ACCADEMIA NAZIONALE DEI LINCEI

Data Protection Policy

Version 1.0 as of November 6, 2024

Summary

1. Scope, purpose, and recipients

This Policy establishes the principles and operating procedures adopted by the Accademia nazionale dei Lincei to effectively, responsibly, and transparently protect personal data in compliance with the requirements of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR) and the Code on the protection of personal data (D.Lgs. n. 196/2003), as amended by D.Lgs. n. 101/2018, which adapts the national regulatory framework to the European Regulation.

The principles and guidelines expressed in this Policy apply to the bodies of the Institution, all employees of the Academy, collaborators, and external consultants, as well as to anyone with access to personal data held and processed by the Academy. It is also shared with all formally designated Data Controllers. It applies to all data held by the Institution relating to identified or identifiable natural persons:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Phone numbers;
- Online identifiers;
- Pseudonyms;
- Other information related to the physical, physiological, economic, cultural, and social identity of a natural person.

As the Data Controller, the Academy is responsible for ensuring compliance with the data protection requirements described in this Policy. Failure to comply may expose the Institution to complaints, regulatory action, fines, and/or damage to its reputation.

The Academy is committed to ensuring the continuous and effective implementation of this Policy and requires all its employees and collaborators to share this commitment.

2. References: Normative, regulatory, and standards

- Law No. 10 of August 2018, n. 101 - *Dispositions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data, as well as the free circulation of such data and repealing Directive 95/46/CE*
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016 - *General Data Protection Regulation*
- Law No. 22 of January 2004 and subsequent amendments – *Code for cultural heritage and landscape*
- Law No. 30 of June 2003, n. 196 – *Code on the protection of personal data*
- Provision by the Guarantor Authority No. 513, dated December 19, 2018 – *Ethical rules for processing for public interest purposes or for historical research, published pursuant to Article 20, paragraph 4, of Law No. 10 of August 2018, n. 101, dated December 19, 2018*
- Circular No. 18 of April 2017, n. 2/2017 – Agency for Digital Italy (AgID) – Replacement of

Circular No. 1/2017 of March 17, 2017, concerning: «Minimum ICT security measures for public administrations (Directive of the President of the Council of Ministers 1 August 2015)»

- Provision by the Guarantor Authority No. 15 of May 2014 – *Guidelines for the processing of personal data carried out by public bodies for publication and dissemination on the web*
- Provision by the Guarantor Authority No. 27 of November 2008 and subsequent amendments – *Measures and precautions prescribed to data controllers carrying out processing using electronic tools, relating to the assignment of system administrator functions*
- Provision by the Guarantor Authority No. 13 of October 2008 – *Waste of electrical and electronic equipment (WEEE) and data protection security measures*
- *Guidelines from the European Archives Group for the application of the European Regulation on the protection of personal data in the archival sector (October 2018)*
- ISO/IEC 27001:2022 – Information security management systems – Requirements
- ISO/IEC 27002:2022 – Information security, cybersecurity, and privacy protection – Information security controls
- ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO/IEC 29100:2011 – Information technology — Security techniques — Privacy framework
- ISO/IEC 29134:2017 – Information technology — Security techniques — Guidelines for privacy impact assessment
- Provision by the Chancellor – Director General n. of – Appointment of the Data Protection Officer

3. Key Acronyms and Definitions

For the purposes of this Policy, the following terms are used:
Academy: Accademia nazionale dei Lincei
Data Protection Authority: The Authority for the protection of personal data
Categories of special personal data: Personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data intended to uniquely identify a natural person, health or sexual life or sexual orientation data of a person
Personal data: Any information relating to a natural person identified or identifiable
GDPR: General Data Protection Regulation (Regulation (EU) 2016/679)
Data subject: The natural person to whom the personal data relates
Pseudonymization: The processing of personal data in such a way that they can no longer be attributed to a specific person without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures intended to ensure that these personal data are not attributed to a natural person identified or identifiable
Data controller: The natural person or legal entity, public authority, service or other body that processes personal data on behalf of the data controller
RPD: Data Protection Officer
Data controller: The natural person or legal entity, public authority, service or other body, either alone or in conjunction with others, which determines the purposes and means of processing personal data.

Processing: any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, registration, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, transmission or dissemination by any means, or any other form of making available, matching or merging, limitation, deletion, or destruction.
UO: organizational unit

4. General principles applicable to the processing of personal data

The Academy complies with the following principles in the collection, use, storage, transmission, and deletion of personal data.

Principle 1: Legality, Accuracy, and Transparency
Personal data must be processed lawfully, accurately, and transparently in relation to the data subject.
To this end, the Academy carries out treatments based on a determined legal basis or, where applicable, to comply with a legal obligation to which it is subject, or for the purpose of performing a contract for which the data subject is a party, with the prior consent of the data subject if the processing is not related to the exercise of public powers to which it is entrusted (legality). The Academy clearly and explicitly informs data subjects about the processing that will be carried out, the specific purposes of the processing, the manner in which the personal data relating to them are collected, used, consulted, or otherwise processed, and ensures that the processing carried out is in accordance with the information provided to the data subject and does not, in any way, prejudice, discriminate against, or mislead the latter (transparency). Accuracy.

Principle 2: Purpose Limitation
Personal data must be collected for specified, explicit, and legitimate purposes and processed in a manner that is not incompatible with those purposes.
The Academy specifies the purposes of processing at the time of collecting data from interested parties and limits subsequent processing to what is necessary to achieve the specified purpose. Further processing permitted compared to the initial purposes is carried out by the Academy for public interest archiving and historical research purposes. These purposes are considered necessary for a relevant public interest for which the Academy, as a public body, is legally obliged. In the execution of these further processing, the Academy implements the technical and organizational measures specified in this Policy to ensure adequate safeguards for the rights and freedoms of data subjects.

Principle 3: Data Minimization
Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
The Academy does not collect or store personal data that is excessive in relation to the purposes of the processing. Where possible and appropriate, the Academy will anonymize or pseudonymize personal data in order to reduce potential risks for data subjects.

Principle 4: Accuracy
Personal data must be accurate and, where necessary, kept up to date.
The Academy ensures the accuracy of the data processed by periodically verifying and updating them, and by applying, where necessary, all reasonable measures to ensure that inaccurate personal data are corrected or deleted.

Principle 5: Limitation of Retention
Personal data must be stored in a form that allows the identification of data subjects for a period no longer than that necessary for the purposes for which they are processed.
To this end, the Academy establishes a retention period for each processing, either for the deletion of personal data or for periodic verification, considering that data initially collected for specific purposes and subsequently subject to further processing for public interest archiving and historical research purposes may be retained for longer periods. Adequate technical and organizational measures will be implemented to protect the rights and freedoms of data subjects.

Principle 6: Integrity and Confidentiality
Personal data must be processed in such a way as to ensure adequate security, including the protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
The Academy ensures adequate security and confidentiality of personal data throughout the processing, identifying the technical and organizational measures to be implemented based on an approach based on risk analysis and management that affects the rights and freedoms of natural persons.

Principle 7: Accountability
The Data Controller is responsible for any personal data processing that has been carried out directly or by third parties on its behalf, and must be able to demonstrate compliance with the relevant regulatory requirements.
To this end, taking into account the nature, scope, context, and purposes of the processing, as well as the risk to the rights and freedoms of natural persons, the Academy implements technical and organizational measures to ensure an adequate level of security and manages the related evidence in order to demonstrate that the processing is carried out in accordance with current legislation and this Policy.

Principle 8: Protection of Data by Design and by Default
The Data Controller must, at the time of determining the means of processing and at the time of processing itself, implement appropriate technical and organizational measures to effectively implement the principles of data protection and to integrate into the processing the necessary safeguards to meet the security requirements provided for in current legislation and to protect the rights of data subjects. To this end, the Academy ensures that in the development, design, selection, and use of applications, services, or products that process personal data or process data to perform their functions, whether operated directly or by third parties, the principles and requirements of data protection are respected. In particular, the Academy ensures the adoption of adequate technical and organizational measures to ensure that only personal data strictly necessary for each specific processing purpose are processed by default.
In order to ensure that all data protection requirements are identified and addressed from the design of new systems or processes, or during the review or integration of existing systems or processes, the IT system administrator (Information Technology) cooperates with the Data Controller to assess the impact of any new use of technology on the security of personal data from the design and by default, so that personal data cannot be made accessible to an unlimited number of natural persons. Each review process must be approved before being implemented.

5. Organizational Model and Responsibilities

Anyone working for or with the Academy has the responsibility to ensure that the processing of personal data complies with the principles and guidelines defined in this Policy. In particular, the Academy has identified the following key roles and their responsibilities regarding the protection of personal data processing:

- **Data Controller:** The Data Controller of personal data is the Accademia nazionale dei Lincei. The functions and responsibilities of the Data Controller are attributed to the President, who is also the legal representative of the Institution. The Data Controller defines and approves general strategies regarding the protection of personal data, determining the purposes and means of processing and identifying the appropriate technical and organizational measures to ensure that processing is carried out in accordance with current legislation and that the Controller is able to demonstrate compliance.
- **Data Protection Officer (DPO):** The DPO was appointed in accordance with Articles 37-39 of the GDPR, by means of a provision by the Chancellor - Director General. The DPO, in the exercise of his functions, is directly accountable to the hierarchical level of the Data Controller, who, in turn, commits to systematically involving him in all matters relating to the protection of personal data, ensuring that he has the necessary resources to carry out his function independently. In particular, the DPO is responsible for the following tasks:
  - Informing and providing advice to the Data Controller, Data Processors, and all personnel in order to ensure that the personal data processing carried out on behalf of the Academy and the internal policies are in compliance with data protection regulations;
  - Monitoring compliance with Regulation (EU) No. 2016/679, the Code on national data protection (D.Lgs. n. 196/2003 and subsequent amendments), as well as the policies of the Data Controller, including the assignment of responsibilities, awareness and training of personnel participating in data processing and control activities;
  - Providing, if requested, opinions on the Data Protection Impact Assessment (DPIA) as required by Article 35 of the GDPR and monitoring its implementation;
  - Cooperating with the Data Protection Authority and acting as a point of contact with it for all matters relating to the processing of personal data, including the preliminary consultation required by Article 36 of the GDPR, and carrying out any consultations necessary in relation to any other matter;
  - Establishing a functioning system to provide timely and appropriate responses to requests from data subjects;
- **Data Processors:** The Data Processors are identified as the managers of the organizational areas of the Academy:
  - Manager of the Chancellor – Secretariat;
  - Manager of administrative and personnel services;
  - Manager of the Library.

  They are appointed by formal act by the Data Controller and are responsible for implementing, in accordance with the instructions provided by the Data Controller, the compliance measures required by current data protection regulations, including, by way of example and not exhaustive:
  - Registering the personal data processing relevant to their organizational area for inclusion in the Register of Treatments;
  - Identifying and appointing authorized data processors within the offices relevant to their organizational area and providing them with training;
  - Identifying and appointing system administrators where present within their organizational area;

    - Carrying out the risk analysis of processing activities within their area of responsibility and identifying the appropriate technical and organizational measures to mitigate these risks;
    - Carrying out the Data Protection Impact Assessment (DPIA) if a particular type of processing presents a high risk to the rights and freedoms of natural persons before proceeding with the processing;
    - Ensuring the identification of the service providers who will act as external Data Controllers to formalize the relevant appointment;
- **Authorized Data Processor:** The Authorized Data Processors are the natural persons who, by their role and activities, carry out manual or automated operations of processing personal data within the scope of their assigned organizational unit. To carry out these operations, the persons entrusted with the task must be authorized by the Data Processor by means of a specific appointment and receive the relevant instructions from them;
- **System Administrator:** The System Administrator is the natural person who carries out technical activities aimed at managing and maintaining applications and data processing systems, network and security devices, with specific access and/or intervention capabilities in the management, modification, assignment of user accounts, identification and authentication credentials. The System Administrator must be authorized by appointment by the Data Processor in whose organizational area technical activities are carried out to manage and maintain a personal data processing system or its components on computer systems.

6. Governance of the personal data processing system

In order to ensure the effective and efficient management of personal data processing in compliance with current regulations, the Academy has adopted the organizational model described in paragraph 5. Within this framework, the individuals involved in personal data processing are designated individually by formal act and are subsequently informed about the responsibilities, competencies, and limitations that the appointment entails.

6.1 Governance of the personal data protection system

To ensure compliance with current regulations, and to ensure an effective and efficient management of personal data processing, the Academy has adopted the organizational model described in paragraph 5. Within this framework, the individuals involved to varying degrees in the processing of personal data are designated individually by formal act and are simultaneously informed about the responsibilities, competencies, and limitations of the role.

6.2 Records of data processing activities

In order to demonstrate compliance with the GDPR, the Academy, through the Data Processors formally designated by it, maintains and updates the Register of Data Processing Activities. This register is a document for census and analysis of processing activities carried out by the Controller or the Data Processor, and its content must always reflect the actual processing activities. The Controller and the Data Processor will ensure that any modifications are promptly recorded in the register, in particular, in terms of methods, purposes, categories of data, and categories of data subjects, while keeping track of any subsequent changes.
The register model adopted by the Controller is attached to this Policy.
The register is maintained in written form, also in electronic format, and made available to the Data Protection Authority, if requested. It must contain verifiable data on both the date of its

establishment and the date of its last update. At the end of each solar year, a static extraction of the register in electronic format is carried out and archived in the Institution's document management system.

6.3 Analysis of risks related to the processing of personal data

The Academy carries out a risk assessment for each new processing, and also whenever there is a significant change in the context or means of processing, in order to identify and implement all the technical and organizational measures that allow to mitigate such risk. By **risk related to processing** is intended the risk of negative impacts on the rights and freedoms of data subjects. These impacts are analyzed through a formal assessment process, in which it is established whether the processing of data involves a risk or a high risk in terms of probability and severity, taking into account the nature, scope, context, purposes of the processing, as well as the technical and organizational measures that the Data Controller believes it can adopt to mitigate such risk. The risk analysis process implemented involves conducting the assessment at the planning stage by the organizational area responsible for the processing. The report of the risk analysis activity constitutes evidence of compliance and is archived in the document management system.

6.4 Data Protection Impact Assessment (DPIA)

When a type of processing may present a high risk to the rights and freedoms of natural persons, the Academy, as the Data Controller, carries out a Data Protection Impact Assessment (DPIA), consulting with the DPO before proceeding with the processing. This assessment will be carried out, in particular, whenever a new technology is introduced to evaluate its impact on personal data processed. To this end, the Academy defines and adopts a formal methodology for carrying out the DPIA in accordance with current regulations and reference standards and best practices. The DPIA is carried out by the organizational area responsible for the specific processing and is prepared according to the document outline attached to this Policy. The DPO provides, if requested, an opinion on the DPIA and monitors its implementation.
If the DPIA indicates that the processing may present a high risk that the technical and organizational measures implemented by the Controller are not able to mitigate, it is consulted in advance with the Data Protection Authority before proceeding with the processing. The report of the DPIA constitutes evidence of compliance and is archived in the document management system by the Data Processor responsible for the processing.

6.5 Security Measures

For each activity carried out, the Academy implements physical, technical, and organizational measures to ensure the security of personal data processed. This includes preventing loss, destruction, unavailability, unauthorized access, and alteration, both accidental and illegal, as well as ensuring compliance with this Policy, due to the actions of individuals, systems, or the physical work environment. The identification of the appropriate security measures to counter the risks determined by the aforementioned violations is carried out by the competent organizational area and the IT Services Unit in all cases where the processing is carried out with the aid of IT tools. Specifically, all organizational units must comply with the IT security policy approved by a directorial decree. Furthermore, the Academy adopts the minimum security measures defined by AgID (Italian National Agency for Digital Services). The IT Services Unit implements a specific procedure to test, verify, and regularly evaluate the effectiveness of the implemented security measures.
Finally, with regard to the disposal and/or reuse of electrical and electronic equipment used for its

institutional activities, which may contain personal data, the Academy adopts appropriate measures, even with the assistance of qualified third parties, aimed at preventing unauthorized access to the personal data stored in the aforementioned equipment, in line with the Provision by the Data Protection Authority No. 13 of October 2008. Specifically, in the case of reuse or recycling of equipment, the following will be evaluated:

- **Technical preventive measures**, such as encryption of individual files, groups of files, or entire volumes of data recorded on one or more devices of type hard disk or on portions of them (partitions, logical drives, file-system) implementing the functionalities of a so-called file-system encryption;
- **Technical measures for secure data erasure**, achievable with software programs, such as *wiping programs or file shredders,* or by formatting hard drives at low level, where possible.

In the case of disposal of equipment, the following will be used to destroy optical or magneto-optical storage media:

- Punching or mechanical deformation systems;
- Physical destruction or disintegration (used for optical media such as CD-ROMs and DVDs);
- High-intensity demagnetization.

6.6 Data Breach Management

A data breach or *data breach* is a security incident that, if not addressed adequately and promptly, can cause physical, material, or immaterial damage to natural persons, for example: loss of control over their personal data or limitation of their rights, discrimination, identity theft or usurpation, financial losses, unauthorized decryption of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social damage to the natural person. For this reason, the regulation stipulates that the Data Controller, within 72 hours of becoming aware of the breach, must notify the Data Protection Authority and, in case of high risk, also the data subjects, unless it can demonstrate that the breach does not pose any risk to the rights and freedoms of the data subjects. In compliance with this requirement, the Academy has established a specific process for managing a potential *data breach* that includes the following steps:

1. Identification and classification of the *data breach* event;
2. Identification of the cause(s) that led to the breach;
3. Risk analysis related to the breach;
4. Communication management with the Data Protection Authority and the data subjects;
5. Registration of all actions taken in the *data breach* register.

The registration of the breach, internal reports, and any notifications to the Data Protection Authority and the data subjects constitute evidence of the *data breach* management process.

6.7 Data Protection Training

The Academy, aware that the protection of personal data processing is a shared responsibility at the institutional level, ensures the planning and delivery of regular training sessions to all personnel. The training program, teaching materials, and attendance records constitute evidence of compliance and are properly retained.

6.8 Compliance Monitoring

To verify that an adequate level of compliance is achieved for all institutional processes in relation to current regulations and this Policy, an annual data protection compliance audit is carried out by

the organizational area responsible for the management and archiving of electronic data and documents, in collaboration with the DPO. Each audit will evaluate compliance with the principles and requirements established in this Policy regarding the protection of personal data, including:

- the assignment of responsibilities;
- raising awareness among those involved;
- training of personnel.

The effectiveness of the implemented operational measures for data protection will also be evaluated, investigating, among other things:

- the respect of the rights of data subjects;
- the management of any breaches that have occurred in the processing of data;
- the management of any complaints from data subjects;
- the level of understanding of data protection policies and information on the processing activities carried out;
- the accuracy of personal data stored;
- the compliance of the activities of the Data Processors;
- the adequacy of procedures for rectifying any deficiencies and breaches of personal data.

The audit report and the corrective action plan, which will be developed in collaboration with the DPO, constitute evidence of the monitoring activity carried out.

6.9 Informative

The Academy ensures compliance with the principle of transparency in the processing of personal data by providing data subjects with a comprehensive information notice for each processing carried out, in accordance with Articles 13 and 14 of the GDPR, prepared using simple and clear language. The information provided to the data subject regarding the processing of their personal data is provided at the time of data collection from the data subject or, if the data is obtained from another source, within a reasonable time, in accordance with the circumstances of the case.
The information provided at the time of data collection from the data subject is as follows:

- the identity and contact details of the Data Controller;
- the contact details of the DPO;
- the purposes and legal basis of the processing;
- any recipients or categories of recipients of personal data;
- the intention to transfer personal data to a third country or international organization, in accordance with Article 13, paragraph 1, letter f) of the GDPR;
- the period of retention of personal data;
- the rights of the data subject (request for access, rectification, erasure, limitation of processing, objection to processing, data portability, complaint to the Data Protection Authority);
- if the processing is based on the legitimate interest of the Controller or relates to special categories of personal data for which the data subject has provided consent, the right to withdraw consent at any time;
- the existence of an automated decision-making process, including profiling, as well as information on the logic used and the consequences of such processing for the data subject;
- whether the communication of personal data is a legal or contractual obligation of the data subject or a requirement for the execution of a contract in which the data subject is a party, as well as the possible consequences of not communicating the data.

If personal data collected for a specific purpose must be processed for further purposes (e.g., archiving for public interest or for historical research), the Academy will provide due notice to the data subject before proceeding with the processing.
Furthermore, if personal data are obtained from a third party, the information notice to the data subject will also specify the source from which the personal data originate and whether this source is publicly accessible. The responsibility for making the information notice available for various processing activities is the responsibility of the organizational area that carries out the processing. The text templates for the information notices are made available to all UOs within the document management system.
Information notices are provided in writing or by other means, including, if necessary, electronically. If requested by the data subject, the information can be provided orally, with certain identification of the data subject.

6.10 Consent

The Accademia nazionale dei Lincei, as a non-economic public entity, may process personal data without the consent of the data subject when processing is necessary for the performance of a task carried out in the public interest or connected to the exercise of public powers, as well as for complying with a legal obligation or executing a contract in which the data subject is a party.
If it is necessary to obtain and receive the consent of the data subject to legitimately proceed with a processing that falls outside the cases mentioned above, the Academy provides data subjects with a request for consent in a clear and easily accessible form, using simple and clear language, and keeps track of the consent provided by the data subject before initiating the processing. The responsibility for making the consent document available for processing is the responsibility of the organizational area responsible for the processing in question. The templates to be used for drafting the consent document, potentially integrated into the information notice on the processing, are made available in the document management system.
The consent document and its registration constitute evidence of compliance and are archived by the organizational area responsible for the processing in the document management system. If the consent is recorded via software applications, the custody of the records is carried out by the IT Services Unit.

6.11 Exercise of rights by data subjects

In accordance with Articles 15-22 of the GDPR, the Academy ensures that data subjects can exercise the following rights:

- the right to obtain confirmation of the existence or non-existence of personal data relating to them;
- the right to access their personal data and the information concerning the purposes of processing, the categories of personal data, the recipients or categories of recipients to whom the personal data are communicated, the retention period, where possible, the existence of an automated decision-making process, and the safeguards in place if personal data are transferred to a third country;
- the right to have inaccurate personal data rectified and to obtain the completion of incomplete data;
- the right to have data relating to them erased in accordance with Article 17 of the GDPR, taking into account the exceptions provided in the same article;

- the right to obtain the limitation of processing in the cases provided for in Article 18 of the GDPR;
- the right to be informed by the Controller of any rectifications, deletions, or limitations of processing made, unless this is impossible or would involve an undue burden;
- the right to receive their personal data in a structured, commonly used, and machine-readable format, and to obtain the direct transfer of their personal data to another Controller, if technically feasible;
- the right to object to the processing of their personal data at any time, for reasons relating to their particular situation, unless the Controller can demonstrate that it has overriding legitimate interests or grounds for carrying out the processing;
- the right to object to automated decision-making, including profiling;
- the right to withdraw consent at any time without prejudice to any obligations or exercised rights based on consent given prior to withdrawal;
- to lodge a complaint with the Data Protection Authority.

The Academy implements a process to ensure that it responds to requests from data subjects without undue delay and, at the latest, within one month of receiving the request. This period, in accordance with Article 12, paragraph 3 of the GDPR, may be extended by two months, if necessary, taking into account the complexity and the number of requests. The Academy will inform the data subject of this extension and the reasons for the delay within one month of receiving the request. If the Academy is unable to comply with the data subject's request, it will inform the data subject without delay and, at the latest, within one month of receiving the request, of the reasons for non-compliance and the possibility of lodging a complaint with the Data Protection Authority and pursuing legal action.

If the data subject's request is manifestly unfounded or excessive, particularly due to its repetitive nature, the Academy may:

a) charge reasonable costs taking into account the administrative costs incurred in providing the information or undertaking the action requested;
b) refuse to comply with the request.

Communications relating to the management of the data subject's rights, which are registered and archived in the Institution's document management system, constitute evidence of compliance.

6.12 Communication and dissemination of personal data

The Academy, as the Data Controller, communicates personal data to other Data Controllers who carry out processing for the performance of a task of public interest or connected to the exercise of public powers, based on legal or regulatory requirements. In the absence of such a requirement, the communication is made when it is necessary to carry out tasks of public interest or to perform institutional functions, and it may be initiated if a period of forty-five days has elapsed since the relevant communication to the Data Protection Authority, without the Authority having adopted a different determination of the measures to be taken to protect the interests of the data subjects.

Similarly, the dissemination of personal data, through the publication on the web of acts, documents, information, and data held by the Academy, is carried out exclusively based on legal or regulatory requirements, specifically falling within the obligations of publication for transparency or for other purposes (e.g., the legal advertisement of certain administrative acts). In complying with the obligations of publishing acts and documents containing personal data on the web, the Academy complies with the Guidelines for the processing of personal data carried out by

public bodies for the purposes of publication and dissemination on the web adopted by the Data Protection Authority on May 15, 2014.
Particular precautions and guarantees, to be implemented through the implementation of appropriate technical and organizational measures, are taken in the cases of online publication of archival documents and related search tools containing personal data, as outlined in paragraph 6.17 "Management of processing for archiving purposes, historical and scientific research" of this Policy, in accordance with the Guidelines of the European Archives Group (EAG) for the application of GDPR in the archival sector.

6.13 Transfer of data abroad

The Academy ensures that the transfer of personal data to countries outside the EU and international organizations is only carried out when those parties guarantee an adequate level of personal data protection. To this end, a process is provided to verify and formalize the specific guarantees of adequacy for each transfer of personal data abroad.

6.14 Processing of special categories of personal data and data relating to criminal convictions and offences

The Academy carries out the processing of special categories of personal data and personal data relating to criminal convictions and offences exclusively in the following cases, after a risk assessment and the implementation of appropriate and specific measures to protect the rights and freedoms of natural persons:

- the data subject has explicitly consented to the processing;
- the processing is necessary to fulfil specific obligations and exercise rights, both of the Controller and of the data subject, relating to labour law;
- the processing is necessary to protect the vital interests or the interests of another natural person, if the data subject is physically or legally incapable of giving their consent;
- the processing relates to personal data made publicly available by the data subject;
- the processing is necessary for the purpose of ascertaining, exercising, or defending rights in judicial proceedings or when judicial authorities exercise their judicial functions;
- the processing is necessary for a relevant public interest, including, according to Article 2 sexies of the Code on the protection of personal data: a) access to administrative documents and public access; b) granting, payment, modification, and revocation of benefits, concessions, grants, other emoluments and licenses; c) conferring honours and rewards; d) recognition of the legal personality of associations, foundations, and entities; e) ascertaining the requirements of honourability and professional competence for appointments, profiles of public authority, to offices and management positions in legal entities, as well as granting patronage, representation and admission to ceremonies and institutional meetings; f) enforcement and protection measures in administrative or judicial proceedings; g) treatments carried out for purposes of archiving in the public interest or historical research, concerning the conservation, organization, and communication of documents held in public archives or private archives declared to be of particular historical importance; h) establishment, management, and termination of employment relationships of any type, even unpaid or honorary, and other forms of employment; i) labour law, occupational and compulsory placement, social security and assistance, protection of minorities and equal opportunities in employment relations, payment

of wages, tax and accounting obligations, workplace health and safety […], ascertainment of civil, disciplinary, and accounting liability […];
- the processing is necessary for occupational health and safety purposes, or for the assessment of the employee's working capacity if such data are processed by or under the responsibility of a professional subject to professional secrecy.

6.15 Personal data protection by Data Processors (external)

The Academy ensures the management of compliance with current regulations on personal data protection in the context of managing suppliers and contractual arrangements:

- only using Data Processors who can provide sufficient guarantees regarding the implementation of technical and organizational measures to ensure that the processing is carried out in compliance with current regulations and this Policy;
- providing for and implementing specific security clauses and measures within data protection agreements within supply contracts.

The contracts signed with the clauses or data protection agreements signed by the parties constitute evidence of compliance and are archived in the Institution's document management system.

6.16 Processing for archiving purposes of public interest and historical research

The Academy processes personal data, including special categories of data as defined in Article 9 of the GDPR, for purposes of archiving in the public interest and historical research. This processing constitutes a legal obligation for the Academy (see Article 30, paragraph 4, Decree-Law No. 42/2004 and subsequent amendments) and is included among the processing activities of significant public interest, as defined in Article 2 sexies, paragraph 2, letter cc, of the Code on the protection of personal data (Decree-Law No. 196/2003 and subsequent amendments). These purposes of processing entail derogations from the principles of limitation of purposes and limitation of data retention, as well as from the rights of data subjects defined in Articles 15-21 of the GDPR. In accordance with Article 89 of the GDPR, the Academy, in these cases, adopts specific technical and organizational measures, in line with the principle of proportionality, to ensure the rights and freedoms of natural persons, in particular in order to ensure compliance with the principle of data minimization by default, including:

- elaborating the Data Retention Plan, which defines which types of files and archival series containing personal data must be selected for permanent retention at the Institution's Historical Archive, in accordance with its institutional mission;
- pseudonymization (reversible) of documents, search tools, and databases, if these purposes of processing can be pursued in this way;

[1] "Notwithstanding the provisions of paragraph 1, the public interest is considered relevant for processing carried out by entities that perform public functions or exercise public powers in the following areas: […] processing carried out for the purpose of archiving in the public interest or historical research, concerning the conservation, organization, and communication of documents held in state archives, in the historical archives of public entities, or in private archives declared to be of particular historical importance, for scientific research purposes, as well as for statistical purposes by entities that are part of the national statistical system (Sistan)."

- application of the regulations on the consultability of documents stored in the archives of public bodies, as provided for in Articles 122-127 [2] of the Code for cultural heritage and landscape;
- restrictions on access to the storage premises of physical archives;
- surveillance in the consultation areas available to users;
- registration of users;
- installation of virus and trojan protection software for digital archives;
- access via password to databases or the restricted area of the website, which is not indexable by search engines, in the event of online publication of documents and search tools containing personal data.

Among the specific measures recognized by national legislation (see Article 102 of Decree-Law No. 196/2003 and subsequent amendments) as a guarantee for the rights and freedoms of natural persons, the application of the **Ethical rules for processing for archiving in the public interest and historical research** is included, to which the Academy complies. Evidence of compliance includes the integration of the Ethical rules into the regulation for the consultation of the academic archive, as well as the signing of the same by the users of the archive upon submitting the request for access.

6.17 Profiling and automated decision-making

The Academy does not carry out automated processing of personal data, nor for decision-making purposes nor for profiling purposes. The navigation data of users of the institutional websites, acquired in the form of cookies, are used solely to improve the use of content and to realize aggregate statistics that do not personally identify the user.

6.18 Complaint Management

Data subjects who wish to lodge a complaint regarding the processing of their personal data must submit a written request to the DPO, sending it to the email address rpd@lincei.it.
An investigation will be carried out regarding the content of the complaint in a manner appropriate to the specific case.
The DPO will inform the data subject of the progress and outcome of the complaint within a reasonable timeframe. If the problem cannot be resolved through consultation between the data subject and the DPO, the data subject may, at their discretion, pursue legal action through mediation, binding arbitration, litigation, or a complaint to the Data Protection Authority.

[2] Specifically, documents containing sensitive data, as well as data relating to criminal proceedings expressly indicated in the regulations on the processing of personal data, become accessible forty years after their date. The term is seventy years if the data are suitable for revealing health information, sexual life, or confidential family relationships.

7. Approval and update of the Data Protection Policy

7.1 Procedures for approval and updating

Approval	Details
Approval body	Board of Directors
Data Protection Officer (DPO)	Davide Paciotti

Cronologia delle modifiche e revisioni	Dettagli
Data of approval	November 6, 2024

7.2 Entry into force of the document

The present Policy comes into effect from December 1, 2024.