

## **Council of Europe Access Info Group (AIG)**

### **Compilation of NGOs replies to questions of the Access Info Group**

*Note: this document contains the information submitted by the Parties in response to the questions of the AIG which were agreed at its tenth meeting (AIG(2025)10)*

## **Table of Contents**

HUNGARY – TRANSPARENCY INTERNATIONAL.....	3
HUNGARY – K-MONITOR .....	4
NORWAY - NORSK PRESSFORBUND.....	10
SLOVENIA - TRANSPARENCY INTERNATIONAL SLOVENIA .....	13
SPAIN - ACCESS INFO AEFP .....	18
SWEDEN - TRANSPARENCY INTERNATIONAL SWEDEN.....	24
SWEDEN - SWEDISH UNION OF JOURNALISTS.....	29

## HUNGARY – TRANSPARENCY INTERNATIONAL

We regularly refer to the Tromso convention, particularly to article 5(2). You may need some background here. Hungary has a seemingly robust legal framework on access to info, but the government keeps on adopting provisions to curtail the accessibility of public interest information. Moreover, public bodies and users of public assets, both of whom should normally disclose or at least make accessible public interest information in their possession, often malignantly deny access. Therefore access to info cases regularly land in court rooms.

Among other typical tactics / legal references used by state agencies to obstruct access, one finds denial of existence of document or denial of possession of document, and in all but one of TI-HU's more than 100 FOI cases, the agency concerned never defines who is in possession of the document thought. This is to say that Art 5(2) of Tromso does not go into practice in Hungary.

Coming closer to your questions regarding archives, management of documents, etc. in one of the FOI litigations TI-HU won in court, the government's defence was based on denial of existence of the document thought by reference to deletion of the document. This was the single case for TI-HU to build arguments on a government agency's document management by-law. The government agency concerned was the Foreign Ministry and the ministry denied to have archived e-mails received from the Hungarian Embassy to Koala Lumpur about procurement of ventilators during Covid. Although it was clear based on the by-law that the Foreign Ministry ought to have archived the e-mail concerned, this was not the practice. Although we won in court, we could not enforce the judgement, because the Foreign Ministry successfully defended itself by citing deletion of the document.

I copy the link of an assessment of Hungary's (lacking) delivery on the RoL milestones:

[https://transparency.hu/wp-content/uploads/2025/12/HU\\_EU\\_funds\\_assessment\\_2025.pdf](https://transparency.hu/wp-content/uploads/2025/12/HU_EU_funds_assessment_2025.pdf)

[https://transparency.hu/wp-content/uploads/2025/12/HU\\_EU\\_funds\\_assessment\\_2025\\_table.pdf](https://transparency.hu/wp-content/uploads/2025/12/HU_EU_funds_assessment_2025_table.pdf)

# HUNGARY – K-MONITOR

Dear Sir/Madam,

K-Monitor Association, in response to the letter of the Secretariat received on 14 November 2025, hereby submits its answers as follows:

**1. How is management, preservation and archiving of documents by public authorities regulated? Please provide an official translation of the relevant regulations in one of the Council of Europe languages (English or French).**

The management, preservation, and archiving of documents by public authorities are regulated in Hungary by

- Act LXVI of 1995 on Public Records, Public Archives, and the Protection of Private Archival Materials (hereinafter referred to as the Act),<sup>1</sup>
- Government Decree No. 335/2005 (XII. 29.) on the General Requirements for Records Management by Bodies Performing Public Functions (hereinafter referred to as the Decree),<sup>2</sup> and
- the internal regulations issued by the individual authorities based on Section 10 of the Act.

No official translations of these regulations have been issued.<sup>3</sup>

**2. Are all documents held by a public authority registered? If so, what information about the documents is put on the register? Who is responsible for the registration? At which point does registration take place?**

Section 3 of the Act defines that ‘record’ (“*irat*”) means any information or set of data, recorded in any system of signs and on any medium, generated or received by a body in the course of its operations or by an individual in the course of their activities, which is to be treated as a single unit (subsection c); a ‘public record’ (“*közirat*”) means any record, irrespective of the time of its creation or place of storage, that belongs or belonged to the archival holdings of a body performing public functions (subsection d).

Pursuant to Section 9(1)(a) of the Act, a body performing public functions is obliged to register, at the time of their receipt or creation, all records received by it or prepared by it which contain *data of substantive relevance* to the body’s operations or its scope of functions.

Pursuant to Section 9(1)(h) of the Act, the register of public records shall include, as metadata, all information necessary to identify the record— including the name, address, and contact details of the sender or addressee— as well as any personal data essential for determining the subject matter of the record.

Section 9(3) of the Act provides that the head of a body performing public functions shall be responsible for ensuring compliance with the requirements set out in paragraph (1), for establishing and operating a records repository suitable for the professional and secure preservation of records, for providing the necessary material, technical, and personnel conditions for records management, and for the use of records management software possessing the appropriate certification.

<sup>1</sup> See the Ministry of Justice’s official legal database: <https://njt.hu/jogszabaly/1995-66-00-00>

<sup>2</sup> See the Ministry of Justice’s official legal database: <https://njt.hu/jogszabaly/2005-335-20-22>

<sup>3</sup> See the Ministry of Justice’s official legal database for translated legislations: <https://njt.hu/translations>

**Are there any exceptions applied to the requirements for registration of documents based on their content?**

Yes.

Section 9(1)(a) of the Act obliges the registration of records that contain *data of substantive relevance* to the body's operations or its scope of functions.

Pursuant to Section 61(2) of the Decree, any *superfluous copies, duplicates*, and working materials that do not contain *data of substantive relevance* must be removed from the file and destroyed in accordance with the procedures set out in the records management regulations, without undergoing the disposal procedure.

The *data of substantive relevance* is not defined by law.

**3. Are there some instructions or policies in place as regards registration of correspondence sent directly to/from a public official?**

Pursuant to Section 34(1) of the Decree, all incoming correspondence must be registered at the time of receipt, but no later than the first working day following its arrival. The procedures governing the registration of incoming correspondence, the handling of returned acknowledgments of receipt and electronic confirmations, and the manner of documenting such registration are determined by the records management regulations of the body performing public functions.

Paragraph (2) provides that the incoming correspondence register shall contain, at a minimum, the following information: (a) the name of the sender;

(b) the date and time of receipt;

(c) in the case of registered postal items, the postal identifier of the correspondence (in particular, the code or registration number);

(d) in the case of electronic correspondence, the identifier assigned to the item by the delivery service; and

(e) the registration identifier assigned by the body performing public functions, either a sequential number combined with the year or a registration identifier allocated from a closed, pre-registered number range.

**4. Are the registers of official documents public?**

No.

Pursuant to Section 67/C(1)(b) of the Act, the person conducting an inspection is entitled, for the purposes of effectively carrying out the inspection, to access the records management registers.

No further information is available on this matter.

**5. Are electronic messages (emails, sms messages, etc) treated in the same way as physical documents?**

Yes.

Pursuant to Section 2(30) of the Decree, a 'correspondence item' means a paper-based document or object, as well as *an electronic document—excluding advertising materials, press publications, and electronic spam*—that has been addressed for the purpose of delivery, either on its envelope, on an accompanying list, or in any other manner clearly and unambiguously linked to the document or object.

The law does not provide specific rules on emails, sms messages.

**6. Do public authorities use a common system for registering documents, or does each public authority use its own system for registration?**

Section 38/A of the Decree defines the so-called *Unified Government Records Management System*, which is to be used by the bodies listed in Annex 1 (e.g. ministries, the police, central bodies of the public administration).

Other bodies may decide on the use of their own system. However, pursuant to Section 9(2) of the Act, in the case of electronic records management, a body performing public functions may use only such records management software as complies with the requirements set out in a separate legislation and possesses the requisite certification.

**7. What criteria do public authorities apply for storing official documents? For example, in what format and where documents are stored?**

There is no general requirement to convert all paper-based records into electronic form. However, pursuant to Section 5(4) of the Act, the paper version of a *public record of administrative value* may be destroyed once an electronic copy has been made.

**8. What criteria do public authorities apply for the retention of documents and what retention periods are applied?**

There is no general rule governing the retention of documents.

Pursuant to Section 11(1) of the Regulation, for each record series, it must be determined which records may not be disposed of and which records may be disposed of after a specified period. In the case of non-disposable records, it must also be indicated which records are to be transferred to the archive after a specified period and which records are to be retained locally by the record creator without a specified time limit. For records that are non-disposable and to be transferred to the archive, as well as for disposable records, the period of archival retention must be specified. The retention and disposal periods for records containing personal data must be determined in accordance with the requirement of purpose-limited data processing.

**9. What criteria do public authorities apply for transferring documents to archives?**

Section 12(1) of the Act provides that complete and closed volumes of public records that may not be disposed of shall be transferred to the competent public archive by the end of the fifteenth year following the calendar year of their creation.

For further details, see the responses provided to the following question.

**10. What criteria do public authorities apply for eliminating/destroying documents?**

The legislation distinguishes between *disposable records* and *non-disposable records*. *Records of permanent value* and *records of administrative value* may not be disposed of.

Pursuant to Section 3(j) of the Act, a document is considered to *be of permanent value* and therefore may not be disposed of if it contains information of significance from economic, social, political, legal, defense, national security, scientific, cultural, technical, or other perspectives, which is indispensable for the study, understanding, and knowledge of historical events, the continuous performance of public duties, and the exercise of citizens' rights, and which cannot be obtained or can only be partially obtained from other sources.

Such documents must be transferred to the archive.

Section 3(w) of the Act provides that a *record of administrative value* is a record containing information necessary for natural or legal persons to carry out their ongoing tasks, to comply with statutory obligations, to exercise or secure their rights, or to safeguard vital personal or legitimate interests.

Pursuant to Section 9(1)(f) of the Act, a body performing public functions is obliged to dispose of the disposable portion of its records, after the expiration of the retention period specified in the archival schedule or upon the cessation of their administrative value, with the authorization of the competent public archive.

Pursuant to Section 11(1) of the Decree, for each record series, it must be determined which records may not be disposed of and which records may be disposed of after a specified period. In the case of non-disposable records, it must also be indicated which records are to be transferred to the archive after a specified period and which records are to be retained locally by the record creator without a specified time limit. For records that are non-disposable and to be transferred to the archive, as well as for disposable records, the period of archival retention must be specified. The retention and disposal periods for records containing personal data must be determined in accordance with the requirement of purpose-limited data processing.

**11. Please describe case-law and/or practice which exist as regards document management and preservation (from courts, ombudsmen, information commissioners, etc).**

The freedom of information case law is dominated by cases in which public bodies claim they would never possess the requested information. Only in very few cases do public bodies acknowledge that they previously held the information but have since destroyed it.

The following section presents the relevant case law that has come to the attention of K-Monitor in recent years.

*Disclosure of fax traffic data*

An individual sought access to the fax traffic data of a notary. Notaries perform public functions by law in Hungary. The courts dismissed the case, holding that the mere number of faxes received by a public authority's fax machine during a given period does not convey information regarding its operation, organizational structure, or effectiveness, but is simply a numerical value. Accordingly, there is no provision requiring notaries to record or maintain such data. On their own, these numerical data do not serve the legislative purpose of ensuring transparency in public affairs.

Alkotmánybíróság (Constitutional Court): 3364/2025. (XI. 12.) AB végzés<sup>4</sup> Fővárosi Törvényszék (second instance): 48.Pf.633.757/2024/5.  
Pesti Központi Kerületi Bíróság (first instance): 14.P.88.409/2023/14.

*The Hungarian Government's COVID-19 procurements*

Transparency International Hungary (TI-HU) requested information from the Ministry of Foreign Affairs and Trade concerning the procurement of ventilators during the COVID-19 pandemic in 2020–2021. The Ministry disclosed part of the requested data; however, with

<sup>4</sup> Case number: IV/00542/2025

<https://alkotmanybirosag.hu/ugyadatlap/?id=5F0DF264934CDA79C1258C6F005BFA60>

regard to the declarations on the transparent ownership structure of the companies contracting with the Government, it claimed that those documents required by law had been destroyed. TI-HU successfully sued the ministry.

Case numbers:

Kúria (extraordinary review before the highest court) Pfv.21340/2022/5. Fővárosi Ítéltábla (second instance) Pf.20462/2022/7. Fővárosi Törvényszék (first instance) P.22319/2021/22.

#### *COVID-19 infection statistics*

A journalist requested the COVID-19 statistics from the National Directorate General of Hospitals, which the public authority refused to disclose. The Deputy Director-General testified in court, stating that the requested data had been deleted. The court did not accept this claim, as the Directorate had failed to provide any internal regulations regarding the management, archiving, or destruction of the data, and thus did not substantiate the fact or manner of their destruction.

Case numbers: Kúria (extraordinary review before the highest court) Pfv.IV.20.670/2022/5.

Fővárosi Ítéltábla (second instance) 2.Pf.20.004/2022/4.

Fővárosi Törvényszék (first instance) 27.P.21.285/2021/24.

#### *Minutes and annexes of Cabinet meetings in 2009*

In 2022, the Prime Minister's Government Office (a ministry) refused to disclose to K-Monitor the minutes and annexes of the Cabinet meetings held in 2009. K-Monitor won the case in 2023; however, the Government Office released only the minutes and not the annexes. As regards the annexes, it claimed that they no longer existed, without providing any further justification. K-Monitor requested the enforcement of the judgment, which the court granted. The Government Office then brought an action against K-Monitor, seeking the termination of the enforcement proceedings. The court dismissed the claim. Enforcement is still pending, but the bailiff has taken no steps to date.<sup>5</sup>

Case numbers:

Kúria (extraordinary review before the highest court) Pfv.IV.20.112/2023/5. Fővárosi Ítéltábla (second instance) 2.Pf.20.564/2022/4.

Fővárosi Törvényszék (first instance) 21.P.20.723/2022/8-II.

Enforcement proceedings:

Fővárosi Törvényszék (second instance) 45.Pf.634.152/2024/6.

Budai Központi Kerületi Bíróság (first instance) 12.G.40.135/2024/17.

#### *Press briefings of Minister Szijjártó*

In 2023, the online news portal 444 requested information from the Ministry of Foreign Affairs and Trade concerning which editorial offices had been invited to press briefings involving Minister Péter Szijjártó held at the Ministry and in Brussels in 2023, and which journalists had participated after email registration. The Ministry claimed that the invitations to the press briefings held in 2023 had already been deleted. The news outlet won the ensuing litigation, as the court found that the Ministry had failed to prove that the emails had in fact been deleted. One of the main issues in the proceedings was how long

<sup>5</sup> Summary on K-Monitor's blog (in Hungarian):

[https://k.blog.hu/2025/06/01/kormanyulesek\\_nyilvanossaga\\_pert\\_nyertunk\\_a\\_kormany\\_ellen\\_ami\\_miatt\\_vegul\\_i\\_ogsz\\_abalyt\\_modositottak\\_e](https://k.blog.hu/2025/06/01/kormanyulesek_nyilvanossaga_pert_nyertunk_a_kormany_ellen_ami_miatt_vegul_i_ogsz_abalyt_modositottak_e)

the emails sent by the Ministry were required to be retained. Following the judgment, the Ministry did not disclose the requested data. The editorial office therefore sought enforcement of the judgment, which the court ordered. The Ministry subsequently brought an action against the outlet seeking the termination of the enforcement proceedings; the court dismissed the claim. Enforcement proceedings are currently pending.<sup>6</sup>

Case numbers: Kúria (extraordinary review before the highest court) Pfv.IV.21.243/2024/5.

Fővárosi Ítéltábla (second instance) 9.Pf.20.179/2024/5. Fővárosi Törvényszék (first instance) 39.P.20.135/2024/7.

---

### **Further observations**

K-Monitor submits that the case law concerning the applicability of the Convention in Hungary is inconsistent.

The report submitted by Hungary to the Secretariat pursuant to Article 14, paragraph 1 of the Convention (CETS No.205) has not indicated the lack of applicability.<sup>7</sup>

Certain court decisions have applied the Convention (Fővárosi Ítéltábla, 2.Pf.20.647/2022/8), while others have held that the Convention is not directly applicable (Kúria Pfv.20.275/2024/4., Fővárosi Ítéltábla, 2.Pf.20.386/2025/5).

The National Authority for Data Protection and Freedom of Information, in case no. NAIH-10502-6/2025, stated that “the Tromsø Convention is not directly applicable in Hungary,” and, accordingly, certain requirements of the Convention have not yet been transposed into the national freedom of information legislation, Act No. CXII of 2011.<sup>8</sup>

K-Monitor is of the view that, following its entry into force in December 2020, the Tromsø Convention is directly applicable in Hungary, having been transposed to the domestic law by ratifying Act No. CXXXI of 2009.<sup>9</sup> Therefore, no further legislative step is necessary to enforce the Convention.

In its letter of 24 November 2025, K-Monitor conveyed this position to the Authority and requested its opinion; however, the Authority has not provided a response.

I hope that this submission will be of assistance in your work and that you will also give due consideration to the further observations provided.

Kind regards,



Sándor Léderer  
K-Monitor  
Director

---

<sup>6</sup> 444's report on the case (in Hungarian): <https://444.hu/2024/10/03/pert-vesztett-a-kulugyminiszterium-igy-kozelebb-kerultunk-annak-bemutatasahoz-hogyan-e-rtelmezi-a-sajtoszabadsagot-szijjarto-peter>

<sup>7</sup> Document reference: AIG/Inf(2022)10REV <https://www.coe.int/en/web/access-to-official-documents/hungary>

<sup>8</sup> See the Ministry of Justice's official legal database for translated legislations: <https://njt.hu/jogszabaly/en/2011-112-00-00>

<sup>9</sup> See the Ministry of Justice's official legal database: <https://njt.hu/jogszabaly/2009-131-00-00>

# NORWAY - NORSK PRESSFORBUND

## **Input to the Council of Europe Access Info Group: Document Management and Preservation in Norway**

The Norwegian Press Association (NP) is an umbrella organization for free, editorcontrolled media that adhere to the Code of Ethics for the Press (Vær Varsom-plakaten) and the Editor's Code (Redaktørplakaten). This includes most media outlets in Norway.

NP's mission is to safeguard and defend freedom of expression and press freedom, in order to strengthen the free press as one of the most important institutions in a democratic society.

Our main tasks are to:

- Promote ethical standards in editor-controlled media.
- Strengthen and protect freedom of expression, press freedom, and freedom of information.

The Norwegian Press Association (NP) appreciates the opportunity to provide analysis and experience regarding the management and preservation of official documents in Norway.

We assume that the Council of Europe Access Info Group already possesses a comprehensive overview of the relevant legal frameworks and regulations currently in place. Therefore, our input will focus on how these laws and regulations function in practice, highlighting the professional experiences of the media in accessing official records.

### **Regulation and practice**

In Norway, there is a broad consensus that documents and information constituting part of the public administration's case processing must be archived and made available for public access. The legal framework—including the new Archive Act—are designed to ensure these democratic rights. However, from the perspective of the Norwegian Press Association (NP), the primary challenge lies in how these regulations are practiced.

Despite the sound intentions of the legislation, there is a gap between legal requirements and daily practice. Oversight reports from the Office of the Auditor General (called Riksrevisjonen, [Dokument 3:3, 2021-2022](#)) and the Archive Agency (Arkivverkets tilsynsrapporter for 2024, referred to in this article, in [september 2025](#)) describe the situation as "strongly critical," citing hundreds of legal violations and a systemic lack of control over journaling and accessibility. This practical failure, often characterized by fragmented routines and the inadequate capture of electronic correspondence, frequently renders the statutory right of access illusory for the press and the public.

### **Regulatory framework and the shift to "functional" vagueness**

On January 1, 2026, a new Archive Act and accompanying regulations entered into force in Norway. In this regard, the press organizations (Norwegian Press Association (NP), the Association of Norwegian Editors (NR), and the Norwegian Union of Journalists (NJ) expressed deep concern that this transition represents a shift toward a "vague" and "functional" regulatory model. By moving central archival principles from primary law into regulations, individual public agencies are granted excessive discretion. We are afraid this will create a "fragmented and unpredictable practice" where the preservation of the democratic record depends on the whims of specific agencies rather than uniform national standards.

### **The "Illusory" Right of Access and Missing Metadata**

A cornerstone of the Norwegian right to information is the public journal (*postjournal*). However, current regulations maintain that the registration of internal documents is largely voluntary. The press organizations contend that this makes the right of access "illusory," as the public and the press cannot request documents they are never made aware of. Furthermore, we see a systemic failure to include case officers' names in journals, which prevents the identification of decision-makers and potential conflicts of interest.

### **Content-based exceptions: From "relevance" to "necessity"**

A primary point of contention is the new "necessity" requirement for archiving documentation. Documentation is now only archived if it is "necessary to show if the body has solved its tasks in a responsible and accountable manner". The press organizations fear this restrictive language—which contradicts the legislative intent of "relevance" expressed in preparatory works—risks a total lack of documentation for the deliberations leading to major public decisions.

### **Electronic correspondence (SMS and Messaging Apps)**

Legally, electronic messages are equivalent to physical documents. In practice, this equivalence is a failure. Sivilombudet (Parliamentary Ombudsman) has clarified that each individual message in a thread or chat log must be considered a distinct "document" under the law and shall therefore be archived ([case 2025/6149](#))

Current practice frequently involves archiving entire chat logs as a single screenshot or a merged PDF. This is a direct violation of "[Arkivforskriften](#)" § 10, which requires that registration must "make it possible to identify the document." Single-file archiving of entire threads fails to capture individual metadata—such as specific timestamps and sender/receiver data for every entry—thereby destroying the traceability required for legal and historical accountability.

There is a profound disconnect between official policy and the practical archiving of correspondence via SMS and messaging apps like Signal and WhatsApp. Agencies frequently claim they lack "systems to register" these messages when they reside on a minister's or a case officers phone.

This was the case in Sivilombudets case (2025/6149). The Ministry of Foreign Affairs failed to journalize message exchanges between the Foreign Minister and the EU's High Representative, wrongly claiming they had no system for such registration. The Ombudsman ruled that the Ministry took an incorrect legal starting point and that their routines were unfit to ensure legal journaling requirements (paragraph 56).

### **Lack of Transparency in Documentation Plans**

Despite their importance for understanding how data is managed, "Documentation Plans" remain largely inaccessible to the public. The press organizations have advocated that these plans must be made public to ensure the media and others can determine what documentation might be missing or how retention schedules are being applied.

### **Artificial Intelligence (AI) and the "Analog Logic"**

While the public sector increasingly uses AI in decision-making, the current regulations are largely silent on this development. The press organizations believe the regulations must explicitly address AI-generated documentation to ensure it is archived and accessible for review. We have proposed that AI should instead be used to automate archiving, such as generating daily logs of all relevant communications for officials to review. The current regulations contain little that can ensure archiving of this type of data.

### Case-Law and reports

Some investigations and reports from oversight bodies highlight challenges regarding the practical implementation of regulations for archiving and documenting official records in Norway:

- **The Office of the Auditor General (“Riksrevisjonen”)**: Has rated the situation as "strongly critical," stating that poor archiving undermines democratic control ([Dokument 3:3, 2021-2022](#))
- **«Arkivlovutvalget» (The Archives Act committee)** assumed that we today experience a significant loss of archives due to an unfortunate interplay between the journaling rules, the Archives Act, and the Freedom of Information Act. ([NOU 2019: 9](#), kap. 14 og kap. 16 punkt 16.3.3. og 16.4.1)
- **The Norwegian Commission for Freedom of Expression** ([NOU 2022: 9](#)), highlights the disconnect between Norway’s legal transparency ideals and the actual administrative culture within the public sector in [chapter 11.4.7.](#)

The commission writes that while the legal framework is intended to ensure access, oversight bodies like the Parliamentary Ombudsman (*Sivilombudet*) and the Office of the Auditor General (*Riksrevisjonen*) have documented a systemic "friction" against granting access, where requests are frequently stalled or delayed for months.

This practice effectively "hollows out" the principle of public access, particularly in controversial cases where documentation might be withheld until decisions are already finalized. Furthermore, digital transformation has led to a documented loss of "archive-worthy" records; for instance, during the COVID-19 pandemic, key decision-making data in the form of SMS and emails went unrecorded or were deleted. The commission refers to the report from the **Coronavirus Commission**, chapter 3.3.3 ([NOU 2021: 6 Myndighetenes håndtering av koronapandemien/ The Authorities' Handling of the Coronavirus Pandemic](#))

The commission also writes that current practices suffer from "meaningless" document titles in public journals, which makes it nearly impossible for the press to identify and request relevant records, ultimately undermining the media’s ability to perform its democratic watchdog function.

An [English summary of the report](#) is available here.

The Norwegian Press Association (NP) would like to thank the Access Info Group for the opportunity to provide this input and for granting an extension to the submission deadline.

We remain at your disposal for any further clarifications or additional contributions should you require them in your ongoing work to strengthen the infrastructure of freedom of expression.

Sincerely,

On behalf of the Norwegian Press Association

Kristine Foss  
Legal advisor

# SLOVENIA - TRANSPARENCY INTERNATIONAL SLOVENIA

**Contact:** Peter Malenšek, Secretary General  
Transparency International Slovenia  
Ljubljana, Slovenia  
E: peter.malensek@transparency.si | T: +386 70 678 876

## 1. Purpose and scope

These comments are submitted by Transparency International Slovenia (TI Slovenia) in response to the AIG questionnaire on document management and preservation (Article 9(c) and 9(d) of the Council of Europe Convention on Access to Official Documents – the Tromsø Convention). The submission focuses on Slovenia’s legal and institutional framework and highlights practical risks and areas where implementation could be strengthened.

The observations below are based on publicly available legal texts and guidance, together with TI Slovenia’s general experience with access-to-information practice. They are not intended to be exhaustive, and we would welcome the opportunity to provide additional examples or clarifications if helpful to the AIG.

## 2. Key observations and risk areas (summary)

- Slovenia has a detailed legal framework on documenting, registering, storing and preserving official records, particularly through the Decree on Administrative Operations (Uredba o upravnem poslovanju) and the Protection of Documents and Archives and Archival Institutions Act (ZVDAGA).
- The Decree establishes a clear duty to document work and register documentary material promptly, and it applies equally to electronic and physical records.
- A key practical risk for effective access to information is incomplete capture of modern communications (e.g., emails that are not formally filed, messaging applications, or use of private accounts for official business).
- Registers of documentary material serve primarily as internal administrative tools; proactive public access to register metadata is limited, which can make it difficult for requesters to know what exists and to formulate precise requests.
- Given the AIG’s interpretation that registration may be evidence of ‘held’ documents but is not a condition for the Convention’s scope, strengthened recordkeeping and audit trails remain essential to prevent ‘off-record’ decision-making.

## 3. Responses to the questionnaire

### 1. How is the management, preservation and archiving of official documents regulated in Slovenia? Please provide an official translation of relevant regulations in English or French.

- Document management in state administration and local self-government is primarily regulated by the Decree on Administrative Operations (Uredba o upravnem poslovanju), which sets duties on documenting work, registering documentary material, managing records in an electronic register, and operational requirements for the document/records management information system.
- Preservation, appraisal, transfer to archives and destruction of documents and archives are regulated by the Protection of Documents and Archives and Archival

Institutions Act (ZVDAGA) and its implementing regulations and technical requirements for electronic records.

- Access-to-information rules (which create strong incentives for robust recordkeeping) are regulated by the Access to Public Information Act (ZDIJZ).
- Available English translations: (i) ZVDAGA English version (unofficial consolidated text) published by the Archives of the Republic of Slovenia; (ii) ZDIJZ English translation published by the Information Commissioner (informative/non-authentic). An official English/French translation of the Decree on Administrative Operations has not been identified by TI Slovenia; the authentic text is published in Slovene in the Official Gazette.

**2. Are all documents held by the relevant public authorities registered? If yes, which information is recorded in registers of official documents, who is responsible for their management, and at what point are documents registered?**

- Under the Decree on Administrative Operations, public authorities must document their work and record it in the 'evidence of documentary material' (evidenca dokumentarnega gradiva). The evidence is described as the fundamental record of an authority's work, and it covers documentary material received or created by the authority.
- The Decree requires that work be organized so that documentary material is recorded without delay, and that documents are registered within a case and forwarded for handling the same day (or at the latest the next working day).
- Key metadata recorded for each document includes at least: document number; document date; receipt/dispatch date; classification sign; subject; short description; whether incoming/outgoing/internal; description of annexes; security classification/markings; and deadline.
- Operational responsibility lies with the authority's main registry office (glavna pisarna) for intake/registration and with the assigned case-handler for ensuring proper filing of documents within the case.

**3. Are exceptions applied to the requirement for registration, based on the content of documents? If so, which documents are excepted and why?**

- The Decree distinguishes 'non-registered material' (neevidenčno gradivo) typically mail that is not important for the authority's operations (e.g., advertisements, greetings, invitations, newspapers). Such material is defined in advance by the head of the authority.
- If the authority takes any action in relation to such material, it must be registered.
- In addition, registration under the Decree is not mandatory for documentary material where registration is regulated by specific sectoral rules (special legislation).
- Confidentiality/classification generally affects access controls rather than whether the document is registered; the Decree foresees recording classification markings as part of the registered metadata.

**4. Is there any guidance, policy or instructions in place for correspondence sent directly to and from a public official, i.e. not through any central registry office? Please describe them.**

- The Decree contains rules for mail addressed for personal delivery to a named public official (e.g., 'personal'). Such mail is not opened by registry staff; however, if it contains documents that should be registered, the addressee must ensure prompt registration.
- For electronic correspondence, the Decree's requirements on electronic operations and the functional requirements for the documentary register information system include connectivity with officials' email mailboxes and the possibility of registering selected email messages in the system.

- A remaining risk area (requiring robust internal policies and controls) concerns official business conducted via private accounts or messaging applications, which may not be automatically captured unless authorities implement explicit internal rules and technical solutions.

**5. Are registers of official documents public? If so, are exceptions applied? Please describe the reasons for which registers might not be made public.**

- The documentary register ('evidence of documentary material') functions primarily as an internal administrative record. There is no general obligation in the Decree on Administrative Operations to proactively publish the register or provide open public access to it.
- Under access-to-information rules (ZDIJZ), registers/metadata may in principle be requested as information held by an authority, but disclosure may be limited by lawful exceptions (e.g., personal data protection, classified information, ongoing procedures, etc.).
- In practice, requesters usually rely on proactive publication obligations (catalogues of public information) and on targeted access requests rather than open access to comprehensive register metadata.

**6. Are electronic messages treated in the same way as physical documents with regard to registration? If yes, which types of electronic messages are concerned? If no, what are the reasons?**

- The Decree explicitly applies to documentary material regardless of whether it is in electronic or physical form, and it defines 'documents' broadly to include records in electronic form.
- The Decree provides for receipt of mail in electronic form, including direct receipt into the documentary register information system, and specifies that electronic mail is not printed for registration purposes.
- The information system for managing the documentary register is expected to support linking with officials' email boxes and registering selected email messages. This indicates that email correspondence relevant to an authority's work is intended to be treated as documentary material.
- A practical gap can arise where communications occur through channels not integrated into the system (e.g., messaging apps), requiring organizational policies to ensure capture into the official record.

**7. Is there a common registration system for all relevant public authorities, or does each public authority operate its own register?**

- Each authority is responsible for maintaining its own 'evidence of documentary material'. The Decree allows internal organizational units to keep separate registers for justified reasons, and it also allows registry office functions to be unified for several authorities while keeping separate registers for each authority.
- The Decree defines the 'information system for managing the documentary register' as a set of information systems necessary for maintaining the register, which suggests that different technical implementations can be used provided they meet required functionalities.

**8. What are the criteria for storing official documents? Please describe what form and where official documents are stored.**

- The Decree requires that the documentary register ensures storage of the documents themselves, their metadata, and the audit trail of actions performed on documents.

- Physical documents are, as a rule, scanned into the register; exceptions may be set for very voluminous materials based on a decision of the head of the authority.
- The information system must support secure storage (including of annexes and electronically signed documents) and separation between active ('unresolved'), current and permanent collections.
- For long-term preservation and archiving (especially for electronic records), ZVDAGA and implementing technical requirements apply, focusing on authenticity, integrity, reliability and usability over time.

**9. What are the criteria for retaining official documents, and for how long are they retained? Please describe what criteria are used for determining retention periods.**

- Retention periods are determined through classification plans and retention schedules, taking into account legal requirements, evidentiary value, administrative value and archival value. Materials of archival value are preserved permanently.
- The Decree requires that the documentary register information system supports, among other things, automatic calculation of retention periods and the recording of document destruction.
- ZVDAGA provides the overarching framework for appraisal and determination of archival material, and it sets rules to ensure that archival material is not destroyed.

**10. What are the criteria for transferring documents to archives, and after what period are documents transferred?**

- Archival transfer is governed by ZVDAGA and implementing regulations. In general terms, documents that have been appraised as archival material are transferred to the competent public archives after they are no longer needed for current administrative operations and after expiry of the applicable retention periods, following appraisal and transfer procedures.
- For electronic records, transfer is typically subject to additional technical and procedural requirements to ensure long-term preservation and accessibility.

**11. What are the criteria for eliminating/destroying official documents, and after what period are documents eliminated/destroyed? Are there safeguards (for example, procedures in place) to ensure that documents are not destroyed prematurely?**

- Elimination/destruction is governed by retention schedules and the rules of ZVDAGA. Destruction is permitted only after expiry of retention periods and subject to safeguards ensuring that documents with archival value are preserved.
- The Decree's documentary register system is expected to support recording of destruction ('registered destruction') as part of the audit trail and governance of documentary material.
- Effective safeguards rely on a combination of (i) clear retention schedules; (ii) internal authorization procedures; (iii) oversight by archival authorities; and (iv) technical controls/audit trails in electronic systems.

**12. Please describe case-law and/or practice regarding document management and preservation. Relevant examples might include cases brought before courts, ombudsmen, or information commissioners.**

- Information Commissioner practice confirms the importance of the 'materialized form' criterion: where a body concludes that the requested information does not exist, it must refuse access (rather than create new information). This underscores the anti-corruption relevance of robust recordkeeping to ensure accountability.

- The AIG has stressed that registration in an authority's document management/archiving system can be evidence that a document is 'held', but registration cannot be treated as a condition for the Convention's scope. This reinforces the need for authorities to ensure that records of decision-making are actually created and preserved, including communications that influence decisions.
- TI Slovenia's general observation is that access-to-information effectiveness is closely linked to consistent capture and preservation of records across all communication channels, and that strengthening audit trails and document management controls is therefore a practical governance priority.

#### 4. Suggested measures to strengthen practice (optional)

- Adopt/strengthen binding internal rules to ensure that all official business conducted by public officials through email, messaging applications or other channels is captured into the documentary register, with clear responsibilities and timelines.
- Increase transparency of register metadata (at least at aggregate level) to make it easier for requesters to identify existing records (while protecting personal data and legitimate confidential interests).
- Ensure consistent implementation across central government, local government and entities exercising public authority, including adequate resourcing of registry functions and periodic training.
- Strengthen audit mechanisms (internal audit, supervisory inspections, archival oversight) focusing on completeness of records, retention compliance and prevention of premature destruction.

#### Annex – Key legal sources and available English translations

- Decree on Administrative Operations (Uredba o upravnem poslovanju), Official Gazette of the Republic of Slovenia, No. 9/2018 (authentic text in Slovene): [https://www.uradni-list.si/\\_pdf/2018/Ur/u2018009.pdf](https://www.uradni-list.si/_pdf/2018/Ur/u2018009.pdf)
- Protection of Documents and Archives and Archival Institutions Act (ZVDAGA) – English version (unofficial consolidated text, for information): [https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Angleska-stran/Zakonodaja/ZVDAGA\\_2014\\_English.pdf](https://www.gov.si/assets/organi-v-sestavi/Arhiv-RS/Angleska-stran/Zakonodaja/ZVDAGA_2014_English.pdf)
- Access to Public Information Act (ZDIJZ) – English translation (for information): <https://www.ip-rs.si/en/legislation/access-to-public-information-act/>
- Information Commissioner guidance on situations where requested information does not exist (materialized form criterion): <https://www.ip-rs.si/informacije-javnega-zna%C4%8Daja/ijz-pri-organih/kako-odlo%C4%8Diti-o-zahtevi>

# SPAIN - ACCESS INFO AEFP

## I. Introduction

In the context of this contribution to the thematic report of the Council of Europe, we would like to emphasise that the right of access to information should be recognised as a fundamental right in the Spanish legal framework. The current Spanish Law on Transparency, Access to Information and Good Governance (Law 19/2013) links access to information to Article 105 b.) of the Spanish Constitution regarding citizens' access to administrative archives and records. **We continue to call for the right of access to information to be linked to Article 20.1.d) of the Spanish Constitution, which provides for the constitutional right to freedom of expression.**

**Regarding public archives, these are considered essential elements in a democratic society, guarantors of rights and obligations, indispensable supports for administrative transparency and irreplaceable testimonial sources of collective memory.** For this reason, we understand them not only as places for the custody of old documents of recognised testimonial value, mainly used as sources for historical studies, but also as **administrative services responsible for managing the processing of public documents from the moment they are generated until their destruction or selection for indefinite preservation.**

**The legal relationships, duties and rights of citizens under state, regional or local legislation and regulations, as well as the procedures for control and support by each of these administrations of the activities of private individuals and legal entities, must be documented, safeguarded and guaranteed at all times by state, regional and local bodies.**

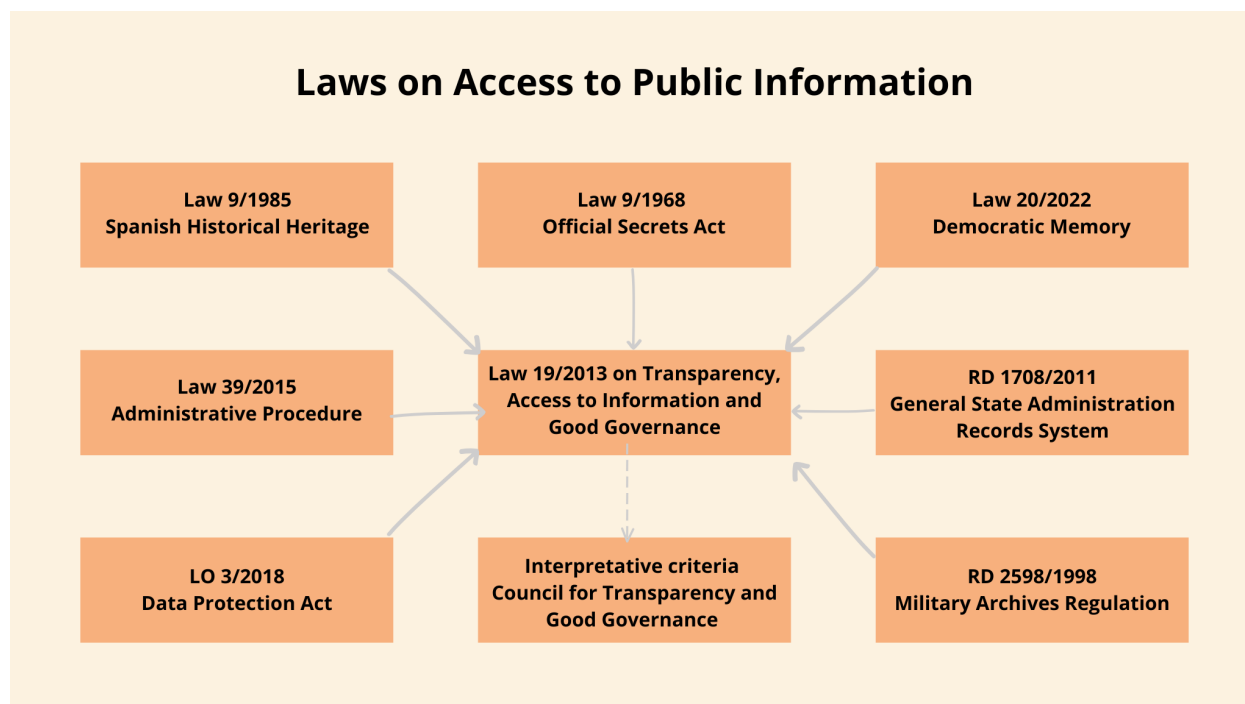
**Consequently, their archives must be managed efficiently and securely, so that the rights of individuals or entities that have established a legal relationship with any of the three levels of government can be exercised and enforced at all times, and access to the documents recording the validity of such rights must always be possible and expeditious, without prejudice to the fundamental legal rights protected by the Constitution (security, prosecution of crimes, honour and privacy).**

**The incorporation of the Tromsø Convention into Spanish law is good news, as it will allow its provisions to be included in existing legislation, which is rather lengthy and sometimes contradictory. Another question is how this should be done, so that it is truly effective in improving the right of access to public information in Spain, under these circumstances.**

**The problem we face in Spain is the lack of unified and comprehensive legislation on document and archive management, including in the digital environment.**

## II. Management of access to public information

Taking into consideration the purpose of this consultation, and the real possibilities for developing points c) and d) of Article 9 of the Tromsø Convention on the management, accessibility and preservation of public documents generated and managed by public administrations, the answer would be "**by complying with current legislation**". But current legislation is a complex web of laws, which can be summarised in the following diagram:



**Despite being a state law, the original shortcomings of the 2013 Law on Transparency, Access to Information and Good Governance, make it a subsidiary or residual norm, placing it in a regulatory category inferior to other norms with the status of Organic Law, especially those relating to the Protection of Personal Data or the Right to Honour.** With the same regulatory status, there are provisions regulating the right of access to public information in the Administrative Procedure Act, the Spanish Historical Heritage Act, the Official Secrets Act and the Democratic Memory Act. The regulations governing the General State Administration Archive System and the access procedure have regulatory status, but do not include those of the Ministries of Justice and Defence, which have their own regulations. In addition, the way in which all these regulations should be applied is defined by Interpretative Criterion 2/2015 of the Transparency and Good Governance Council regarding the application of the limits established in Articles 14 and 15 of the 2013 Law on Transparency, Access to Information and Good Governance.

On the other hand, **current legislation continues to contain an inexplicable diversity of procedures for accessing public information depending on the physical location of the information and its processing status:**

- Kept in an office archive: Law 19/2013
- Kept in a central archive: Royal Decree 1708/2011, Law 16/1985
- Kept in an intermediate archive: Royal Decree 1708/2011, Law 16/1985
- Kept in a historical archive: Royal Decree 1708/2011 (sixth additional provision 2), Law 16/1985

It should be noted that **an Open Administration Law is currently in the draft stage**, which will presumably replace both the current Transparency Law and the Spanish Historical Heritage Law (only the part corresponding to access to information). In principle, **it seems that now there is a possibility of unifying the procedure of access to public information regardless of where it is located, including measures related to document and archive management**. However, it only includes the current Additional Provision 7 and Final Provision 1, presenting pros and cons.

- The **First Additional Provision explicitly repeals the current content of Article 57 of the Spanish Historical Heritage Law, which contained the "golden rule" of access to public information with specially protected personal data, applying a period of 25 years from the death of the deceased or 50 years from the completion of the file containing the data**. This rule has been widely applied and, on too many occasions, interpreted differently depending on each archive, and has even been moderated or nuanced through the Democratic Memory Act in specific cases, which certainly needed a complete overhaul.
- **The problem is that the proposed alternative wording** refers to generic regulations and to the Open Administration Act itself, which regulates this matter in Article 21 in a way that **is too lax and will cause** even more complex **interpretation problems** than those posed by the original wording. In fact, this has been the thrust of the arguments presented by the AEFPP in the public hearing and information process on the draft bill. We propose adding as a criterion "the differentiated and superior public interest in access to documents relating to the coup d'état, the war and the dictatorship and all other sets of documents that may be necessary for the clarification of facts linked to crimes against humanity", already regulated in Law 20/2022 on Democratic Memory, as this provision would lapse if approved in this way. [APLAA Amendments - Google Documents](#)

### **III. Document and archive management**

The main problem in **the case of document management is the scarcity of regulations and the absence of a common policy across the entire General State Administration for the management of electronic documents** and the implementation of electronic document management systems.

In **the absence of a general archives law, reference must be made to the Spanish Historical Heritage Law and Royal Decree 1708/2011, which regulates the Spanish archives system and the General State Administration**. The **absence of the term "document management" in both cases is striking**; only in the first paragraph of Royal Decree 1708/2011 is this concept mentioned, without further elaboration. It was not until the ministerial restructuring of 2024 that the functions of the Ministry of Culture included "the coordination of the document management system of the General State Administration, with an emphasis on the management of electronic document heritage, in order to implement policies and procedures that allow for the control of the creation, reception, transmission, maintenance and access to public information, facilitate decision-making by administrative bodies and guarantee the rights of citizens".

On the contrary, the regulations governing the functioning of public administrations do contemplate document management since the development of **the National Interoperability Scheme** in 2010 (Royal Decree 4/2010) and its **technical interoperability standards**, which establish the requirements that public documentation must meet to be legally valid and interoperable (authentic, complete, etc.) and even the obligation to have an institutional

**electronic document management policy.** With the approval of **Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations**, the obligation to process documents electronically and the **requirements for administrative electronic documents to be considered valid** were established: use of formats that can be identified and treated differently; identification data that allow them to be individualised; a time reference indicating when they were issued; **minimum required metadata** and corresponding electronic signatures (art. 26).

Regarding the **preservation and disposal of public documentation**, Law 16/1985 of 25 June on Spanish Historical Heritage is extremely protective, establishing:

- protection of **all public documentation** considered **part of the Spanish Historical Heritage from the moment of its creation** (Art. 49.2, 52.1):
- basic prevention against the **uncontrolled disposal of documents** (Art. 55), which is considered an administrative offence (Art. 76.1.j) regardless of any criminal liability that may be incurred;
- an **administrative authorisation regime for disposal**, developed by Royal Decree 1164/2002 of 8 November, *which regulates the preservation of documentary heritage of historical value, the control of the disposal of other documents of the General State Administration and its public bodies, and the preservation of administrative documents in formats other than the original.*

In implementation of this law, Royal Decree 1401/2007 of 29 October created the **Higher Commission for the Classification of Administrative Documents for the General State Administration**, whose purpose is to study and issue opinions on the periods of retention or transfer, accessibility and use, and disposal of documents or document series. And in Royal Decree 1708/2011, of 18 November, *which establishes the Spanish Archival System and regulates the Archival System of the General State Administration and its Public Bodies and their access regime*, the functions to be performed by the different types of archives, the classification commissions and the departmental archive coordination working groups in the General State Administration system were established.

This administrative regime of administrative authorisation for disposal has been included in the implementing regulations of Law 39/2015, **Royal Decree 203/2021, of 30 March, approving the Regulations on the operation and functioning of the public sector by electronic means**. Three articles are devoted to this issue:

- Article 53 establishes **regulated destruction in accordance with the deadlines set out in the official retention schedules, which reflect the rulings of the Higher Commission for the Classification of Administrative Documents.**
- Article 54 expressly establishes that public administrations "**must preserve in electronic format all documents that form part of an administrative file and all documents with probative value created outside of an administrative procedure**" and must do so "**in a manner that allows access to them and includes, at a minimum, their identification, content, metadata, signature, structure and format.**"
- Article 55 provides that **all electronic documents and files of the state public sector shall be accessible in the single electronic archive of the General State Administration once the procedures have been completed and within the time limits determined by the Higher Commission for the Classification of Administrative Documents** in accordance with the regulations. Furthermore, "**the management of the single electronic archive shall guarantee the authenticity, preservation, integrity, confidentiality, availability and chain of custody of the files and documents stored, as well as access to them.**"

Despite this regulatory development and the good work of the Higher Commission for the Classification of Administrative Documents for the General State Administration, which has enabled the approval of multiple specific retention schedules for each type of public documentation (document series), **the implementation of electronic processing without proper management of electronic documents is preventing the preservation of the documentation currently being generated.** The loss of electronic documents in public administrations is immeasurable, with documentation scattered and uncontrolled in network folders and obsolete applications, or even deleted to free up space. In most cases, valid electronic files are not being generated, with a lack of training among public employees who are unaware that an electronically signed PDF without metadata is not a valid administrative document.

**The result is that public documentation is not being entered into the single electronic archive, as it does not meet the validity requirements, and the administrations do not have document management systems that allow automated entry into the electronic archive.**

#### **IV. New developments in 2025**

Throughout 2025, there were **several initiatives promoting greater awareness of the importance of document management.** For example, the inclusion of several **commitments that would influence the implementation of proper document management in public administrations, particularly in the General State Administration, in the V Open Government Plan:**

- **Commitment 2 - Transparency and access to information, to strengthen the legal and strategic framework: Open Administration Act** (Ministry of Digital Transformation and Public Administration), reform of the Official Secrets Act (Ministry of the Presidency, Relations with the Courts and Justice) and the **Archives Act** (Ministry of Culture), which aims to update and adjust other sectoral regulations and serve as a framework for other provisions of the various public administrations in the field of archives and document management.
- **Commitment 4 - of Open Administration: Document Management System of the General State Administration** (Ministry of Digital Transformation and Good Governance), with the aim of "having a Document Management System or alternative system that allows the establishment within the General State Administration (AGE) of an **Electronic Document Management System (SGDE)** and an **Electronic Archive Document Management System (SGDEA)**, linked to each other and supported by a Register of Procedures. These systems will enable the implementation of a common electronic document management policy throughout the General State Administration, ensuring the traceability, preservation, access and reuse of documents throughout their life cycle." To this end, a regulatory adaptation is planned that "must comply, among other aspects, with the provisions of the Tromsø Convention, which recognises the right of access to public documents and requires that such documents be duly registered to facilitate their accessibility and management in accordance with standardised criteria."
- **Commitment 5 on digital governance and artificial intelligence:** Implementation of a tool for document processing and management (Ministry of Finance).

The Draft for the **Open Administration Bill** also includes a new **final provision 7 that reflects the requirements of sections c) and d) of Article 9 of the Tromsø Convention:**

"Additional provision seven. Information management in the field of the General State Administration.

1. The General State Administration shall take appropriate measures to manage its information effectively, so that it is easily accessible, and shall follow clear and defined procedures for the preservation and destruction of public information in accordance with the provisions of Royal Decree 1164/2002 of 8 November, which regulates the preservation of documentary heritage of historical value, the control of the disposal of other documents of the General State Administration and its public bodies, and the preservation of administrative documents in formats other than the original. "

But most important is the provision in section 2, which states that:

"(...) within the General State Administration, a **comprehensive document management system** must be implemented in which policies and procedures are documented to control the creation, receipt, transmission, maintenance and access to public information, to ensure that it is created and used by authorised and identified persons and that all actions taken in relation to it are recorded, so that it is protected against any unauthorised addition, deletion, modification or concealment." And section 3 states that "Within the scope of the General State Administration, the transparency obligations provided for by current legislation shall be incorporated into the life cycle of documents to **ensure effective access by citizens to public information from the design of the document management system.**"

The difficulty lies in the fact that **the Draft Bill does not specify what "document management system" means, and what material, personal and procedural requirements are necessary for its proper development and to fulfil its purpose**, considering both analogue and digital documentation, with all the requirements established in the National Interoperability and Security Schemes. A document management system requires **technological development**, a policy that establishes the **conceptual and regulatory framework of reference** and defines the processing programme, and **people to implement the policy and processing programme** using the technical tool. At present, **there is no common policy for the management of electronic documents at the level of the General State Administration**, only some ministries have developed their own, nor is there a technical solution that covers the management of electronic documents from their creation, only for the final archiving phase, **nor a team to lead this implementation in a coordinated manner for the entire General State Administration**, as should be promoted by the Ministry of Culture, which finally has this competence included among its functions by the 2024 royal decree on structure.

## **V. Conclusion**

Close attention will be paid to the parliamentary process of the Open Administration Bill and the final drafting, and whether it will be passed or not. We also await a potential new Draft on the General Archives Law.

**Beyond the legal regulations**, we would like to emphasise that, to comply with the points outlined in the Tromsø Convention, it would be essential to act in other organisational and professional areas:

1. **Assigning public archives to the departments responsible for organisation in the various administrations, not exclusively to Culture and Heritage**; in the General State Administration, to the Ministry of Public Service or the Presidency of the

Government, including the interdepartmental assignment of civil service bodies specialising in archives.

2. **Creation of a National Archives Agency, integrating all civil and military archives of a national nature into a single network.**
3. **Provision of staff and material and financial resources** to enable the extension of **public archive** opening hours, extending them from Monday to Saturday in the morning and afternoon.
4. **Development of an Archival Infrastructure Plan** that will lead, among other objectives, to the **decongestion of saturated** paper-based **infrastructures**, such as the National Historical Archive and the General Archive of the Administration, and the **creation of the necessary infrastructures for the management of private documentary collections that may be incorporated into state archives**, including the **facilities and applications necessary to ensure the permanent preservation of electronic documentation as well.**

# SWEDEN - TRANSPARENCY INTERNATIONAL SWEDEN

In Sweden we have the "Offentlighetsprincipen" (Public Access to Information and Secrecy Act), you can find it in English here: <https://www.government.se/information-material/2009/09/public-access-to-information-and-secrecy-act/>. See a short summary of the act below (translated using Microsoft):

---

<https://www.regeringen.se/sa-styrs-sverige/grundlagar-och-demokratiskt-deltagande/offentlighetsprincipen/>

### *The principle of public access to official documents*

The principle of public access to official documents is central to the Swedish legal system. It means that the public, often private individuals and representatives of the media, have the right to insight into and access to information about the activities of the state and municipalities.

The principle of public access to official documents is expressed in various ways in Sweden's constitutions, for example through the right to freedom of expression, the freedom of information for public officials and through the publicity of public documents.

### *What is an official document?*

Documents are anything that contains information of any kind: texts, images, or information stored in some other way, such as in a computer or on a USB stick. A document is public if it is kept by an authority and has been received by or drawn up by the authority. Backup copies are not considered to be public documents, like, for example, memos and draft decisions. Provisions on the right to access public documents are contained in the Freedom of the Press Act.

### *Which public documents are public?*

The main rule is that public documents are public. The right to access public documents can be limited by confidentiality, which means a prohibition to disclose information orally or in any other way. It may be the case that some information in an official document is covered by confidentiality and others are public. Provisions on secrecy are mainly contained in the Public Access to Information and Secrecy Act (2009:400).

---

## **Report by TI Sweden on the Public Access to Information and Secrecy Act**

Transparency International Sweden released a report looking into how the Act works in practice in September 2025 - it is in Swedish but it might be of interest to you. I have translated (using Microsoft) the press release, the background of the report and the results for you. The full report is attached but can also be found here: <https://www.transparency.se/nyheter/offentlighetsprincipen-i-praktiken>.

### **Press release**

*Test of the Public Access to Information and Secrecy Act – 158 public organisations did not meet the requirements*

In connection with the International Day for Universal Access to Information, Transparency International Sweden (TI Sweden) publishes the report "The Public Access to Information and Secrecy Act in Practice". The report examines the extent to which public organisations in

Sweden comply with the requirement of the Public Access to Information and Secrecy Act for prompt processing of requests for public documents.

In the spring of 2025, we asked 612 public organisations, i.e. Swedish authorities, municipalities and regions, to provide a specific document - guidelines for secondary occupations. 575 organizations got back to us, which corresponds to a response rate of 94%.

"Testing whether the Public Access to Information and Secrecy Act works in practice is important to ensure transparency and the public's opportunity for transparency in public activities. It is part of the preventive work against corruption. The high response rate shows that the vast majority of public organizations have satisfactory processes for handling a request for public documents," says Ulrik Åshuvud, Secretary General of Transparency International Sweden.

#### *Good compliance but remaining challenges*

Two-thirds of the organisations surveyed responded within a day, thus complying with the urgency requirement as recommended by the Parliamentary Ombudsmen.

"That a majority of the public organizations responded within a day is fundamental. What is worrying is that 158 organizations (27%) did not live up to the urgency requirement. The fact that 9 percent of the municipalities and 4 percent of the authorities, after reminders, did not respond at all to the inquiry is not acceptable", Ulrik Åshuvud continues.

#### *Organisation size – not a decisive factor*

The differences between large and small organizations were marginal. Among the authorities, there were more small authorities that never returned, but for the municipalities a reverse pattern was found – larger municipalities had a higher proportion of non-responses than smaller ones. This suggests that increasing organizational size does not necessarily lead to better handling of incoming requests.

#### *Lack of transparency when using contact forms*

13 of the surveyed organizations used contact forms instead of e-mail to receive requests for public documents. These organisations had a significantly worse result compared to the total: only 46 per cent met the urgency requirement, and a quarter did not respond at all.

"It is important that organisations do not put up obstacles by, among other things, using contact forms where citizens feel that it is difficult to get in touch and feedback is lacking," Ulrik Åshuvud points out.

#### *Important to review routines on an ongoing basis*

TI Sweden encourages public organisations to actively follow up and evaluate the response rate and response time to incoming requests for public documents to ensure that they meet the urgency requirements of the Public Access to Information and Secrecy Act. Organisations using contact forms should supplement the form with an automatic confirmation with a case number to ensure traceability and transparency.

### **Background (page 1 in the report)**

The Public Access to Information and Secrecy Act is a fundamental pillar of Swedish democracy. Among other things, it guarantees the public's right to access public documents and creates transparency and the opportunity for accountability in the public sector.

A request to access an official document must be processed promptly (Chapter 2, Section 16 of the Parliamentary Ombudsman), which according to the Parliamentary Ombudsman (JO) means that it should be processed within one day.

"The Parliamentary Ombudsman has stated in a number of decisions that a decision on the question of whether a document can be disclosed should normally be given on the same day as the request was made."

To review how the Public Access to Information and Secrecy Act is complied with, Transparency International Sweden (TI Sweden) has surveyed all Swedish municipalities and regions as well as government agencies with at least five employees. By requesting the public organisations' guidelines for secondary occupations, two factors were tested:

- Compliance with the Public Access to Information and Secrecy Act - if we were notified of the requested document
- Compliance with the urgency requirement - we interpreted responses within 24 hours as having met the urgency requirements in accordance with the Parliamentary Ombudsman's recommendation

The request was made through a private email address to mimic contact from an ordinary citizen. The response rate was high, with an average of 94 percent.

### **Results and recommendations (page 7-9)**

- 2/3 of the public organisations responded within 24 hours, which means that a majority meet the urgency requirement according to the Parliamentary Ombudsman's recommendation.
- 158 organizations did not live up to the urgency requirement, while 9% of the municipalities and 4% of the authorities left our request completely unanswered. This raises questions about procedures for handling incoming cases.
- Despite preventive measures to avoid our request being viewed as spam, some of the missed responses can likely be explained by a lack of spam folder control.
- Differences in organization size show no clear correlation with response rate.
- Organizations that use contact forms perform worse than average.
- Among the organisations that met the urgency requirement, the response rate was highest in the first hour after receiving the request.

### *Good compliance but remaining challenges*

TI Sweden's survey of compliance with the Public Access to Information and Secrecy Act among all municipalities and regions as well as authorities with at least five employees shows that a majority comply with both the act and its urgency requirements. Furthermore, a majority of the organisations that submitted a response within the Parliamentary Ombudsman's recommendation responded within half a day. This result is positive and welcome in the work against corruption, as the Public Access to Information and Secrecy Act contributes to increased transparency, enables accountability and strengthens the public's ability to scrutinise the public sector.

Despite the generally good response rate, there are discrepancies that should be noted. 158 organisations (27%) did not respond within the Parliamentary Ombudsman's recommendation of a one-day response time, and 9% of the municipalities and 4% of the authorities did not respond to our request at all, despite being reminded. One possible explanation is that the request was incorrectly classified as spam. However, we do not believe that this explanation is an excuse for organizations to leave requests unanswered, as they should have procedures in place to check incorrectly filtered messages.

### *Organisation size – not a decisive factor*

During the course of the survey, we expected that smaller public organisations would have a worse result compared to larger organisations - with fewer responding within the Parliamentary Ombudsman's recommendation and a lower response rate. The assumption was made taking into account limited human resources and possibly less developed procedures for case management. However, the results showed that the differences between large and small organizations were marginal. Among the authorities, there were more small authorities that never returned, but for the municipalities a reverse pattern was found – larger municipalities had a higher proportion of non-responses than smaller ones. This suggests that increasing organizational size does not necessarily lead to better handling of incoming requests.

*Lack of transparency in the use of contact forms needs to be addressed*

A clear pattern emerges among the organizations that use contact forms instead of e-mail to receive requests for public documents. These organisations had a significantly worse result compared to the total: only 46% met the urgency requirements of the Public Access to Information and Secrecy Act, and 23% did not respond at all. The fact that a significant proportion of these organisations are made up of large authorities with extensive contact with citizens makes this particularly serious.

In all cases where the request was sent via a contact form, we lacked a confirmation with a case number. This makes it difficult to follow up. It is also difficult to know whether the request has been received by the business at all.

This lack of traceability and transparency makes it difficult for the public to communicate with public organizations. We therefore recommend that these organisations review the design of their contact forms and ensure that they enable follow-up and confirmation of received requests.

*Limited generalizability*

It should be emphasized that the requested document in this study – guidelines for outside occupations – is relatively easy to identify and disclose. The results of the survey are therefore not necessarily representative of more complex requests, such as when a confidentiality assessment needs to be made.

***Recommendations***

- Review spam control procedures to catch cases that have been incorrectly filtered out.
- If the organisation uses contact forms, supplement with an automatic confirmation function where the sender receives a case number and contact details for follow-up.
- We encourage public organisations to actively follow up and evaluate the response rate and response time to incoming requests for public documents to ensure that they meet the urgency requirements of the principle of public access to official documents.

# SWEDEN - SWEDISH UNION OF JOURNALISTS

## **1. How is management, preservation and archiving of documents by public authorities regulated?**

The primary legal framework governing document management in the Swedish public sector is the Public Access to Information and Secrecy Act (Offentlighets- och sekretesslagen, 2009:400). This act guarantees the public's right to access official documents and sets out rules on how authorities should handle, store, and preserve these records. In addition, the Archives Act (Arkivlagen, 1990:782) establishes the responsibilities of public authorities regarding the long-term preservation and archiving of documents.

Swedish public authorities are required to register and organise documents systematically. The procedures ensure that records are accessible both internally and to the public, unless exempted by secrecy provisions. Authorities must also implement secure systems for handling both physical and electronic documentation.

## **2. Are all documents held by a public authority registered? If so, what information about the documents is put on the register? Who is responsible for the registration? At which point does registration take place?**

In Sweden, not all documents held by a public authority are necessarily registered. However, according to the Swedish principle of public access to official documents ("offentlighetsprincipen"), public authorities are generally required to register incoming and outgoing official documents that are received or created as part of their official activities. The registration typically includes key details such as the date the document was received or created, the sender or recipient, a brief description or subject of the document, and a reference or registration number assigned to the document. Date and registration number are required by law.

The responsibility for registering documents lies with the public authority that receives or creates the documents. Within the authority, this task is usually handled by the registrars or administrative staff who manage records and archives.

Registration should take place as soon as possible after a document is received or created, in order to ensure transparency and facilitate public access. The aim is to register documents without unnecessary delay.

## **3. Are there any exceptions applied to the requirements for registration of documents based on their content?**

Yes, there are exceptions to the requirement for registration of documents by public authorities in Sweden that are based on the content of the documents. While the majority of official documents are registered to uphold transparency and public access, certain categories of documents are exempt from registration. Notably, drafts, internal working materials, and documents that are deemed preparatory or not finalised are typically excluded from registration.

Additionally, documents that contain sensitive information—such as those related to national security, personal privacy, or classified matters—may be subject to specific handling procedures and may not be registered in the same way as ordinary official documents.

**4. Are there some instructions or policies in place as regards registration of correspondence sent directly to/from a public official?**

Public authorities have established policies and routines for handling such correspondence. These typically require that any official communication—letters, emails, or messages—sent directly to a public official in the course of their duties is to be registered in the authority’s records system. This registration captures key details such as the date received or dispatched, the sender or recipient, the subject matter, and a reference or registration number.

However, exceptions may apply to certain types of correspondence, such as personal messages unrelated to official business, drafts, or internal working materials. In such cases, registration is not required. The distinction between official and private correspondence is important, and guidance on this is usually provided in internal policies or administrative manuals.

**5. Are the registers of official documents public?**

Yes, in Sweden, the registers of official documents maintained by public authorities are generally public. This accessibility is part of the Swedish principle of public access to official documents (“offentlighetsprincipen”), which ensures transparency and enables the public to request information about registered documents.

**6. Are electronic messages (emails, sms messages, etc) treated in the same way as physical documents?**

Yes, in Sweden, electronic messages—such as emails, SMS messages, and other forms of digital correspondence—are generally treated in the same way as physical documents when they are received or created by a public authority as part of its official activities. According to the Swedish principle of public access to official documents (“offentlighetsprincipen”), all documents, regardless of format, that are received or produced by a public authority can be considered official documents.

If an electronic message contains information relevant to the authority's work, it is subject to the same rules regarding registration, archiving, and potential disclosure to the public as a physical document. This ensures transparency and public access, regardless of whether the document is on paper or digital.

**7. Do public authorities use a common system for registering documents, or does each public authority use its own system for registration?**

In Sweden, each public authority is generally responsible for managing its own system of document registration. While the principles and legal requirements for what information must be registered are set out in national laws—such as the Public Access to Information and Secrecy Act (“offentlighets- och sekretesslagen”)—there is no single, unified nationwide system that all authorities are obligated to use. Instead, individual authorities typically implement their own registration systems and procedures, provided these comply with the overarching rules for transparency, registration, and public access.

**8. What criteria do public authorities apply for storing official documents? For example, in what format and where documents are stored?**

Official documents may be stored in various formats, including physical (paper) and digital forms. Increasingly, authorities are transitioning to digital storage solutions, using secure electronic archives and document management systems that support long-term preservation and efficient retrieval.

- 9. What criteria do public authorities apply for the retention of documents and what retention periods are applied?**
- 10. What criteria do public authorities apply for transferring documents to archives?**
- 11. What criteria do public authorities apply for eliminating/destroying documents?**

In Sweden, the preservation and disposal of public records are governed primarily by the Archives Act (1990:782), together with regulations and guidelines issued by the National Archives. The Archives Act establishes the general principle that public records shall be preserved and that disposal (gallring) may take place only when permitted by law or by regulations issued under the Act.

The Public Access to Information and Secrecy Act (2009:400) does not regulate retention periods as such, but instead governs the public's right to access official documents and sets out rules on secrecy and confidentiality, including how long secrecy may apply to certain types of information.

Detailed retention and disposal periods for different categories of records are determined through regulations from the National Archives and through decisions made by each individual authority in its records management or information management plans. In practice, certain types of records, such as accounting material or personnel-related documentation, are often retained for a number of years after their administrative use has ended, in accordance with applicable regulations and established practice.

- 12. Please describe case-law and/or practice which exist as regards document management and preservation (from courts, ombudsmen, information commissioners, etc).**