Manual for the management of document flows of the Alessandro Volta secondary school

Summary

PREMISES

The "Guidelines on the training, management and storage of IT documents", issued by the AgID, provide for the obligation for Public Administrations to draw up a formal provision and publish the Document Management Manual on their institutional website.

This Document Management Manual, adopted by the school [denomination] in order to comply with the above provisions, describes the document management system and provides instructions for the correct functioning of the service for keeping the IT protocol, management of document flows and archives.

In detail, the Manual describes the organizational model adopted by the school for document management and the document life cycle management process, as well as providing specific instructions regarding the administrative document and the IT document, the IT protocol and the access, transparency and privacy.

The Manual is intended for the widest internal and external circulation, as it provides complete instructions for correctly carrying out the operations of formation, registration, classification, collation and archiving of documents. Therefore, this document is addressed not only to protocol operators but, in general, to all employees and external parties who interact with the bodies of the Institute.

GLOSSARY

AGiD Agenzia per l'Italia Digitale (*Agency for Digital Italy*)

HOA Homogeneous Organizational Area

DAC Digital Administration Code (Legislative Decree no. 82/2005 and subsequent amendments)

D.L. Decree-law

L.D. Legislative Decree

PMD Prime Ministerial Decree

PD Presidential Decree

AGSD Administrative and General Services Director

GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27th April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and repealing Directive 95/46 / CE

PAI Public Administrations Index

CE Certified E-mail

OE Ordinary E-mail

DPO Data Protection Officer

HCPT Head of Corruption Prevention and Transparency

RUP Sole Manager of the Procedure

ROU Responsible Organizational Unit

1. THE DOCUMENT MANAGEMENT MANUAL

This manual describes the document production and management system, including for conservation purposes.

In line with the reference regulatory framework, the manual is aimed at regulating the activities of creation, acquisition, registration, classification, assignment, collation and archiving of IT documents, as well as the management of the documentary and archival flows of the school, as well as, albeit in a residual way, the management of non-IT documents. These activities are aimed at the correct identification and availability of documents acquired and created by the school as part of the exercise of its administrative functions.

The manual, therefore, constitutes an operational guide for all those who manage documents within the educational institution, in order to facilitate the proper performance of document management operations.

1.1. METHOD OF APPROVAL AND UPDATE

The Head of Document Management[1] is responsible for preparing the manual, which is adopted with a provision by the Headmaster.

The manual must be periodically updated by carrying out the census of the activities / practices in place, their rationalization, the identification and definition of the organizational and management aspects in terms of phases, times and human resources involved in the automation of document flows in compliance of the legislation.

[1] For further details on this figure, see par. "2.2. - Roles and responsibilities".

Any event likely to affect the operation and effectiveness of the manual itself must be promptly reported to the Head of Document Management, in order to take the appropriate measures regarding any modification and / or integration of the procedure itself.

1.2. FORMS OF ADVERTISING AND DISCLOSURE

In line with the provisions of the "*Guidelines on the training, management and storage of IT documents*"[2] (hereinafter, also "Guidelines"), adopted by the AgID with Resolution no.407/2020 and later updated with Resolution no. 371/2021 (to be implemented by 1st January 2022), or that the manual is made public by publishing it on the institutional website in a clearly identifiable part of the "Transparent Administration" area, provided for by art. 9 of L.D. 33/2013[3], this manual is made available for public consultation by posting it on the institutional website of the school.

2. THE ORGANIZATIONAL MODEL

2.2. HOMOGENEOUS ORGANIZATIONAL AREA

Art. 50, paragraph 4, of the PD 28th December 2000, n. 445 "*Consolidated text of legislative and regulatory provisions on administrative regulation" establishes that "Each Administration identifies, within its own legal system, the offices to be considered for the purposes of the single or coordinated management of documents for large homogeneous organizational areas, ensuring uniform classification and filing, as well as internal communication between the areas themselves* ".

The school identifies within itself a single Homogeneous Organizational Area (HOA), which corresponds to a single protocol register, called (*A827740*).

The HOA can be sub-divided into Responsible Organizational Units (ROU), that is the set of offices which, by type of institutional mandate and competence, administrative function pursued, objectives and activities carried out, present needs for the management of the documentation in a unified and coordinated way.

The articulation of the ROU is shown in the Attachment [*attachment number*].

The above attachment is subject to change. The insertion / cancellation / updating of ROUs must be formalized with a provision signed by the Head of Document Management and implemented in this manual.

2.2. ROLES AND RESPONSIBILITIES

The educational institution, in order to ensure uniform processing of documents, timely application of the provisions and periodic monitoring of the methods of use of document management tools, must include the following figures:

---

[2] Please note that the AgID Guidelines are binding, as specified by the Council of State - in the context of the opinion given on the draft legislative decree of the corrective to Legislative Decree 82/2005 no. 2122/2017 of 10.10.2017. It follows that, in the hierarchy of sources, these Guidelines are also framed as a regulatory act, albeit of a technical nature, with the consequence that they are fully operable before the administrative judge in the event of violation of the provisions contained therein. In the event that the violation is committed by the subjects referred to in art. 2, paragraph 2, of the aforementioned L.D. 82/2005, it is also possible to submit a specific report to the Ombudsman, pursuant to art. 17 of the same Code.

[3] Art. 9, paragraph 1, of the L.D. 33/2013, provides that: "*For the purposes of full accessibility of the information published, a special section called" Transparent Administration "is located on the home page of the institutional sites, which contains the data, information and documents published pursuant to of current legislation. In order to avoid any duplication, the aforementioned publication can be replaced by a hypertext link to the section of the site containing the relevant data, information or documents, ensuring the quality of the information referred to in Article 6. The administrations may not have filters and other technical solutions to prevent web search engines from indexing and searching within the "Transparent administration" section* ".

- the **Head of Document Management** and his vicar[4];
- the **Conservation Manager**;
- the **Head of Corruption Prevention and Transparency**;
- the **Data Protection Officer**, pursuant to art. 37 of EU Regulation 679/2016.

Furthermore, in addition to the figures listed above, the importance of identifying the **Contact Person for the Public Administrations Index** (PAI), subject to which the Headmaster entrusts the task, both organizational and operational, of interacting with the manager of the PAI for the insertion and modification of the data of the school, as well as for any other matter concerning the presence of the same at the PAI[5].

The **Head of Document Management** is the person in possession of suitable professional requirements or technical-archival professionalism, in charge of the service for the maintenance of the IT protocol, the management of document flows and archives, pursuant to art. 61 of the PD 28th December 2000, n. 445, which produces the payment package and transfers its contents to the storage system.

Taking into account the above, the Head of Document Management is identified within the school, in the person of the (*Headmaster*)[6].

The Head of Document Management and his vicar are appointed by a specific provision of the Headmaster.

The **Conservation Manager** is the person in possession of suitable legal, IT and archival skills, who operates in accordance with the provisions of art. 44, paragraph 1-quater, of L.D. 82/2005 (hereinafter also "DAC")[7].

In particular, the Conservation Manager:

a) defines the conservation policies and functional requirements of the conservation system, in compliance with current legislation and taking into account international standards, based on the specificities of the digital objects to be preserved (IT documents, IT aggregations, IT archives), the nature of the activities that the holder of the conservation object carries out and the characteristics of the IT document management system adopted;
b) manages the conservation process and ensures compliance with current legislation over time;
c) generates and signs the payment report, according to the procedures set out in the conservation manual;

---

[4] As defined in the "*Guidelines on training, management and storage of IT documents*" issued by the AgID "*The Public Administrations, within their own system, shall: [...] appoint, in each of the HOAs, the Head of Document Management and one of his vicars, in possession of suitable juridical, IT and archival skills* ".

[5] The "*Guidelines of the Index of digital domiciles of public administrations and managers of public services* (PAI)", adopted by the AgID, in paragraph 2.2, establish that "*The Head of the Body in the accreditation application appoints a PAI Contact which has the task of interacting with the PAI Operator for the insertion and modification of data, as well as for any other matter concerning the presence of the Entity in the PAI*".

[6] It should be noted that, even in the event that the Head of Document Management is identified in a figure other than the Headmaster, some tasks and responsibilities remain with the same Head, in compliance with the provisions contained in art. 4, paragraph 2, and in art. 25 of L.D. 165/2001.

[7] Art. 44, paragraph 1-quater, of the DAC provides that: "*The conservation manager, who works in agreement with the security manager and the information systems manager, may entrust, pursuant to article 34, paragraph 1-bis, letter b), the conservation of IT documents to other subjects, public or private, who offer suitable organizational, technological and personal data protection guarantees. The person in charge of the conservation of the public administration, who works in agreement, as well as with the managers referred to in paragraph 1-bis, also with the person in charge of document management, carries out the conservation of the IT documents in accordance with the provisions of Article 34, paragraph 1-bis* ".

d) generates and signs the distribution package with a digital signature or a qualified electronic signature, in the cases provided for in the conservation manual;
e) monitors the correct functionality of the storage system;
f) carries out periodic checks, with a frequency not exceeding five years, of the integrity and legibility of IT documents and documentary aggregations of the archives;
g) in order to guarantee the conservation and access to IT documents, it adopts measures to promptly detect any degradation of the storage systems and recordings and, where necessary, to restore correct functionality, adopts similar measures with regard to format obsolescence;
h) provides for the duplication or copy of IT documents in relation to the evolution of the technological context, in accordance with the provisions of the conservation manual;
i) prepares the necessary measures for the physical and logical security of the conservation system;
j) ensures the presence of a public official, in cases where his intervention is required, guaranteeing him the assistance and resources necessary for carrying out the activities assigned to him;
k) ensures the competent bodies provided for by the regulations in force the assistance and resources necessary for carrying out the verification and supervisory activities;
l) provides for the central and peripheral state administrations to pay the IT documents, the IT aggregations and the IT archives, as well as the tools that guarantee their consultation, respectively to the Central State Archives and the territorially competent State Archives, according to the deadlines set by art. 41, paragraph 1, of the Code of cultural heritage[8];
m) prepares the conservation manual and takes care of its periodic updating in the presence of significant regulatory, organizational, procedural or technological changes.

In the event that the conservation service is entrusted to a conservator, the aforementioned activities or some of them, with the exception of letter m), may be entrusted to the person in charge of the conservation service, it being understood in any case that the general legal responsibility conservation processes cannot be delegated, it remains the responsibility of the Conservation Manager, who is also called to carry out the necessary verification and control activities in compliance with the regulations in force on services outsourced by Public Administrations.

The role of the Conservation Manager can be played by the Head of Document Management or also by other figures. Taking into account the above, the Conservation Manager is identified, within the school, in the person of the (*Headmaster*).

The Conservation Manager is appointed by a specific decree of the Headmaster.

The **Head of Corruption Prevention and Transparency** (HCPT) is the person to whom the request for civic access can be presented, if the same concerns data, information or documents subject to mandatory publication pursuant to L.D. 33/2013[9].

The HCPT, in addition to reporting cases of non-fulfillment or partial fulfillment of the obligations regarding publication provided for by current legislation, deals with requests for review of applicants who have been totally or partially denied generalized civic access, or who do not have received no response within the established deadline (see, for more details, what is specified in paragraph 6.2.2).

[8] Art. 41, paragraph 1, of the Cultural Heritage Code provides that: "*The judicial and administrative bodies of the State shall send to the central State archives and to the State archives the documents relating to business which have been exhausted for over thirty years, together with the instruments which guarantee consultation. The draft and drawing lists are paid seventy years after the year of birth of the class to which they refer. The notarial archives pay the notarial deeds received from notaries who ceased their professional practice before the last hundred years* ".
[9] Art. 5, paragraph 3, lett. d), L.D. 33/2013.

The **Data Protection Officer** (DPO) is the person appointed by a specific decree of the Headmaster, who has the task of monitoring compliance with the legislation on the protection of personal data, i.e. the EU Regulation 679/2016 (hereinafter, also "GDPR") and L.D. 196/2003 (hereinafter, also "Privacy Code"), as amended by Legislative Decree 101/2018.

The Data Protection Officer must be involved in all matters concerning the management and protection of personal data and has the task of both informing and making school staff aware of the obligations deriving from the aforementioned legislation and collaborating with the Data Controller and the Data Processor, where necessary, in carrying out the impact assessment on data protection[10].

On this point, the "*Guidelines on data protection officers*", adopted by WP29 on 13th December 2016, amended on 5th April 2017, specify that "*Ensuring the timely and immediate involvement of the DPO, through his information and consultation right from the initials, will facilitate compliance with the RGPD and promote the application of the principle of privacy (and data protection) right from the design stage; therefore, this should represent the standard approach within the structure of the data controller / manager. In addition, it is important that the DPO is counted among the interlocutors within the aforementioned structure, and that he participates in the working groups that each time deal with the processing activities* ".

As regards the methods by which the Data Protection Officer interfaces with the Document Management Officer and with the Conservation Manager regarding the adoption of the security measures of the IT document management system, please refer to what described in detail in paragraph 6.1.

2.3. ORGANIZATIONAL MODEL ADOPTED

[*In the case of adoption of a centralized system*]

The registration system is unique for the school and a "centralized" system is adopted, whereby all communications are managed, both incoming and outgoing, by a single UOR that takes care of their registration. In detail:

- **incoming communications**, regardless of the type of communication (via certified e-mail, OE or paper format) arrive at the single access point, where they are recorded in the protocol and sorted in the various ROUs according to the competence;
- **outgoing communications** are transmitted to a single ROU, which takes care of their registration and their sending.

The ROUs and the persons authorized for the receipt, assignment, consultation, registration, classification and archiving of documents are identified by the Head of Document Management through internal organizational documents.

---

[10] The person in charge of data protection is governed by Recital n. 97 and by art. 37 - 39 of EU Regulation 679/2016, as well as the Guidelines on data protection officers, already referred to in the text (*http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/ docweb / 5930287*).
This figure has the task of: assessing the risks of each treatment; collaborating with the Data Controller / Data Processor, where necessary, in conducting an impact assessment on data protection; informing and sensitising the Data Controller or Data Processor, as well as the employees of the latter, about the obligations deriving from the Regulation and other provisions on data protection; cooperating with the Guarantor and act as a contact point for the Guarantor on any matter related to the treatment; supporting the Data Controller or the Manager in any activity related to the processing of personal data, also with regard to keeping a register of processing activities. The Data Protection Officer is identified among the subjects in possession of specific requirements, professional skills and specialist knowledge in the field of data protection, in line with the functions that he is called to perform and that he must be able to fulfil in full independence and in the absence of conflicts of interest.

2.4. E-MAIL BOXES

The school is equipped with an institutional Certified Electronic Mailbox (CE) for the management of the service for keeping the IT protocol, the management of document flows and archives. The certified email address is published in the index of public administrations.

The box above constitutes the virtual address of the HOA's registered office. The school is also equipped with an institutional ordinary electronic mail box (OE), useful for managing e-mail messages with attached documents and any attachments, having administrative relevance.

In addition, the school uses internal ordinary e-mail boxes ("service") to be entrusted to the management of a ROU or a single operator[11].

The binding provisions relating to the terms and methods of use of CEs and OEs are published on the institutional website of the educational institution.

3. THE LIFE CYCLE OF THE DOCUMENT

The life cycle of the document is divided into the production, management and conservation processes:

- the document **production process** consists mainly in the acquisition of paper, computer and / or telematic documents or in the creation of the same;
- the **management process** involves all activities starting from the registration of the document, to the classification, assignment and current collation / archiving;
- the **conservation process** takes the form of the transfer of documents from the current archive to the storage archive (from which they can possibly follow the discarding and relocation activities) and from the storage archive to the historical archive.

The following paragraphs provide an overview of the processes divided by:

- production and management process;
- conservation process.

3.1. PRODUCTION AND MANAGEMENT PROCESS

The production and management process provides a summary of the activities to be implemented with reference to both the production of the document and the management phases of the same. The production process is divided into "Production Process - Acquisition" and "Production Process - Creation", in order to respectively distinguish the activities relating to incoming documents from those relating to documents processed by the school.

With reference to document management, details of the following phases are provided: classification, collation, archiving.

3.1.1. PRODUCTION AND MANAGEMENT PROCESS - ACQUISITION

The "Production and management process - Acquisition" is described by differentiating the case in which the input is a paper document from the case in which it is computerized, given that the documents coming from outside can be of a paper or computer nature.

In the case of an **incoming paper document**, in the acquisition phase, the receiving school:

[11] Pursuant to the Directive of 27 November 2003 of the Minister for Innovation and Technologies, "*It therefore appears necessary that public administrations provide all employees with an e-mail box (even those for which the provision of a personal computer) and to activate, in addition, special institutional boxes entrusted to the responsibility of the competent structures.*"

- issues a stamped receipt, should the document be delivered by hand[12];
- verifies the competence of the document itself.

In the case of documents received by mistake at the school but addressed to other subjects, the document:

- it is returned by post;
- if the envelope that contains it is opened by mistake, it is logged in and out, by inserting the note "Document received by mistake" in the subject field and in the classification field, and it is returned to the sender by adding the words "Received and opened by mistake ".

If the document is the responsibility of the receiving educational institution, the registration phase follows in which the operator responsible for registration:

- evaluates whether the document is to be registered (see par. "4.8. - Protocol of a document");
- in the event that the document is to be registered, proceeds with the scan and subsequent verification of compliance with the original of the computer copy (see par. "5.10. - Methods of carrying out the scanning process ");
- verifies the presence of special categories of personal data, referred to in Article 9 of EU Regulation 679/2016, for the purpose of implementing the security measures provided for in paragraph 6.1;
- arranges for the classification of the document on the basis of the classification holder;
- provides for the registration of the document upon entry;
- affixes the stamp containing the data contained in the protocol signature through the specific functionality of the IT protocol service or, only in case of impossibility, proceeds manually.

In the assignment phase, the protocol operator assigns the document to the competent staff according to the following assignment methods and rules [*procedures and allocation rules*]. The Head of document management, or the vicar, can, in any case, rectify the assignee of the document.

After the registration, classification and assignment phases, it is necessary to proceed with the document collation / archiving phase.

[*In the case of hybrid storage*]

For paper documents, hybrid storage is provided, in which both the original analog document and the computer copy are stored. Therefore, the Head of the management:

- inserts the paper document in a new file or in an existing file within the current paper archive;
- inserts the IT document in a new file or in an existing file within the current electronic archive.

[*In the case of replacement conservation*]

For paper documents, substitutive storage is provided, with which the legal validity of an electronic document is guaranteed over time, understood as a representation of acts or facts and data on a support, be it analog or computer. Therefore, the Head of the management:

[12] As a rule, the protocol service does not issue receipts for documents that are not subject to regular registration. The simple affixing of the date stamp on the copy has no legal value and does not entail any responsibility of the administrative staff of the school regarding the receipt and assignment of the document.

- certifies the compliance of the IT document with the paper document, pursuant to art. 22, paragraph 2, of the DAC;
- can destroy the paper document;
- inserts the IT document in a new file or in an existing file within the current electronic archive.

It should be noted that the documents listed by the PMD of 21st March 2013[13] cannot be destroyed, for which the obligation to keep the paperwork remains even in the case of replacement storage.

[*In both cases (hybrid storage and substitute storage)*]

For these activities, the Head of Management may have a specific delegation to the assignee or to other personnel specifically identified.

In the case of an **incoming IT document**, in the acquisition phase, the receiving school verifies the competence of the document.

In the case of documents received erroneously on the CE or OE box of the school, the protocol operator sends the message back to the sender with the words "Message received by mistake - not the responsibility of this Administration". In addition, if the document has been incorrectly registered, the protocol officer cancels the registration, according to the procedures described in this manual, or logs the outgoing document indicating as object "Registered by mistake".

If the document is the responsibility of the receiving school, the registration phase follows in which the protocol operator:

- evaluates whether the document is to be registered (see par. "4.8. - Protocol of a document");
- if the document is to be registered, proceeds to verify the validity of the signature (if present)[14];
- verifies the presence of special categories of personal data, referred to in Article 9 of EU Regulation 679/2016, for the purpose of implementing the security measures referred to in paragraph 6.1;
- arranges for the classification of the document on the basis of the classification holder[15];
- provides for incoming registration.

---

[13] The Annex to the Prime Ministerial Decree of 21st March 2013 concerning "*Identification of particular types of unique original analogue documents for which, due to publicistic needs, the obligation to preserve the analogue original remains or, in case of conservation substitute, their conformity with the original must be authenticated by a notary or other public official authorized to do so with a declaration digitally signed and attached to the electronic document, pursuant to art. 22, paragraph 5, of the Digital Administration Code, referred to in Legislative Decree 7 March 2005, n. 82 and subsequent amendments*", lists the following among the unique original analogue documents for which the conservation of the original paper remains mandatory:
a) acts contained in the Official Collection of the legislative acts of the Republic;
b) judicial, procedural and judicial police acts for the following twenty years;
c) works of art;
d) documents of historical and artistic value, including those in the possession of the armed forces;
e) documents, including historical - state-owned ones, kept in state archives, libraries and discotheques, including acts and documents kept in the historical library of the former Experience Studies Center of the Central Directorate for Prevention and Technical Safety of the Department of V.V.F., public rescue and civil defense;
f) notarial deeds;
g) deeds kept by notaries pursuant to law no. 89, before their delivery to the notarial archives;
h) deeds kept in the notarial archives.

[14] For further information, see chap. "4. - The administrative document ".

[15] In the event of doubts regarding the title holder item to be attributed to the document, the protocol operator discusses the correct classification with the manager of document management.

In the assignment phase, the protocol operator assigns the document to the competent staff. The Head of Document Management can, in any case, rectify the assignee of the document.

If the legal system provides, for particular categories of electronic documents, obligations relating to the use of specific file formats or additional restrictions on generic formats, the educational institutions, fulfilling these obligations, accept the aforementioned electronic documents only if produced in formats or with mandatory additional constraints.

With digital preservation, the current collation / archiving phase is carried out in which the appropriately enabled users insert the IT document either in a new file or in an existing file within the current electronic archive.

3.1.2. PRODUCTION AND MANAGEMENT PROCESS - CREATION

In the "Production and management process - Creation", only the IT document is considered as input to the process (see par. "4.6. - IT document").

In the creation phase, the document:

- is drawn up by the competent staff and sent to the Headmaster or other responsible staff (e.g., AGSD) for the revision of the same, or it is drawn up by the Headmaster himself;
- is subsequently approved either by the Headmaster or by other responsible personnel on the basis of their competence.

In the elaboration and revision phase, it is possible to circulate the document among the interested parties by registering it as a "draft".

The computer documents produced, regardless of the software used for their creation, before their digital signature, are converted into one of the standard formats required by current legislation[16], in order to ensure their non-alterability during the access and storage phases and the immutability of the content and structure over time.

It is possible to use formats other than those listed in Annex 2 "*File formats and dump*" of the Guidelines, by carrying out an interoperability assessment, carried out on the basis of the indications provided in the same Annex[17].

The formats used by the school, according to the interoperability assessment, are: PDF, XML and TIFF.

In the registration phase, the protocol operator provides:

- to verify the presence of particular categories of personal data, referred to in Article 9 of EU Regulation 679/2016;
- to the classification of the document on the basis of the classification title[18];
- to the protocol registration.

In the current collation / archiving phase, the protocol operator inserts the IT document into an already existing file or, in the event that the file is not present, creates it or requests its creation from the appropriately enabled user.

---

[16] Annex 2 to the "*Guidelines on the training, management and storage of IT documents*" issued by the AgID.

[17] The assessment of interoperability, as part of the IT management of documents, is carried out periodically and, in any case, every year, in order to promptly identify changes in the conditions expressed by the points listed above. The document management manual contains the list of formats used and the interoperability assessment.

[18] In the event of doubts regarding the title holder item to be attributed to the document, the protocol operator discusses the correct classification with the manager of document management.

After the collation / archiving phase, the document can be subject to a new assignment or publication.

3.1.3. MANAGEMENT PROCESS - CLASSIFICATION

Classification is the mandatory operation that allows you to organize documents, according to a logical order, in relation to the functions and skills of the educational institution. It is performed starting from the classification holder.

The holder, referred to in Annex [*1*], is the set of logical items hierarchically structured and divided into divisional degrees (title / class / possible subclass), established on the basis of the functions of the Administration.

It is defined by a specific decree of the Headmaster and is unique at the level of the school.

All documents received and produced by the educational institution, regardless of the medium on which they are trained, are classified according to the classification holder; through this operation, in addition to the complete code of the classification index (title, class and any subclass), the document is also assigned the repertory number of the file. The aforementioned operation is mandatory when registering the protocol, but subsequent changes can be made.

The necessary and fundamental classification is prodromal to the insertion of a document within a given file.

3.1.4. MANAGEMENT PROCESS - SORT

Collation is the activity of logical reconnection (and, in the case of paper documents, also physical) of a document within the archival unit that collects the previous ones, in order to keep alive the archival bond that binds each individual document to its practice.

Each document, after its classification, is included in the reference file. The documents are archived within each file or, if necessary, sub-file, according to the chronological order of registration.

The dossiers are organized by[19]:

- **deal**, which includes documents relating to a non-procedural competence, but which, in administrative practice, the educational institution must concretely bring to fruition. The deal file has an opening date and a limited duration. In fact, it is closed when the deal is closed;
- **activity**, which includes documents produced in carrying out a simple administrative activity that implies obligatory responses or mere obligations, for which therefore the adoption of a final provision is not envisaged. It generally lasts one year;
- **natural person**, which includes all documents, even with different classifications, which refer to a natural person. The files in the name of individuals are almost always current for many years;
- **legal person**, which includes all documents, even with different classifications, which refer to a legal person. The files in the name of individuals are almost always current for many years;
- **administrative procedure**, within which a plurality of documents are stored which represent homogeneous administrative actions and are destined to end with an administrative measure. The file is closed at the end of the administrative procedure[20].

[19] Annex 5 to the "*Guidelines on the training, management and storage of IT documents*" issued by the AgID.

[20] In accordance with art. 41, paragraph 2, of the DAC, "*The public administration in charge of the procedure collects in an electronic file the deeds, documents and data of the procedure itself trained by anyone;* [...] ".

Within the files it is possible to create sub-files.

Each office is responsible for managing the practices of its own competence. If a document gives rise to the initiation of a new procedure, the person in charge opens a new file. In order to determine the type of document aggregation (type of series and type of dossiers) to be adopted, reference is made to the Organizational Plan of document aggregations, shown in Annex [*1*]. A document can also be assigned to multiple sets. The formation of a new dossier takes place through the "**opening**" operation which includes the registration of some essential information. The IT file, in fact, bears the indication[21]:

- the administration responsible for the procedure, which takes care of the constitution and management of the file itself;
- of the other participating administrations;
- the person in charge of the procedure;
- the subject of the procedure;
- the list of contained documents;
- the identification of the dossier itself.

The file is usually opened at the last level of the hierarchical structure of the holder. In some cases, it is also possible to use the first level (title), such as for natural person files.

In the presence of a document to be included in a dossier, the subjects in charge of collating, with the aid of the search functions of the IT protocol system, whether it is part of an ongoing proceeding, or if it initiates a a new procedure:

1. if it is part of an ongoing proceeding:
- select the relevant file;
- link the document protocol registration to the selected file (if it is a paper document, they ensure the physical insertion of the same in the relevant correspondence);
2. if you initiate a new proceeding:
- perform the operation of opening the file referred to in the previous paragraph;
- assign the file on the recommendation of the person in charge of the procedure;
- link the protocol record of the document to the open file.

The file is closed at the end of the procedure. The closing date refers to the date of the last document produced. When an error occurs in the assignment of a dossier, the user authorized for the collation operation corrects the information entered in the computer system and sends the dossier to the relevant ROU. The computerized document management system keeps track of these steps, storing for each of them the identification of the operator making the change with the date and time of the operation.

The issues are noted in the file directory. The file repertoire, divided by each title of the holder, is the management and retrieval tool of the files. The structure of the repertoire mirrors that of the classification holder and therefore varies in conjunction with the updating of the latter. While the holder represents in abstract the functions and skills that the school can exercise on the basis of its institutional mission, the repertory of files represents in practice the activities carried out and the documents produced in relation to these activities. The repertoire shows:

- the opening date;
- the complete classification index (title, class and any subclass);
- the file number (and any other partitions into sub-sets and inserts);
- the closing date;
- the subject of the dossier (and possibly the subject of the sub-dossiers and inserts);

[21] In accordance with art. 41, paragraph 2-ter, of the DAC.

- the annotation on the status of the case to which the file refers (ongoing case to be included in the current archive, closed file to be sent to the deposit archive, closed file to send to the historical archive or to be discarded).

The repertoire of dossiers is constantly updated.

In addition to being included in a dossier, a document can be included in one or more documentary series, which represent aggregations of documents with homogeneous characteristics, grouped for example according to type of document (e.g. resolutions, decrees, invoices) or origin (i.e. if produced by the same body, such as the School Council or the Teaching Body) or the subject matter (e.g. documents relating to a PON project)[22].

The documents within a series, not being aggregated using the classification title as in the case of files, may belong to different titles and classes. The documentary series itself, therefore, is not classified according to the partitions of the holder.

Specific indications on how to insert documents in document aggregations are contained in the Appendix "*Focus on document aggregations of educational institutions*" to the "*Guidelines for document management in educational institutions*".

3.1.5. MANAGEMENT PROCESS - ARCHIVING

The educational institutions define in their manual the management of the archives referring to the following archival structure[23]:

- **current archive**: concerns the documents necessary for current activities;
- **filing archive**: this concerns documents that are still useful for administrative or legal purposes, but are no longer indispensable for dealing with current activities;
- **historical archive**: it concerns the historical documents selected for permanent conservation.

Archiving, for some types of documents, can take place in archives managed centrally by the Ministry of Education. By way of example, the applications received by the school through the Online Instances Service, which allows for the digital submission of applications related to the main administrative procedures of the Administration, are registered at the entrance by the HOA specifically set up at the Ministry of Education, and are made available to educational institutions.

Taking into account that the current archive is organized on an annual basis and that the passage from the current archive to the deposit archive is possible only if the file contains documents relating to concluded proceedings, it is necessary to verify which files contain documents relating to a closed case. This verification can be carried out:

- at the end of each year, so that the files of the cases not closed by the previous December are "dragged" into the current archive of the new year and the files of the closed cases are "dragged" into the deposit archive;

or,

- during the year if the case is closed.

Given that it would be too expensive and almost useless to keep the archive in its entirety indefinitely, it must be periodically subjected to a rational selection, which must be foreseen from

[22] This definition of "document series" is based on paragraph 4 of Annex 5 to the "*Guidelines on the training, management and storage of IT documents*" issued by the AgID.

[23] "*Guidelines on the training, management and storage of IT documents*" issued by the AgID.

the moment the documents are created, and must be regulated in the conservation plan[24] (Annex 2), to in turn integrated with the classification system. To this end, thinning is inserted (activity performed in the current archive).

Thinning is a preparatory activity for correct document conservation: at the time of closing the file, for example, or before its transfer to the archive archive, any correspondence of a transitory and instrumental nature must be selected and extracted from the dossier by the operator in charge of handling the file. In other words, it is a question of extracting from the file the copies and documents that have an instrumental and transitory character, used by the operator in charge or by the person in charge of the procedure, but which exhaust their function when the final provision is issued or are not strictly connected to the procedure (e.g., notes, memos, copies of legislation and documents of a general nature).Within the filing archive, the discarding operation takes place which must not be applied, unless otherwise indicated by the Archival Superintendency, on documentation belonging to the historical archive whose files have been exhausted for over 40 years, while it can always be carried out on the documentation of the filing archive, which contains all the closed files that have not matured for 40 years of conservation.

The lack of space in the archives as well as the excessive production and storage of even useless papers cannot justify the unauthorized destruction of documents or even the cancellation of electronic documents[25], since the discarding of documents from the school archives is subject to the authorization of the Archival Superintendency[26]. The deletion of electronic documents is also a form of waste.

Without prejudice to the above, the discarding operation is supported by the maximum conservation and discarding limit, thanks to which the list of documents and files for which the mandatory retention period has elapsed and which are therefore susceptible to discard is produced annually. The documents selected for permanent storage are filed together with the instruments that guarantee access to them in the State Archive competent for the territory or transferred to the separate archive section, in accordance with the provisions in force on the protection of cultural heritage.

3.2. STORAGE PROCESS

The management cycle of an IT document ends with its payment into a storage system that is consistent with the provisions of the DAC and the "*Guidelines on training, management and storage of IT documents*". The conservation process involves four stages:

- payment to the deposit archive;
- waste;
- payment to the historical archive;
- relocation.

In this context, the person in charge of conservation is inserted, whose tasks have been described in the previous paragraph 2.2.

Pursuant to art. 34, paragraph 1-bis, of the DAC, as amended by art. 25, paragraph 1, lett. e), of the D.L. 76/2020 (so-called "Simplification Decree"), converted with Law no. 120/2020, the Public Administrations can proceed with the conservation of IT documents:

a) within its own organizational structure;

[24] Art. 68, paragraph 1, of Presidential Decree 445/2000.
[25] Art. 169, Legislative Decree 22 January 2004, n. 42 "*Code of cultural heritage and landscape, pursuant to article 10 of the law of 6 July 2002, no. 137* ".
[26] Art. 21, paragraph 1, Legislative Decree 22 January 2004, n. 42 "*Code of cultural heritage and landscape, pursuant to article 10 of the law of 6 July 2002, no. 137*".

b) entrusting it, totally or partially, in compliance with the regulations in force, to other subjects, public or private who possess the quality, safety and organization requirements identified, in compliance with European regulations, in the "*Guidelines on training, management and storage of IT documents*" as well as in a regulation on the criteria for the provision of IT document storage services issued by AgID[27], having regard to the need to ensure compliance of the documents stored with the originals as well as the quality and safety of the storage system .

For the storage of electronic documents, the school uses the following model [*internal / external*].

The conservation system guarantees access to the stored object for the period provided for by the conservation plan of the owner of the object of conservation and by the current legislation, or for a longer time that may be agreed between the parties, regardless of the evolution of the technological context. .

Pursuant to art. 44, paragraph 1-ter, of the DAC, as most recently amended by the D.L. 76/2020, "In all cases in which the law prescribes conservation obligations, even for private subjects, the IT document conservation system ensures, as far as it is stored, characteristics of authenticity, integrity, reliability, legibility, availability, according to the methods indicated in the "Guidelines".

In any case, the storage systems must allow for the possibility of eliminating documents where necessary (where required by current legislation).

Also take into account the retention and discard period of documents that contain personal data. According to the current legislation on the protection of personal data, in fact, this period of time must not exceed that necessary for the purposes for which the data were collected or subsequently processed.

3.2.1. TRANSFER INTO THE DEPOSIT ARCHIVE

During the deposit phase[28] the person responsible for keeping the archives[29]:

- periodically checks all the files in the current archive, both paper and electronic, in order to identify those for which the processing has already been completed and compiles a list of the documentation present in the closed files;
- provides for the thinning by eliminating any correspondence of a transitory and instrumental nature present in the file;

---

[27] The AgID adopted with Resolution no. 455/2021 the "*Regulation on the criteria for the provision of IT document storage services*" and the related annexes. Annex A, in particular, sets out the requirements for the provision of the conservation service on behalf of Public Administrations. The regulation also provides for the establishment of a marketplace for conservation services as an autonomous section of the *Cloud Marketplace* to which public and private subjects who intend to provide the IT document conservation service on behalf of Public Administrations can register. Registration in the marketplace is not mandatory but the registrars who intend to participate in assignment procedures by the Public Administrations must also meet the requirements set out in the aforementioned regulation and are subject to the supervision of AgID.

[28] Art. 67 of the Presidential Decree 445/2000 governs the transfer of documents to the deposit archive, providing, in detail, that "*1. At least once every year, the manager of the service for the management of document flows and archives transfers files and documentary series relating to proceedings concluded in a specific filing archive set up at each administration. 2. The transfer must be carried out respecting the organization that the issues and series had in the current archive. 3. The person in charge of the document flows and archives management service must compile and keep a list of the files and series transferred to the repository archive.*".

[29] The person responsible for keeping the archives can be the Headmaster or other staff in possession of suitable professional requisites or archival technical professionalism, in charge of the service for keeping the IT protocol, the management of document flows and archives, pursuant to 'art. 61 of the Presidential Decree 28 December 2000, n. 445.

- provides for the payment of all documentation, both paper and electronic, present in the list in the filing archive;
- provides for the payment in the current archive of the new year of the documentation of the practices belonging to the files present in the current archive (still in the process of being processed).

3.2.2. WASTE

In the storage archive, the activities relating to the rejection phase are carried out in which the person responsible for keeping the archives:

- periodically checks the type and storage times of the documentation, both paper and electronic, present in the storage archive to identify the one to be discarded by applying the provisions of the conservation and discard maximum limit;
- proceeds with the compilation of a list of documents to be discarded and sent to the Superintendency for approval and communicates it to the Head of Document Management;
- in the case of paper documents, sends the documentation on the list to the person responsible for destroying the paper;
- eliminates the electronic documentation present in the list approved by the Superintendency.

In case of external assignment of the conservation service, the list of archiving packages containing the documents to be discarded is generated by the person in charge of the conservation service and sent to the person in charge of the conservation who, in turn, verified compliance with the established deadlines. from the maximum conservation and discarding limit, it communicates it to the Head of Document Management.

3.2.3. TRANSFER INTO THE HISTORICAL ARCHIVE

In the phase of deposit in the historical archive[30], the person responsible for keeping the archives:

- check whether in the filing archive there are practices that have been exhausted for over 40 years, both in paper and electronic form;
- prepares a list containing all the documentation present in the dossiers themselves, should there be dossiers that have been exhausted for more than 40 years;
- sends the list of documentation to be paid to the competent personnel, in the case of paper documentation, which must identify a historical archive with sufficient space to carry out the payment.

3.2.4. RELOCATION

The delocalization phase is initiated in the event that, after having carried out the discarding operations and after having made any payment in the historical archive, from the verification of the degree of saturation of the paper deposit archive, it appears that the archive is saturated. In the event that the paper filing archive should be saturated, the person responsible for keeping the archives:

[30] Art. 69 of the Presidential Decree 445/2000, entitled "*Historical Archives*", provides that "*The documents selected for permanent conservation are transferred together with the instruments that guarantee access to them, in the State Archives competent for the territory or in the separate archive section in accordance with the provisions in force provisions on the protection of cultural heritage*".

- identifies the documentation to be relocated by selecting it from the one closest to the discard date;
- draws up the list of documents to be relocated.

The competent employee:

- analyzes the documentation received;
- identifies a structure with sufficient space in the archives;
- authorizes the delocalization of the documentation to an internal structure if this is available.

The person responsible for keeping the archives sends the request for authorization to the competent Superintendency. Once approval is received from the competent Superintendency, the person responsible for keeping the archives sends the documentation to be relocated.

4. THE ADMINISTRATIVE DOCUMENT

Administrative document, pursuant to art. 1, paragraph 1, lett. a), of the Presidential Decree 28 December 2000, n. 445, means "*any representation, however formed, of the content of documents, including internal ones, of public administrations or, in any case, used for the purposes of administrative activity*". As part of the document management process, the administrative document from an operational point of view can be classified as a document:

- received;
- sent;
- of external significance;
- of internal importance.

On the basis of its nature, however, it can be classified into a document:

- analog;
- IT.

The art. 40, paragraph 1, of the DAC, as last amended by art. 66, paragraph 1, of Legislative Decree 13 December 2017, n. 217, establishes that "*Public administrations form the originals of their documents, including those relating to registers, lists and public registers, by electronic means according to the provisions of this code and the Guidelines*".

As regards the transmission of documents between Public Administrations, pursuant to the provisions of art. 47 of the DAC, it must take place:

- through the use of e-mail[31]; that is to say
- in application cooperation.

The aforementioned communications are valid for the purposes of the administrative procedure once their origin has been verified. Paragraph 2 of the aforementioned art. 47, establishes that "*For the purposes of verifying the origin, communications are valid if: a) they are signed with a digital signature or other type of qualified electronic signature; b) or have a protocol signature as per article 55 of the decree of the President of the Republic of 28 December 2000, n. 445; c) or else it is possible to ascertain the origin otherwise, according to the provisions of current legislation or the Guidelines. In any case, the transmission of documents by fax is excluded; d) or transmitted*

[31] As reported in Appendix C of Annex 6 to the Guidelines for the training, management and storage of IT documents, the use of electronic mail is "*to be understood as a transitional method pending the application of communications between HOAs through application cooperation*" . Therefore, application cooperation is identified as the only way to aim for the communication of administrative documents registered between HOAs.

through certified electronic mail systems as per the decree of the President of the Republic February 11, 2005, n. 68 ".

Specific indications on the exchange of registered administrative documents between HOAs are contained in Annex 6 to the *"Guidelines on the training, management and storage of IT documents".*

4.1. DOCUMENT RECEIVED

Incoming correspondence can be acquired by the educational institution with different means and methods based on both the transmission method chosen by the sender and the nature of the document. An electronic document can be delivered[32]:

- by ordinary e-mail (OE);
- by certified e-mail (CE);
- via removable media (e.g., CD, pendrive).

An analog document, assuming that the main types of analog documents that reach schools are telegrams, documents by ordinary and registered mail, can be delivered:

- through the traditional mail service;
- pro manibus.

The documents, analog or digital, of which the author is not identifiable are regularly opened and registered with the protocol (with the indication "Anonymous sender"), unless otherwise assessed by the Headmaster, who will carry out any checks.

Documents received without signature but whose sender is still clearly identifiable, are registered (with the indication "Unsigned document") and forwarded to the person in charge of the procedure, who will assess the need to acquire the necessary signature for the completion of the documents.

The notarial function of the protocol (i.e. registration) is to certify the date and certain origin of a document without interfering with it. It will then be the task of the person in charge of the procedure to assess, on a case-by-case basis, for the purposes of its effectiveness with regard to a business or a specific administrative procedure, whether the unsigned document can be considered valid or not[33].

4.2. DOCUMENT SENT

The electronic documents are sent to the electronic address declared by the recipients, enabled to receive mail electronically.

4.3. EXTERNAL RELEVANCE DOCUMENT

By external relevance document we mean any document received / transmitted by / to another Body or other natural or legal person. Management is regulated by the DAC.

4.4. INTERNAL RELEVANCE DOCUMENT

For documents of internal relevance we mean all those that for any reason are exchanged between ROUs or persons of the school itself.

They can be distinguished in:

- **informal communications between ROUs** (documents of a mainly informative nature): by informal communications between units we mean exchanges of information that have no

[32] As regards the transmission of documents between Public Administrations, specific indications are contained in art. 47 of the DAC.

[33] For further information on the types of electronic subscription, see par. "4.6.1 - Electronic signatures".

probative legal value, nor relevance for the purposes of administrative action. These communications usually take place via OE and are not subject to registration and archiving;
- **exchange of documents between ROUs** (documents of a predominantly legal-evidential nature): by exchange of documents between units we mean official communications of a certain importance for the purposes of administrative action and which must be kept track of. Communications of this kind must in any case be registered.

4.5. ANALOG DOCUMENT

By analogue document we mean "*the non-IT representation of legally relevant deeds, facts or data*"[34].

The paper document is defined as "original" in its definitive drafting, perfect and authentic in its substantive and formal elements, including all the guarantee and information elements of the sender and recipient, printed on headed paper and with an autograph signature[35].

The signing of a document determines:

- the **identification of the author** of the document;
- the **authorship** of the document: by signing the document the author assumes the authorship of the same, also in relation to its content. In this regard, there is talk of non-repudiation of the signed document;
- the **integrity** of the document: the document written and signed manually guarantees against material alterations by people other than the one who put it in place.

4.6. IT DOCUMENT

By electronic document we mean "*the electronic document that contains the computerized representation of legally relevant deeds, facts or data*"[36]. The IT document, as specified in paragraph 2.1.1. of the "*Guidelines on the training, management and storage of IT documents*" issued by AgID, is formed by one of the following methods:

"*a) creation through the use of software tools or qualified cloud services that ensure the production of documents in the formats and in compliance with the interoperability rules set out in Annex 2;*

b) acquisition of an IT document electronically or on IT support, acquisition of an image copy of an analog document on IT support, acquisition of a computer copy of an analog document;

c) storage on IT support in digital format of information resulting from IT transactions or processes or from the electronic submission of data through forms or forms made available to the user;

d) generation or grouping, even automatically, of a set of data or records, coming from one or more databases, even belonging to more interoperating subjects, according to a predetermined logical structure and stored in static form ".

The IT document is unchangeable if its storage on IT support in digital format cannot be altered in its access, management and storage.

Depending on whether the IT document is formed according to one of the methods listed above, its immutability and integrity are guaranteed by one or more of the operations indicated in the aforementioned Guidelines, in paragraph 2.1.1. (page 13).

---

[34] Art. 1, paragraph 1, lett. p-bis), Legislative Decree 7 March 2005, n. 82, DAC.

[35] For further information on the receipt of unsigned documents, see par. "4.1. - Document received ".

[36] Art. 1, paragraph 1, lett. p), Legislative Decree 7 March 2005, n. 82, CAD. The definition is also contained in art. 1, paragraph 1, lett. b), of the Presidential Decree 445/2000: "*b) IT DOCUMENT: the IT representation of legally relevant deeds, facts or data.*".

At the time of the formation of the unchangeable electronic document, the relative metadata must be generated and permanently associated with it. The set of metadata associated by the school with IT documents and IT administrative documents correspond to the mandatory ones provided for in Annex 5 of the *"Guidelines on training, management and storage of IT documents".* Further metadata may be identified to be associated with particular types of IT documents, such as documents subject to particular registration.

[In case of determination of further metadata to be associated with particular types of IT documents]

The additional metadata and the particular types of IT documents to which they must be associated are shown in the Attachment *[attachment number].*

A native IT document cannot be converted into analog format before its possible acquisition in a computer protocol or archiving system. In the case of documents subject to signature, it is possible to use the advanced electronic signature (FEA), made available to educational institutions by the Ministry. The School Managers and the Directors of the General and Administrative Services of the State Educational Institutions of all levels can also use the digital signature, through the specific function on the SIDI. The aforementioned signature methods are outlined and analyzed in the next paragraph.

4.6.1. ELECTRONIC SIGNATURES

The electronic signature is the ordinary way of signing electronic documents. In particular, the current legislation on the subject identifies different types of electronic subscription:

- electronic signature, or the set of data in electronic form, attached or connected by logical association to other electronic data, used as an authentication method (Article 3, No. 10, EU Reg. No. 910/2014);
- advanced electronic signature, that is the set of data attached or connected to an IT document that allows the identification of the signatory and guarantees a unique connection with the latter (Article 3, No. 11, EU Reg. No. 910 / 2014);
- qualified electronic signature, or an advanced electronic signature based on a qualified certificate (Article 3, No. 12, EU Reg. No. 910/2014);
- digital signature, or a particular qualified electronic signature based on a qualified certificate and on a system of cryptographic keys (Article 1, paragraph 1, letter s), DAC).

In consideration of the type of technology used, the digital signature is the most secure type of signature. It is governed by art. 24 of the DAC which, in paragraphs 1, 2, 3 and 4, provides that *"1. The digital signature must uniquely refer to a single subject and to the document or set of documents to which it is affixed or associated. 2. The affixing of a digital signature integrates and replaces the affixing of seals, punches, stamps, marks and trademarks of any kind for any purpose envisaged by current legislation.For the generation of the digital signature, a qualified certificate must be used which, at the time of signing, has not expired or is not revoked or suspended. 4. According to the Guidelines, the validity of the certificate itself, as well as the identification elements of the holder of the digital signature and of the certifier and any limitations of use, must be detected through the qualified certificate. The guidelines also define the methods, including temporary ones, for affixing the signature ".*

It should also be taken into account that according to the provisions of art. 24, paragraph 4-bis, of the DAC, if a digital signature or another type of qualified electronic signature based on a revoked, expired or suspended electronic certificate is affixed to an electronic document, the document is unsigned, unless suspended status has been canceled. In any case, any revocation or suspension,

however justified, takes effect from the time of publication, unless the revocant, or whoever requests the suspension, proves that it was already aware of all the interested parties.

It is also represented that Article 20, paragraph 1-bis, of the DAC, as amended by art. 20, paragraph 1, lett. a) of Legislative Decree 13th December 2017, n. 217, establishes that *"The electronic document satisfies the requirement of the written form and has the effectiveness provided for by article 2702 of the Civil Code when there is a digital signature, other type of qualified electronic signature or an advanced electronic signature or, in any case, is formed, after computer identification of its author, through a process having the requirements set by the AgID pursuant to Article 71 in such a way as to guarantee the security, integrity and immutability of the document and, in a clear and unequivocal manner, its traceability to the author. In all other cases, the suitability of the IT document to meet the requirement of written form and its probative value can be freely assessed in court, in relation to the characteristics of security, integrity and immutability. The date and time of formation of the IT document are enforceable against third parties if affixed in accordance with the Guidelines ".*

Pursuant to art. 20, paragraphs 1-ter and 1-quater, of the DAC, introduced by art. 20, paragraph 1, lett. b), of the Legislative Decree 13 December 2017, n. 217: *"(1-ter) The use of the qualified or digital electronic signature device is presumed to be attributable to the holder of the electronic signature, unless the latter proves otherwise. (1-quater) The provisions concerning the filing of deeds and documents electronically in accordance with the legislation, including regulations, on the subject of the electronic process remain valid ".*

From the above provisions, it is possible to identify the probative effectiveness of the IT document, based on the type of signature affixed to it. In detail:

- **documents signed with a "simple" electronic signature** satisfy the requirement of the written form and their probative value can be freely evaluated in court, in relation to the characteristics of security, integrity and immutability of the signature itself;
- **documents signed with advanced electronic signature, qualified electronic signature and digital signature** meet the requirement of the written form and have the effectiveness provided for by art. 2702 of the Civil Code[37], or they make full proof up to a complaint of forgery;
- **documents signed with digital signature with revoked, expired or suspended certificate** are full proof until denied, pursuant to the provisions of art. 2712 of the Italian Civil Code[38].

It is also noted that art. 25 of the DAC, entitled "Authenticated signature", provides that the electronic signature or any other type of advanced electronic signature, authenticated by the notary or other public official authorized to do so, is recognized pursuant to art. 2703 of the Italian Civil Code[39].

[37] Art. 2702 of the Italian Civil Code establishes that "*The private deed is full proof, up to a complaint of forgery, of the origin of the declarations by the person who signed it, if the person against whom the deed is produced recognizes the signature, or if this is legally considered to be recognized*" .

[38] Art. 2712 of the Italian Civil Code establishes that "*Photographic, computer or cinematographic reproductions, phonographic recordings and, in general, any other mechanical representation of facts and things form full proof of the facts and things represented, if the one against whom they are produced does not deny their conformity the facts or the things themselves* ".

[39] Art. 2703 of the Italian Civil Code establishes that "*1. The signature authenticated by the notary or other public official authorized to do so is recognized. 2. The authentication consists in the attestation by the public official that the signature has been affixed in his presence. The public official must first ascertain the identity of the person who signs* ".

The DAC[40] also establishes that the acts listed in numbers 1 to 12 of art. 1350 of the Italian Civil Code must be signed with a qualified electronic or digital signature, under penalty of nullity. The acts referred to in n. 13, of the aforementioned art. 1350 of the Civil Code, on the other hand, in addition to the types of signature mentioned above, they can also be signed with an advanced electronic signature or must be formed with the additional methods referred to in Article 20, paragraph 1 bis, first sentence[41].

The protocol registration of an IT document signed with a digital signature is performed after the protocol operator has verified the validity of the digital signature with a special function on the protocol system.

Without prejudice to the foregoing, electronic documents can also be unsigned and in this case the rules contained in par. "4.1. - Document received "[42].

Lastly, it is noted that, in all paper documents that come from and are generated by automated systems, the signature on the paper document of the responsible officer can be replaced by the

wording by the "*Handwritten signature replaced by the press, pursuant to art. 3, paragraph 2, Law 39/1993* ".

4.7. MINIMUM CONTENT OF DOCUMENTS

Administrative documents, both analogical and IT, having external relevance, must contain the following information:

- name and logo of the sending administration;
- full address of the administration (street, number, postcode, city, province);
- certified e-mail address of the school;
- indication of the educational institution and the ROU that produced the document;
- the telephone number of the ROU and the RUP (optional, at the bottom of the page if applicable);
- Tax code, VAT number, iPA code, unique code for the F.E.

In addition, the document must contain at least the following information:

- place and date (dd / mm / year) of preparation of the document;
- protocol number;
- subject of the document.

It must not contain the reference to the fax number, in accordance with the provisions of art. 14, paragraph 1-bis, of the decree-law of 21st June 2013, n. 69, as amended by law no. 98, containing "*Measures to promote the diffusion of the digital home*", which establishes that, for the purpose of verifying the origin of communications, the transmission of documents by fax between Public

[40] Art. 21, paragraph 2-bis, of the DAC.

[41] Art. 1350 of the Italian Civil Code establishes that "*The following must be done by public act or by private writing, under penalty of nullity: 1) contracts that transfer the ownership of immovable property; 2) contracts that constitute, modify or transfer the right of usufruct on immovable property, the surface right, the rights of the grantor and the leaseholder; 3) the contracts which constitute the communion of rights indicated in the previous numbers; 4) contracts that constitute or modify the easements, the right of use on immovable property and the right of residence; 5) deeds of renunciation of the rights indicated in the previous numbers; 6) the contracts for the redemption of the lease fund; 7) anticresi contracts; 8) leasing contracts for real estate for a duration of more than nine years; 9) company or association contracts with which the enjoyment of real estate or other real estate rights is conferred for a period exceeding nine years or for an indefinite period; 10) deeds that constitute perpetual or life annuities, subject to the provisions relating to State revenues; 11) deeds of division of real estate and other real estate rights; 12) transactions involving disputes relating to the legal relationships mentioned in the previous issues; 13) other acts specially indicated by the law* ".

[42] For further information on the receipt of unsigned documents, see par. "4.1. - Document received ".

Administrations is in any case excluded. It is the faculty of the Head of Document Management to add other rules for the determination of the contents and for the definition of the structure of the IT documents. It should also be noted that in terms of access to administrative documents[43], each educational institution is responsible for specifying precisely the registration details of a document on its own protocol systems.

The indication of these elements (including the object) must comply with the standards indicated in this manual[44]. This is because an essential prerequisite for the full enjoyment of the right to access the documents is the availability of the latter which is ensured by a correct and standardized definition / transcription of the object.

4.8. PROTOCOLABILITY OF A DOCUMENT

They are subject to mandatory registration, pursuant to art. 53, paragraph 5, of the Presidential Decree n. 445 of 2000, the documents received and sent by the administration and all IT documents[45].

Furthermore, art. 40-bis of the DAC, as amended by articles 37, paragraph 1, and 66, paragraph 1, of the Legislative Decree 13 December 2017, n. 217, provides that they are the subject of protocol registration pursuant to article 53[46] of the Presidential Decree. n. 445 of 2000, "*the communications that come from or are sent to digital domiciles elected pursuant to the provisions of article 3-bis, as well as the requests and declarations referred to in article 65 in compliance with the Guidelines*".

On the other hand, the following are excluded from mandatory registration[47]:

- the official gazettes;
- the official bulletins and newsletters of the Public Administration;
- the acknowledgment of receipt of the circulars and other provisions;
- statistical materials;
- internal preparatory acts;
- newspapers, magazines;
- the books;
- advertising materials;
- invitations to events;
- all documents already subject to special registration by the Administration.

In the event that it is necessary to attribute a certain date to an electronic document not subject to registration produced within the school, the rules for "time validation" referred to in the Prime Ministerial Decree of 22nd February 2013 "*Technical rules on the subject generation, affixing and verification of advanced, qualified and digital electronic signatures, pursuant to articles 20, paragraph 3, 24, paragraph 4, 28, paragraph 3, 32, paragraph 3, letter b), 35, paragraph 2, 36, paragraph 2, and 71* ".

---

[43] As part of the access regulations, art. 1, paragraph 1, lett. d), of Law 241/1990 defines the administrative document as "*any graphic, photocinematographic, electromagnetic or any other type of representation of the content of documents, even internal or not related to a specific procedure, held by a public administration and concerning activities of public interest, regardless of the public or private nature of their substantive discipline* ".

[44] For further information, see par. "5.2. - Writing of protocol data ".

[45] The "*Guidelines on the training, management and storage of IT documents*", issued by the AgID, provide that "*The computer registration of documents is represented by the set of data in electronic form attached or connected to the IT document for the purpose of identification univocal of all documents produced and acquired. For the Public Administration, the provisions of Article 53, paragraph 5, of the TUDA apply*. "

[46] Art. 53, paragraph 5, of the Presidential Decree 445/2000, the first period provides that "*Documents received and sent by the administration and all IT documents are subject to mandatory registration*".

[47] Art. 53, paragraph 5, of Presidential Decree 445/2000.

In particular, the "time validation" makes it possible to establish the moment in time in which the IT document was formed and is defined as the result of an IT procedure capable of offering a time reference that can be opposed to third parties.

The tool for obtaining this result is the "time stamp"[48], or "*the time reference that allows time validation and which demonstrates the existence of computer evidence in a certain time*".

5. THE IT PROTOCOL

5.1. PROTOCOLATION

By protocol we mean the activity of registration of the protocol through which the affixing or association to the document, in a permanent and non-modifiable form, of the information concerning the document itself.

The documents that must be registered in the protocol are indicated in paragraph “4.8. - Protocollability of an administrative document ".

Each protocol number identifies a single document and any attachments thereto and, consequently, each document with its attachments bears a single, unchangeable protocol number.

So it is not allowed:

- register a document already registered;
- manually affix the protocol signature, except in cases in which affixing via the application can deteriorate the fundamental information of the document (e.g. overlapping of the incoming stamp to the outgoing stamp, presence of a plasticized adhesive label that would be blackened by the printer);
- in case of mass shipment and arrivals, affix a signature such as: 1741/1, 1741/2, 1741/3, etc. or give them the same protocol number;
- register acts of internal relevance in the official register without using the appropriate internal registration method;
- select a registration number on the date of receipt of the document in order to carry out the registration operation at a later date;
- sign the document after registration;
- associate further attachments produced or received subsequently to a previous registration.

The logging for each document is carried out by storing the following elements[49]:

- protocol number of the document automatically generated by the system and recorded in an unchangeable form;
- protocol registration date assigned automatically by the system and recorded in a non-modifiable form;
- sender for the documents received or, alternatively, the recipient or recipients for the documents sent, registered in an unchangeable form;
- object of the document, registered in an unchangeable form;
- date and protocol of the document received, if available;
- the imprint of the electronic document, if transmitted electronically, consisting of the sequence of binary symbols, capable of uniquely identifying its content, recorded in an unchangeable form;
- information relating to the internal administration assignment and any classification[50].

[48] Art. 1, paragraph 1, of the Prime Ministerial Decree of 22nd February 2013.

[49] These elements are defined in art. 53, paragraph 1, of the Presidential Decree 445/2000.

[50] This element is provided for by the "*Guidelines on the training, management and storage of IT documents*" issued by the AgID.

The registration operation, as described above, must be carried out only after having loaded the main document and its attachments on the system (which must all bear the same protocol number).

5.2. WRITING OF PROTOCOL DATA

The computerized management of the school's document flows requires particular attention to the quality of the information associated with the documents concerned, in the registration phase, in order to prevent them from being unavailable or difficult to trace.

For this purpose, the rules that the users of the IT protocol system must comply with for the preparation of the following data are set out below:

TYPEOF DATA	**RULES**
Personal names	- First the name and then the surname - All caps **Example:** MARIO ROSSI
Professional and / or institutional qualifications	Always omitted
Names of cities and states	In Italian, in full and without pointing **Example:** San Vitaliano (Na) and not S. Vitaliano (Na)
Names of firms and companies	- If they contain personal names, the previous rules apply - Use initials, in capital letters and without periods or, alternatively, acronyms - The company form without points **Example:** GIUSEPPE BIANCO, ACME SpA
Entities and associations in general	Use capitalized and non-period abbreviations where available
Ministries	Use the shortened and bulleted form of the word Ministry alone, or the acronym **Example:** MIN. EDUCATION, or MI
Second level entities	Use the extended form or known acronyms
Abbreviations in general	Capitalized and without periods **Example:** MI
Quotation marks and superscripts	- Type the character directly from the keyboard - Do not perform the Windows copy and paste function
Dates	Use the following number format:

	DD-MM-YYYY or DDMMYYYY **Example:** 20-07-2020 or 20072020 and not 20/07/2020

In addition to the above, the educational institution adopts the following additional rules for the preparation of data: [*list of additional rules*].

5.3. PROTOCOL MARKING

The protocol signature is the affixing or association to the original of the document, in a permanent and non-modifiable form, of information regarding the document itself. The signature operation is carried out by the application automatically and simultaneously with the protocol registration operation[51]. It allows you to identify each document unambiguously.

The minimum information required in the protocol signature is[52]:

- the progressive number of the protocol[53];
- the protocol date;
- the identification in summary form of the Administration or Organizational Area identified.

The protocol signature operation can include any other useful or necessary information, if such information is already available at the time of protocol registration. When the document is addressed to other Administrations and is formed and transmitted with IT tools, the protocol signature can include all the registration information of the document.

The protocol signature of the school, in compliance with the technical rules set out above, adopts the minimum set of information and uses as the identification of the Administration the code with which the school is uniquely identified on the Public Administrations Index.

5.4. DEFERRAL OF THE PROTOCOL REGISTRATION

The protocol records of documents received by the school are made on the day of arrival and in any case no later than three working days from receipt of said documents. If the protocol registration cannot be carried out within the times indicated above, the Manager may authorize the registration at a later time, however setting a time limit and giving value, in the case of predetermined deadlines, to the arrival date stamp, specifying the 'authorization through specific internal notes. The deferred protocol consists in the postponement of the registration deadlines and is applied to incoming documents.

5.5. RECEIPT OF PROTOCOLATION

Receipt of documents via PEC involves sending two different types of receipts to the sender: one linked to the certified mail service, one to the IT protocol service. In the case of receipt of electronic documents through certified e-mail, the notification to the sender of the delivery of the message is ensured by the certified e-mail service, used by the school with specific standards.

In the case of documents received via OE, an acknowledgment of receipt with relative electronic signature in XML format of the document is sent through the appropriate function ("Forward" or "Reply").

---

[51] Art. 55, paragraph 2, Presidential Decree 445/2000 and "*Guidelines on the training, management and storage of IT documents*", issued by the AgID, p. 20.

[52] This information is defined in art. 55 of the Presidential Decree 445/2000.

[53] Pursuant to art. 57, paragraph 1, of the Presidential Decree 445/2000 44 "*The protocol number is progressive and made up of at least seven numerical digits. The numbering is renewed every calendar year.* ".

5.6. DAILY LOG OF PROTOCOL

The protocol register is the tool through which it is possible to uniquely and certainly identify the documents received and sent by registering certain elements that characterize each single document. For this reason, the protocol register performs a fundamental legal evidential function, certifying the existence of a specific document within the document management system and guaranteeing its authenticity.

Therefore, in accordance with current legislation, the official protocol register is unique, both for incoming and outgoing registration, and in internal mode and the progressive numbering of the protocol registrations is unique regardless of the organizational model adopted. The numbering closes on December 31st and starts again on the following January 1st. It updates automatically and daily.

The daily protocol register consisting of the list of information entered with the protocol registration operation must be produced automatically within the same day.

It must be sent automatically by the protocol system, in a format that guarantees that it cannot be modified. In order to guarantee the non-modifiability of the registration operations, the daily log register is transmitted within the next working day to the storage system[54].

It is specified that with reference to the protocolling carried out exclusively on the official protocol register, the operator who manages the sorting of documents can define a protocol registration as “confidential” and assign it by competence to an assignee user.

Please note that the following documents are subject to confidential registration:

- documents relating to personal events or private or particular facts;
- documents of a political nature or direction which, if made public, may hinder the achievement of the set objectives;
- documents whose simultaneous advertising may cause prejudice to third parties or to the good performance of the administrative activity.

You can set an expiration date to the confidential character of the document. Once the confidentiality terms have expired, the document becomes visible to those who are enabled.

5.7. EMERGENCY REGISTER

In the event of interruptions in the operation of the IT protocol system due to accidental or planned technical causes, pursuant to art. 63 of the Consolidated Law, the protocol registrations are made in an emergency register[55].

---

[54] "*Guidelines on the training, management and storage of IT documents*", issued by the AgID.

[55] Art. 63 of the Presidential Decree 445/2000 provides that "*1. The person in charge of the service for keeping the IT protocol, managing document flows and archives authorizes the carrying out, even manually, of the protocol recording operations on one or more emergency registers, whenever for technical reasons it is not possible to use the normal procedure informatics. The cause, the date and time of the start of the interruption as well as the date and time of the restoration of the system's functionality are shown in the emergency register. 2. If the inability to use the IT procedure extends beyond twenty-four hours, for reasons of exceptional gravity, the person responsible for keeping the protocol may authorize the use of the emergency register for subsequent periods of no more than one week. The details of the authorization provision must be reported in the emergency register. 3. For each day of emergency recording, the total number of manually recorded operations is reported in the emergency log. 4. The numerical sequence used on an emergency register, even following subsequent interruptions, must in any case ensure the unambiguous identification of the documents registered within the documentary system of the homogeneous organizational area. 5. The information relating to documents registered in an emergency is entered into the computer system, using a special data recovery function, without delay in restoring system functionality. During the recovery phase, each document registered in an emergency is assigned a protocol number of the ordinary IT system, which permanently maintains the correlation with the number used in an emergency* ".

The Head of Document Management authorizes with his own provision the preparation of the emergency register in paper or digital form and, upon restoration of the functionality of the IT protocol system, all the registrations made are entered into the system, continuing the numbering of the general protocol reached at the time of service interruption. This registration is also associated with the protocol number and the registration date shown on the emergency protocol, maintaining a correlation with the number used in an emergency. The cause, date and start time of the interruption of the protocol system are reported in the emergency register. In these cases, the Emergency Registration Forms must be completed in their entirety and signed.

If the interruption of the protocol system operation lasts for more than twenty-four hours, the Document Management Manager, in accordance with current legislation, authorizes the use of the emergency register for subsequent periods of no more than one week; in such cases, in addition to the above information, the details of the authorization provision are reported in the emergency register.

5.8. SPECIAL REGISTERS

Within the school, special registers are established that can be removed from consultation by those who are not expressly authorized and for which particular forms of confidentiality and access may be provided. Only electronic documents or images of paper documents must be uploaded to these registers according to the instructions contained in the decree establishing the particular register in question, which must be fully reported in this manual.

Documents that are subject to special registration by the educational institution and which, pursuant to art. 53, paragraph 5, of the Presidential Decree 445/2000, are excluded from registration and are defined in this manual, with indication of how to manage the related registers.

The following documents are subject to special registration:

- *the resolutions of the Institute Council and the Teaching Body;*
- *the reports of the School Council, the Executive Board, the Teaching Body, the Class Councils;*
- *the decrees of the Headmaster;*
- *diplomas;*
- *the certificates issued by the schoo*l.

For the management of the processing of particular IT registrations, the registers of the aforementioned list are identified.

The procedures for managing the registers listed above are described below: *paper and electronic*.

5.9. CANCELLATION OF PROTOCOL REGISTRATIONS

The need to modify even one of the mandatory fields of the protocol registration recorded in non-modifiable form, to correct errors that occurred during manual data entry or through the interoperability of the sender and recipient protocol systems, entails the obligation to cancel the entire protocol registration.

Only the manager of document management is authorized to cancel or to issue provisions for the cancellation of protocol registrations. The cancellation of a protocol registration must be requested with a specific e-mail, adequately motivated, addressed to the Head of Document Management who, only following the assessment of the particular issue, can authorize the cancellation.

The canceled information must remain stored in the database to be subjected to the processing required by the procedure. In this case, the procedure for indicating cancellation shows the

the wording "canceled" in a position that is always visible and in any case such as to allow the reading of all the original information together with the date, the identification of the operator and the details of the authorization measure. The system records the correction, the date and the person who intervened.

At the time of cancellation of a general protocol registration, the application requires the motivation and details of the cancellation provision.

5.10. PROCESSING METHOD OF THE SCANNING PROCESS

The scanning process is divided into the following phases:

- acquisition of images in such a way that each document, even consisting of several pages, corresponds to a single file in a standard format enabled for storage;
- verification of the correctness of the image acquisition and the exact correspondence of the images obtained with the paper originals;
- link of the images to the respective protocol recording, in a non-modifiable way;
- storage of images, in an unchangeable way.

In line with process certification[56], the protocol operator, downstream of the scanning process, certifies the conformity of the scanned document to the original document.

In short, the compliance of the computerized image copy of an analog document is ensured through[57]:

- certification from a public official;
- affixing of the digital signature or qualified electronic signature or advanced electronic signature or other type of signature pursuant to art. 20, paragraph 1-bis, or the qualified or advanced electronic seal by the person making the comparison.

The certificate of conformity of the copies can be inserted in the IT document containing the copy by image or be produced as a separate IT document containing a time reference and the imprint of each copy by image.

The electronic document containing the certificate is signed with a digital signature or a qualified or advanced electronic signature of the notary or the public official authorized to do so.

In any case, documents that cannot be scanned due to their physical characteristics (non-standard or particularly bulky formats) are not reproduced in image format.

It should be noted that if documents contain particular categories of personal data referred to in art. 9 of EU Regulation 679/2016, the protocol operator, with the necessary qualifications, must mark the document as containing confidential data[58].

6. ACCESS, TRANSPARENCY AND PRIVACY

6.1. PROTECTION OF PERSONAL DATA AND SECURITY MEASURES

The school's document management system must adopt a mechanism of compliance with the legislation on the protection of personal data, pursuant to EU Reg. 679/2016 and Legislative Decree 196/2003, amended by Legislative Decree no. Lgs. 101/2018[59].

---

[56] See, in this regard, articles 22, paragraph 1-bis, and 23-ter, paragraph 1-bis, of the DAC and Annex 3 to the "*Guidelines on the training, management and storage of IT documents*" issued by AgID.

[57] Art. 22 of the DAC.

[58] For further information, see par. "6.1 - Protection of personal data and security measures".

[59] "*The Guidelines on the training, management and storage of IT documents*" issued by the AgID, establish that "*[...] the person in charge of document management or, where appointed, the coordinator of document management, in*

The educational institution must take initiatives aimed at complying with the provisions of EU Regulation 679/2016, with particular reference to:

- the principle of lawfulness of data processing;
- the principle of minimization of data processing[60];
- to exercise the rights referred to in Articles 15-22 of the GDPR by the interested parties;
- the methods of processing and the data requirements;
- to the information provided to the interested parties and to the relative consent when due;
- to the risk analysis on the rights and freedoms of the interested parties;
- to identify the Data Protection Officer;
- to identify the subjects authorized to process the data;
- to the risk analysis on the rights and freedoms of the interested parties;
- security measures[61].

Without prejudice to the foregoing, the concept of accountability and the ability to adopt an effective process for data protection are of particular importance, so that the risk of their possible violation is minimized.

To this end, the Head of Document Management, in agreement with the Head of Conservation, with the Head of Digital Transition, and having acquired the opinion of the Head of Personal Data Protection, prepares the security plan of the IT document management system, providing for appropriate technical and organizational measures to ensure a level of security adequate to the risk of personal data protection, pursuant to art. 32 of EU Reg. 679/2016, also according to the types of data processed, such as those referable to the particular categories referred to in Articles 9-10 of the Regulation itself.

On this point, the Privacy Guarantor in the Opinion on the "*Guidelines on the training, management and storage of IT documents*" of 13th February 2020, highlighted that the mere reference to the measures referred to in the AgID circular of 18th April 2017, n. 2/2017, as part of the security requirements to which the various subjects involved in the processing are required, is not in itself sufficient to ensure the adoption of adequate processing security measures, in compliance with the Regulation, pursuant to which, on the other hand, it is necessary to concretely evaluate the risks that may derive, in particular, from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, to personal data transmitted, stored or otherwise processed.

The educational institution is therefore required to adopt suitable and preventive security measures, aimed at safeguarding the personal data processed, in order to minimize the risk of destruction or loss, even accidental, of unauthorized access or unauthorized processing. permitted or not in accordance with the purposes of the collection, in relation to the knowledge acquired on the basis of technical progress, their nature and the specific characteristics of the treatment.

Specifically, the technical / organizational measures adopted by the school are as follows:

a) *pseudonymisation and encryption of personal data;*
b) *the ability to ensure the confidentiality, integrity, availability and resilience of the processing systems and services on a permanent basis;*

---

agreement with the person in charge of the conservation of referred to in paragraph 4.6, with the person in charge of the digital transition and having acquired the opinion of the person responsible for the protection of personal data, prepares the security plan of the IT document management system, providing for appropriate technical and organizational measures to ensure an adequate level of security the risk regarding the protection of personal data, pursuant to art. 32 of EU Regulation 679/2016 (GDPR), also depending on the types of data processed, such as those referable to the particular categories referred to in Articles. 9-10 of the Regulation itself. ".

[60] Art. 5, paragraph 1, lett. c), of EU Regulation 679/2016.

[61] The security measures must "*guarantee a level of security adequate to the risk*" of the processing; in this sense, art. 32 par.1 of EU Regulation 679/2016 offers an open and non-exhaustive list.

c) *the ability to promptly restore the availability and access of personal data in the event of a physical or technical incident;*
d) *a procedure for testing, verifying and regularly evaluating the effectiveness of technical and organizational measures in order to guarantee the security of the processing.]*

6.2. RIGHT OF ACCESS TO DOCUMENTS

6.2.1. DOCUMENTAL ACCESS

The right of access means, pursuant to art. 22, paragraph 1, lett. a), of Law 241/1990, "*the right of interested parties to view and to extract copies of administrative documents*".

The applicants must be bearers of a direct, concrete and current interest, corresponding to a situation that is legally protected and linked to the administrative document and related documents.

Interested parties must make a reasoned access request, an objective assessment of the position of the applicant being necessary to verify the existence of a link of instrumentality with respect to a legally protected situation linked to the document to which access is requested.

The right of access is excluded for[62]:

- documents covered by state secrecy;
- tax proceedings;
- the activity of the Public Administration aimed at issuing general regulatory or administrative acts;
- selective procedures containing psycho-attitudinal information.

The right of access to administrative documents takes priority over the right to confidentiality in all those cases in which the ostensive request is intended to protect and defend one's legal interests.

The educational institution must carry out an objective assessment regarding the position of the applicant to verify the existence of an instrumentality link with respect to a legally protected situation connected to the document to which access is requested, also taking into account any provisions in the specific regulation for document access, adopted by the school, in compliance with the provisions contained in the ANAC resolution 1309/2016.

As far as privacy profiles are concerned, Legislative Decree 196/2003 in art. 59, entitled "*Access to administrative documents and civic access*" provides that "*1. Without prejudice to the provisions of Article 60, the conditions, methods, limits for exercising the right of access to administrative documents containing personal data, and the related judicial protection, remain governed by the law of 7 August 1990, no. 241, and subsequent amendments and by the other legal provisions on the subject, as well as by the related implementing regulations, also for what concerns the types of data referred to in articles 9 and 10 of the regulation and the processing operations that can be carried out in execution of a request of access.* ".

In short, it is noted that compared to[63]:

- *Personal data*: the right to access administrative documents can prevail over the interest in confidentiality, in compliance with the principle of minimization;
- *Sensitive and judicial data*: the right to access prevails only where it is strictly essential;
- *Highly sensitive data (genetic data and / or suitable for revealing the state of health and sexual life)*: the right of access prevails only if the legally relevant situation that you intend

[62] Art. 24, Law 241/1990.
[63] Art. 24, paragraph 7, Legislative Decree 241/1990; Art. 59 and 60, Legislative Decree 196/2003.

to protect with the request for access to administrative documents consists of a right of personality or in another fundamental right or freedom.

In this regard, in the management of access and consultation of documents held by the school by third parties, the Manager is required to constantly update the person in charge of the protection of personal data.

In any case, in the case of direct access to its archives, the Administration that owns the data, issues to the proceeding Administration a specific authorization in which any access limits and conditions are indicated, aimed at ensuring the confidentiality of personal data pursuant to current legislation also through the stipulation of specific service agreements.

Similarly, in the event that a confidential registration is carried out (as indicated in paragraph 5.8.), The complete visibility of the document is only possible for the user assignee by competence and for the protocol operators who have the application permission of confidential registration (permission associated with the role). All other users (even if included in the right list of competence) can only access the registration data (for example, protocol number, registration date), while the data relating to the protocol profile (for example, classification) are obscured.

The documents are never viewed by users without access rights, even in the face of a general search in the archive or a full text search.

6.2.2. GENERALIZED CIVIC ACCESS (FOIA)

The right to generalized civic access (FOIA) concerns the possibility of accessing data, documents and information held by Public Administrations in addition to those subject to mandatory publication provided for by Legislative Decree 33/2013[64].

Applications can be submitted by anyone, regardless of particular qualification requirements, and without the need for motivation.

Generalized civic access is aimed at:

- ensure access to anyone regardless of ownership of subjective legal situations;
- promote participation in the public debate;
- encourage widespread forms of control over the pursuit of institutional purposes and the use of public resources.

In order to examine the requests, educational institutions should also adopt adequate organizational solutions, such as, for example, "*the concentration of the competence to decide on access requests in a single office (equipped with adequate professional resources, which specialize over time , accumulating know-how and experience), which, for investigative purposes, communicates with the offices that hold the requested data* ", as indicated in the ANAC Resolution

[64] Generalized civic access is provided for by art. 5, paragraph 2, of Legislative Decree 33/2013 and differs from the simple civic access referred to in paragraph 1 of the same article, which establishes that "*The obligation established by current legislation for public administrations to publish , information or data entails the right of anyone to request the same, in cases where their publication has been omitted* ". As previously highlighted, the request for civic access, if it relates to data, information or documents subject to mandatory publication pursuant to Legislative Decree 33/2013, is presented to the Head of Corruption Prevention and Transparency.

1309/2016[65]. Without prejudice to the above, the schools receiving the application must issue an express and motivated provision within the next thirty days.

It is represented that generalized civic access is limited if a public interest is jeopardized, that is:

- public safety and public order;
- national security;
- defense and military matters;
- international relations;
- the political and financial and economic stability of the state;
- conducting investigations into crimes and their prosecution;
- the regular performance of inspections.

The educational institution must also carry out an evaluation activity with the balancing technique, case by case, between the public interest in generalized disclosure and the protection of interests considered valid by the legal system. The refusal is necessary to avoid a concrete prejudice to the protection of one of the following private interests:

- protection of personal data;
- freedom and secrecy of correspondence;
- economic and commercial interests, including intellectual property, copyright and trade secrets[66].

On requests for review presented by applicants to whom access has been totally or partially denied or who have not received a response within the established deadline, the Head of Corruption Prevention and Transparency decides with a reasoned provision, within twenty days.

If access has been denied or postponed for reasons of protection of personal data protection, the Head of Corruption Prevention and Transparency, without prejudice to the comparison with the DPO, must provide, after consulting the Data Protection Officer, who decides within ten days of the request. The term for the adoption of the provision by the HCPT is suspended until the opinion of the Officer is received and in any case for a period not exceeding the aforementioned ten days[67]. In the cases of negative or partially negative responses listed above, the educational institution is required, in any case, to provide adequate and complete motivation.

Specific indications and operational recommendations on the FOIA are contained in the Circular of the Minister for Simplification and Public Administration no. 2/2017 concerning "*Implementation of the rules on generalized civic access (so-called FOIA)*", in particular:

- competent offices;
- decision times;
- counter-interested parties;
- refusals not allowed;
- dialogue with applicants;
- Access register.

[65] The ANAC Resolution no. 1309 of 28 December 2016, containing *"Guidelines containing operational indications for the purpose of defining the exclusions and limits to civic access pursuant to art. 5 c. 2 of Legislative Decree 33/2013*" was adopted pursuant to of article 5-bis, paragraph 6, of Legislative Decree 33/2013 which establishes that "*For the purposes of defining the exclusions and limits to civic access referred to in this article, the National Anti-corruption Authority, 'agreement with the Guarantor for the protection of personal data and after consulting the unified conference referred to in article 8 of legislative decree 28 August 1997, no. 281, adopts guidelines containing operational indications* ".

[66] See, on this point, art. 5-bis of Legislative Decree 33/2013 and the ANAC Resolution 1309/2016.

[67] Art. 5, paragraph 7, of Legislative Decree 33/2013.

On 28 June 2019, the Ministry of Public Administration also adopted circular letter no. 1/2019 in order to provide the Public Administrations with additional "*guidelines and clarifications*" with respect to the "*operational recommendations*" referred to in circular no. 2/2017 and the ANAC Guidelines adopted in agreement with the Guarantor for the protection of personal data in 2016. The profiles processed concern:

- application criteria of a general nature;
- cost regime;
- notification to the counter-interested parties;
- participation of the counter-interested parties in the review phase;
- deadline for proposing the request for review;
- technological support tools.

6.2.3. ACCESS REGISTER

The register of access requests presented for all types of access is set up at the school, in accordance with the provisions of the aforementioned documents, namely, ANAC Resolution no. 1309/2016, as well as the Circular of the Minister for Public Administration n. 2/2017, and the subsequent Circular of the Minister for Public Administration no. 1/2019.

The register is established through the organized collection of requests with the indication of the subject, the date and the relative outcome (with the date of the decision), which will be published on the institutional website of the educational institution on a quarterly basis. The implementation of the register takes place through the use of the computer protocol system and document flows which the school is equipped with pursuant to Presidential Decree n. 445 of 2000, of the DAC and related technical rules.