messaging, all available metadata such as the details of the sender and recipient and the time the content was sent or received);

2. The screenshot should be imported into a Microsoft WORD document (with the metadata either added separately or incorporated as part of the screenshot) and that document converted to PDF format.

3. The PDF document should then be registered in either CMSEO or Ares depending on whether or not it is case or administrative-related.