



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

To: Ms. Teresa Anjinho
European Ombudsman
[Redacted]

Athens, 24/11/2025

Subject: ENISA reply to the Ombudsman's letter of 27/08/2025 – information on the actions taken on the improvement suggestion

Dear Ms. Anjinho,

In your letter of 27 August 2025, you informed ENISA about your Decision to close case 1689/2024/MIG with the conclusion that the Agency had accepted the Ombudsman's proposal. As a matter of good administration, you required that ENISA should provide a list of documents that it identifies when it replies to a request for public access to documents under Regulation 1049/2001, unless the very disclosure of a list undermines interest(s) to be protected. ENISA was requested to inform you by 26 November 2025 of any action taken in relation to this requirement.

Following your recommendation, let me share with you that ENISA has updated its internal policy on public access to documents requests, by including the following provision:

"In case where ENISA finds that no or only very limited public access can be granted, it shall try and address the access request by providing information instead, as it facilitates a requester's understanding of the institution's decision and the formulation of a request for review, if necessary. For this reason, the Agency shall aim to provide a list of the documents that it identifies while replying to a request for public access to documents under Regulation 1049/2001, unless the very disclosure of a list undermines the interest(s) to be protected."

Attached herewith, please find the applicable ENISA Policy, as Annex.

I remain available for any further information or clarification you may require.

Yours Sincerely,

[Redacted]
Head of Unit, Executive Director's Office

Annex: ENISA Policy on public access to documents requests



ENISA POLICY 2025-02 ON PUBLIC ACCESS TO DOCUMENTS (PAD) REQUESTS

1. SCOPE AND PURPOSE

The scope of this policy covers public access to documents (PAD) requests pursuant to Regulation (EC) 1049/2001¹ that is applicable to ENISA as per Article 28 of the Regulation (EU) 881/2019 (Cybersecurity Act)².

The arrangements for implementing Regulation (EC) No 1049/2001 have been adopted by means of the Decision No MB/2019/17³ of the Management Board of ENISA on public access to ENISA documents.

This policy addresses the practical modalities for handling of PAD requests that are submitted to the Agency, including the relevant processes and workflows that are followed and replaces the Policy on PAD requests of May 2019⁴.

2. BACKGROUND

Transparency is a guarantee of greater legitimacy, efficiency and responsibility of the public administration with respect to its citizens in a democratic system.

Article 15(3) TFEU states that:

“Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union institutions, bodies, offices and agencies, whatever their medium, subject to the principles and the conditions to be defined in accordance with this paragraph”.

Article 26 (1) of the CSA stipulates that the Agency's activities should take place with a high level of transparency.

Against that background, in order to effectively support the timely handling of the access to documents requests, this policy aims to outline with clarity the process within the Agency and the key actors involved.

¹ [Regulation - 1049/2001 - EN - EUR-Lex \(europa.eu\)](#) Official Journal, OJ L 145 31/05/2001, p. 0043 – 0048.

² [Regulation - 2019/881 - EN - EUR-Lex \(europa.eu\)](#), Official Journal, OJ L 151, 7.6.2019, p. 15–69.

³ [MB Decision 2019-17 on public access to ENISA documents.pdf](#)

⁴ [ENISA Policy on Public Access to Documents \(PAD\) Requests 2019](#).

3. DEFINITION OF DOCUMENTS

The notion of '**Document**'⁵ is understood within the meaning of Article 3(a) of the Regulation (EC) No 1049/2001.

It is any content drawn up or received by ENISA, in whatever medium (written on paper or stored in electronic form or as a sound, visual or audio-visual recording) concerning a matter related to the policies, activities and decisions falling within the competence of ENISA and carried out in the framework of its official tasks and activities.

The definition of 'document' covers any document, regardless of its purpose, the importance of its content, the way in which it is presented, its size and length. This includes emails (except for personal correspondence with no professional content) and internal documents (documents which either have not been finalised or are not intended for publication).

Also documents related to the operational functions of ENISA fall under the obligation of transparency of Article 26 of the Cybersecurity Act. These include inter alia replies to questionnaires, operational topics, minutes/records of coordination meetings, case notes, presentations, operational and analysis reports.

The right of access applies only to existing documents. This includes documents, information and data that can be extracted from a database by means of a routine search tool. Accordingly, requests for access to information/data contained in a database shall fall under the framework of the Regulation (EC) No 1049/2001 and shall be treated as requests for access to documents provided that the data can be extracted from the database by means of a normal or routine search.

European Ombudsman provided practical recommendations for the EU administration for recording of text and instant messages. While dealing with requests for public access to documents that could cover text and instant messages, the Ombudsman recommends to consider all locations where such messages might be stored, including electronic devices used by staff, and assist staff potentially holding such messages in their searches, for example by giving instructions. The decision to record a certain piece of information in the administration's document management system should be made on the basis of the content of the document, not on its medium (which may be a letter, an email, a text or instant message).

4. ASSESSMENT OF DOCUMENTS

The fact that a piece of information falls under the concept of 'document' of Article 2(3) of the Regulation (EC) No 1049/2001 as developed by case law, does not mean that it will automatically be released in case of a request for access.

Indeed, access may be denied if an exception foreseen under Article 4 of the Regulation (EC) 1049/2001 applies to the whole or part(s) of the "document".

Special diligence should be given for the treatment of sensitive documents under Article 9 of the Regulation (EC) 1049/2001 and in accordance with ENISA's rules on protection of European Union Classified Information (EUCI).

With regard to the requests for public access to documents under Regulation (EC) No 1049/2001¹¹ or information requests in relation to grants and procurement, the process described in the Guidance Note of the European Commission⁶ shall be consulted and respected.

4.1 EXCEPTIONS TO THE RIGHT OF ACCESS

In accordance with Article 4 (1) and Article 4(2) of the Regulation (EC) 1049/2001, the Agency shall refuse the access to a document if disclosure would undermine the protection of:

⁵ The adopted definition is in line with [2023-01 ENISA Document Management Policy](#).

⁶ [GUIDANCE NOTE ACCESS TO INFORMATION AND DOCUMENTS RELATED TO PROCUREMENT AND GRANTS](#).

- Public interest as regards public security, defence and military matters, international relations, the financial, monetary or economic policy of the Community or a Member State.

In the case of ENISA, this could include also the cybersecurity of ENISA's own operations, as well as the cybersecurity of ENISA's stakeholders.

- Privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data.

In the case of ENISA, the main applicable regulation is Regulation (EU) 1725/2018 (EUDPR), in particular Article 9 (Transmissions of personal data to recipients established in the Union other than Union institutions and bodies). In each PAD request where EUDPR is applicable, the ENISA's DPO should be involved and a careful analysis should be conducted on the necessity and proportionality of the transfer, in line with EDPS recommendations and relevant case law.

- Commercial interests of a natural or legal person, including intellectual property, court proceedings and legal advice, the purpose of inspections, investigations and audits; unless there is an overriding public interest in disclosure.

Access may also be refused by ENISA in accordance with Article 4(3) of the Regulation (EU) 1049/2001, regarding a document drafted only for internal use or received by the Agency, which relates to a matter where the decision has not been taken and if the disclosure of the document would seriously undermine the decision-making process, unless there is an overriding public interest in disclosure. This exception covers all internal (not finalised) documents and relevant communication between ENISA staff members, as well as between ENISA staff members and other relevant stakeholders.

Refusal to grant access could also apply to a document containing opinions for internal use as part of deliberations and preliminary consultations within the Agency, even after the decision has been taken, if disclosure of the document would seriously undermine the decision-making process, unless there is an overriding public interest in disclosure.

4.2 PRIOR CONSULTATION OF THIRD PARTY

As regards third party documents, i.e. documents that have been provided to the Agency by a third party, ENISA may only disclose them in the context of a PAD request, after having received the consent of the owner of the document.

In the absence of any reply, or if the owner cannot be found or identified, the system of exceptions provided in paragraph will be considered, taking account of the legitimate interests of the third party on the basis of the information at its disposal.

In case of documents reflecting Member States' positions, the respective Member States shall be consulted, in accordance with the principle of loyal cooperation.

5. HANDLING PROCESS

5.1 ACTORS AND STEPS TO BE FOLLOWED

The key actors associated with the handling of PAD requests at ENISA are as follows:

1. **The PAD request coordinator:** this function is performed by duly delegated staff within the Executive Director's Office. The PAD request coordinator:

- a. Manages the functional mailbox that is used for PAD requests (access-documents@enisa.europa.eu);
 - b. Conducts a first assessment of the request, in particular whether it qualifies or not as PAD request. The EDO/Compliance Sector may be consulted if needed.
 - c. Registers the incoming request and acknowledges receipt to the applicant.
 - d. Conducts first research on the subject of the request, considering registered documents and makes a generic desktop research about publicly available documents (related to the request) and information about the requester i.e., in case it is a journalist).
 - e. In case contributions from specific Units are needed, informs the competent Heads of Units on the request, by providing any related information and setting clear deadlines, and ensures that the response is provided on time.
 - f. Provides a first draft reply on the basis of the information received and initiates the relevant ARES workflow with the standard template (See Annex I: "ARES workflow for PAD requests"). In case of sensitive cases, the ARES workflow will be marked as confidential. In case of questions, the EDO/Compliance Sector may be consulted.
 - g. Registers the final draft reply in ARES and dispatches to the requester.
 - h. Maintains and updates the PAD requests inventory:
 - i. Monitors the timelines for response to the PAD requests and informs the Head of Compliance on pending requests and upcoming deadlines.
2. **The Compliance Officer:** performs a legal and quality check of the draft reply, in particular assessing whether the reply is in compliance with the applicable legal framework as contained in Regulation (EC) 1049/2001 and whether exceptions are applicable. The Compliance Officer may undertake some of the tasks of the PAD request coordinator in certain cases.
 3. **The Data Protection Officer:** reviews draft replies where a data protection aspect is involved and makes an assessment on the basis of the Regulation (EU) 2018/1725 and/or other relevant applicable data protection rules.
 4. **The Head of Sector for Compliance:** reviews the draft reply and validates from compliance perspective.
 5. **The Head of Executive Director's Office:** reviews and approves the draft reply; signs the final reply.

5.2 HANDLING PAD REQUESTS AT ENISA

5.2.1 Timeline & process

Initial and confirmatory applications should be answered within 15 working days from the date of registration of the application

As soon as the application is registered by the PAD coordinator, an **acknowledgement of receipt** shall be sent to the applicant from the dedicated functional mailbox access-documents@enisa.europa.eu, unless the document(s) requested is already publicly available. In such case the reply with the link to the public document(s) can be provided shortly after receipt of the application.

The day from which the time limit runs is the day of registration.

The acknowledgement of receipt shall indicate the date when the 15 working days period expires.

Failure to reply to an initial application within the prescribed time-limit shall entitle the applicant to make a confirmatory application.

If the request is not sufficiently clear, EDO must ask the applicant to provide additional information. In that case, the 15 working day time-limit is suspended and restarts only once the applicant has provided the requested information.

In the case of complex or insufficiently precise applications, the deadline may exceptionally be extended by 15 working days (total of 30 working days). In this case, a holding reply must be sent to the applicant explaining the reasons for the extension of the deadline.

5.2.2 Third-party documents

The PAD request coordinator or/and the responsible line manager shall contact the third party/owner of the document and ask for the information related to the PAD request. The third party/ originator of the document consulted should respond about the possibility on not to disclose the document **within 5 working days**.

If the originator of the document objects to the disclosure on the basis of the exceptions provided for in Article 4 of the Regulation (EU) 1049/2001, the Agency should confirm the refusal and not overrule the third party at the initial level.

5.2.3 Language

Requests for access to documents can be submitted in any of the official EU languages. The reply must be written in the same language. The reply can be sent in another language than the language of the request upon written agreement of the applicant.

5.2.4 Response to PAD requests

Any decision which is (partly) negative shall be duly justified, on the basis of the exceptions mentioned in Article 4 of the Regulation (EC) 1049/2001, which have to be appropriately interpreted and applied.

The reasoning for denying access must establish a link between the relevant exception(s) and the specific content of the document(s) concerned, and show that disclosure would result in a reasonably foreseeable risk to an interest protected by the relevant exceptions.

In the event of partial disclosure, the parts of the document which are covered by the exceptions must be redacted permanently before disclosing it to the applicant. The reply shall inform the applicant of the available remedies.

In case where ENISA finds that no or only very limited public access can be granted, it shall try and address the access request by providing information instead. as it facilitates a requester's understanding of the institution's decision and the formulation of a request for review, if necessary. For this reason, the Agency shall aim to provide a list of the documents that it identifies while replying to a request for public access to documents under Regulation 1049/2001, unless the very disclosure of a list undermines the interest(s) to be protected.

The exceptions to public right of access provided for in Regulation (EC) No 1049/2001 are applicable for a maximum period of 30 years. The exceptions relating to protection of privacy or commercial interests and the specific provisions on sensitive documents may, however, apply beyond that period, if necessary.

In all cases, the reply to the applicant shall be signed by the Head of EDO and sent from the dedicated functional mailbox.

5.2.5 Retention period and data protection

Administrative retention period (ARP), as specified in ENISA Specific Retention List ⁷, for access to documents applications is 5 years.

Personal data processing in PAD requests is detailed under the relevant data protection record⁸.

ANNEX 1

ARES WORKFLOW FOR PAD REQUESTS

STEP	ARES ROLE	ACTOR	INSTRUCTIONS
1	RED	PAD request coordinator or Compliance Officer	1. Launches e-signatory. 2. Uploads the draft reply and supporting documents.
2	CONTRIB	Compliance Officer (if not involved in the step 1) [optional]	Reviews the response provided by the PAD request coordinator.
3	CONTRIB	Delegated staff member [optional]	1. Provides necessary input for the draft uploaded by PAD request coordinator. 2. Uploads any additional supporting documentation if needed.
4	VISA	Line Manager [optional]	Verifies and approves the reply.
5	VISA	Head of Compliance	Verifies content of draft reply.
6	VISA	Data Protection Officer (where applicable)	Verifies data protection compliance.
7	RED	PAD request coordinator	1. Checks the editorial correctness of the draft reply. 2. Inserts the request's ARES registration number and the signature date. 3. Links the reply with the registered request.
8	SIGN	Head of EDO	Checks and validates the reply. Signs the ARES workflow.
9	EXP	PAD request coordinator	1. Registers and send. 2. Files document.

⁷ ANNEX 2 – ENISA Specific Retention List of the [2023-01 ENISA Document Management Policy+annexes.pdf](#)

⁸ [Appeals management and access to documents requests](#).