UNIVERSITÀ DI PARMA

2022

REGULATION ON PROTECTION OF PERSONAL DATA

Automatically translated by DeepL

PERSONAL DATA PROTECTION REGULATION

Summary

DEFINITIONS

This is meant by:

1. processing **shall mean** any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic means, such as collection, recording, organisation, storageadaptation or alterationretrieval, consultation, usedisclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
2. **personal data shall mean** any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, reference in particular to an identifier such as a name, an identification number, location data, an online identifier or to one or more features of his physical, physiological, genetic, mental, economic, cultural or social identity;
3. **special categories of data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data capable of uniquely identifying a natural person, data concerning health or sexual life or sexual orientation;
4. **genetic data:** personal data relating to hereditary or acquired genetic characteristics of a natural person that provide unambiguous information on the physiology or health of that natural person, and which result in particular from the analysis a biological sample of that natural person;
5. **biometric data:** personal data obtained by specific technical processing relating to physical, physiological or behavioural characteristics of a natural person, which enable or confirm their unambiguous identification, such as facial image or dactyloscopic data;
6. **Health-related data:** personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's state of health;
7. **controller:** the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria applicable to its designation may be established by Union or Member State law;
8. **controller:** the natural or legal person, public authority, service or other external body that processes personal data on behalf of the controller;
9. **privacy contact person:** the person charge of the structures within which personal data are managed for institutional purposes, identified on the basis of the competences attributed to the organisational function or institutional office he/she holds, as defined in Article 10.1 of these regulations;
10. **privacy delegate: a** figure designated by the Privacy Officer to carry out operationally the tasks assigned to him/her and to interface with the DPO/DPO as defined in Article 10.2 of this Regulation;
11. **scientific responsible:** research holders, within the framework of national and international and assimilated figures as defined in Article 10.3 of these regulations;

12. **Privacy** Team: a group supporting the DPO/RPD and liaising with various articulations of the entity as defined in Article 7 of these regulations;
13. **digital transition : a** figure whose duties are defined by Article 17, paragraph 1-sexies of the Digital Administration Code (issued by Legislative Decree No. 82 of 7 March 2005, as resulting from the subsequent amendments and additions, including the latest supplementary and corrective provision of Legislative Decree No. 217 of 13 December 2017);
14. **person responsible for the preservation of computerised documents: a** figure whose duties are defined by Article 44 of the Digital Administration Code (issued by Legislative Decree No. 82 of 7 March 2005, as resulting from the subsequent amendments and additions, including the latest supplementary and corrective provision of Legislative Decree No. 217 of 13 December 2017);
11. **IT Security Officer:** head of the Organisational Unit that coordinates IT security activities in the University;
12. **authorised processors:** natural persons formally authorised and instructed to process personal data under the direct authority of the Controller and/or Privacy Officer and for the purposes established by the Controller (Articles 4, 29, 32, 39 of the EU Regulation);
13. **subject**: the natural person to whom the personal data refer;
14. **consent of the data subject:** any manifestation of the data subject's free, specific, informed and unambiguous will, whereby the data subject indicates his/her assent, by way of a statement or unambiguous affirmative action, that personal data relating to him/her be processed;
15. **third party:** the natural or legal person, public authority, service or other body other than data subject, the controller, the data processor, the Privacy Contact Person and the persons authorised to process personal data under the direct authority of the data controller or processor;
16. **recipient:** the natural or legal person, public authority, service or other body receiving communications of personal data, whether a third party or not. However, public authorities that may receive communications of personal data in the framework of a specific investigation in accordance with Union or Member State law are not considered recipients. The processing such data by these public authorities is in accordance with the applicable data protection rules according to the purposes of the processing;
17. **profiling:** any form of automated processing personal data consisting of the use of such personal data to evaluate certain personal aspects relating a natural person, in particular to analyse or predict aspects of that person's professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
18. **Pseudonymisation:** the processing of personal data in a way that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organisational measures to ensure that such personal data is not attributed to an identified or identifiable natural person;
19. **limitation of processing:** the marking of personal data stored with the aim of limiting their processing in the future;
20. **archive:** any structured set of personal data accessible according to specified criteria, regardless of whether that set is centralised, decentralised or functionally or geographically distributed;

21. **Data Protection Officer (DPO)**: is a figure provided for in Article 37 of Regulation (EU) 2016/679. It is an individual designated by the data controller or data processor to perform support and control, advisory, training and information functions in relation to the application of the GDPR.;
22. **processing activities register:** list, in paper or digital form, of the personal data processing activities carried out under one's own responsibility by the Controller and the Processor in accordance with their respective competences;
23. **data protection impact assessment:** a procedure to describe the processing, to assess its necessity and proportionality and to ensure the management of risks to the rights and freedoms of natural persons related to the processing of their personal data;
24. **personal data** breach**:** a breach of security leading accidentally or unlawfully to the destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed;
25. **main establishment:** as defined in Article 4(16) and Recitals 36 and 37 of the EU Regulation. In the case of a controller with establishments in more than one Member State, the place of its central administration in the Union, unless decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to order the implementation of those decisions, in which case the establishment which has taken such decisions is deemed to be the principal establishment;
26. **representative:** the natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27 of the EU Regulation, represents them in relation to their respective obligations;
27. **enterprise:** any natural or legal person, regardless of its legal form, engaged in an economic activity, including partnerships or associations regularly engaged in an economic activity;
28. **Enterprise group means** a group consisting of a parent company and the companies controlled by it;
29. **Binding Corporate Rules:** the personal data protection policies applied by a controller or processor established on the territory of a Member State to the transfer or set of transfers of personal data to a controller or processor in one or more third countries, in the context of a group of undertakings or a group of undertakings carrying on a common economic activity;
30. **supervisory** authority: the independent public authority established by a Member State pursuant to Article 51 of the EU Regulation: for Italy, the Garante per la protezione dei dati personali;
31. **cross-border processing:** processing of personal data which takes place in the course of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; processing of personal data which takes place in the course of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to affect data subjects

in more than one Member State;

32. **supervisory authority concerned: a** supervisory authority concerned with the processing personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of the supervisory authority are or are likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority;
33. **Relevant and reasoned** objection**:** an objection to the draft decision as to whether or not there is an infringement of this Regulation, or whether or not the action envisaged in relation to the controller or processor complies with this Regulation, which objection clearly demonstrates the relevance of the risks posed by the draft decision with regard to the fundamental rights and freedoms of data subjects and, where applicable, the free movement of personal data within the Union;
34. **international organisation:** an organisation and bodies governed by public international law subordinate to it or any other body established by or on the basis of an agreement between two or more States.

ARTICLE 1 - PRINCIPLES AND SCOPE

These Regulations, adopted in implementation of REGULATION (EU) 27 April 2016, No. 679 (hereinafter EU Regulation) and Legislative Decree No. 196/2003 as amended by Legislative Decree.
No 101/2018 (hereinafter the Personal Data Protection Code), regulates the protection of individuals in relation to the processing of personal data and the free movement of such data within the University of Parma
The University as data controller processes data with or without the aid of automated processes.
The data is processed with respect for fundamental rights and freedoms, the dignity of the person concerned and the right to protection of personal data.
The processing operations carried out by the University for the achievement of its institutional purposes do not require the consent of the data subject and are based on the condition set out in Article 6(1)(b)(e) of the EU Regulation.
The University considers the lawful, correct and transparent processing of personal data a priority action in order to establish and maintain a relationship of trust with students, staff and third parties.
All those who process personal data within University because they are expressly authorised to do so or in order to carry out the tasks proper to the structure to which they functionally belong, must carry out the processing in accordance with the personal data protection policy set out in these Regulations.

Personal data is processed by the University in application of the principles laid down in Article 5 of the EU Regulation.
In particular, the personal data are:

1. Treated in a lawful, fair and transparent manner with regard to the person concerned (lawfulness, fairness and transparency);
2. Collected for specified, explicit and legitimate purposes, and subsequently processed a manner not incompatible with those purposes (purpose limitation). A further

processing of personal data for archiving in the public interest, scientific or historical research or statistical purposes is not considered incompatible with the original purpose;

3. Adequate, relevant and limited to what necessary in relation to the purposes for which they are processed (data minimisation);
4. accurate and, if necessary, updated. Reasonable steps shall be taken to delete or rectify in a timely manner data that are inaccurate in relation to the purposes for they are processed (accuracy);
5. Retained in a form which permits identification of data subjects for no longer than the purposes for which they are processed: personal data may be retained for longer periods provided that they are processed solely for archiving purposes in the public interest, scientific or historical research or statistical purposes, subject to the implementation of appropriate technical and organisational measures required by the EU Regulation (retention limitation);
6. Processed in a manner that ensures adequate security of personal data from unauthorised or unlawful processing and from accidental loss, destruction or damage, including protection by appropriate technical and organisational measures (integrity and confidentiality).

Taking into account the state of the art, the costs of implementation, as well as the nature, context and purpose of the processing, the University shall adopt appropriate technical and organisational measures capable of demonstrating compliance with the principles set out in the preceding paragraph (accountability).

ARTICLE 2 - LEGAL BASIS OF PROCESSING

The University is a Public Administration within meaning of art. 1, c. 2 of Legislative Decree 165/2001 and subsequent amendments, pursues purposes of general interest, operates under administrative law and exercises public powers. Therefore, the processing of personal data in the exercise of its institutional tasks finds its lawfulness in the condition provided for by Art. 6(1) of the EU Regulation.

Processing must always be necessary for the pursuit of the purposes for which it is lawfully carried out (principle of necessity) and must not be detrimental to the fundamental rights and freedoms of natural persons (Art. 1(2) EU Regulation)'.

ARTICLE 3 - CIRCULATION OF DATA WITHIN THE UNIVERSITY

Access to internal data by the University's structures and employees is inspired by the principle of the free flow of information within the University and aimed at achieving institutional purposes.

The University shall organise information and data at its disposal by means of tools, including IT tools, designed to facilitate their access and use.

Access to personal data by the structures or employees of the University, connected with the performance of the activity inherent to their specific function, is fulfilled, subject to a formal request explaining the reasons, to the extent necessary

the pursuit of the institutional interest, without prejudice to the applicant's liability arising from the improper use of the data.

ARTICLE 4 - TYPES OF DATA PROCESSED BY THE UNIVERSITY

The University carries out, with appropriate measures and taking into account the state of art, the costs implementation, as well as the nature, object, context, and purpose of the processing, processing of personal data for the performance of its institutional purposes, as identified by legal, statutory and regulatory provisions, and within the limits imposed by the Data Protection Code, EU Regulation, and the and Measures of the Data Protection Authority.
The University carries out the processing of personal data provided for by legislative and regulatory provisions concerning, by way of example but not limited to:

1. Data, also of a particular nature, relating to subordinate, para-subordinate or self-employed staff, including persons whose employment relationship has ended or other staff working in various capacities at the University:
    a. competition/selection tests;
    b. labour relationship management; training and further education; research project management; research monitoring and evaluation; technology transfer activities;
    c. Welfare policies and the use of benefits; health and safety of people in the workplace; provision of fixed and mobile telephone service.
2. Data on students in the broadest sense, for all activities and modalities related to student status and graduates:
    a. orientation activities;
    b. delivery of entrance tests or verification of entry requirements;
    c. disbursement of path training e management of career (from matriculation to graduation);
    d. internship activities; job placement activities;
    e. fundraising, institutional communication and information, and community development activities;
    f. statistical surveys and evaluation of teaching;
    g. dissemination of the final paper or related elements; mentoring, assistance, social inclusion services
    h. services and activities for the right to education;
    i. disciplinary proceedings against students.

3. Data on teaching and research (including health-related research).

4. Data relating to management, third-party and/or cross-cutting activities:
    a. space management;
    b. station management;
    c. management of institutional bodies and offices;
    d. accident management;
    e. library services;
    f. protocol and document storage services;
    g. purchase of goods and services, conclusion of contracts, debt collection, management of the

litigation;
h. e-mail services and collaboration tools;
i. federated service delivery (e.g. Eduroam);
j. tracking of non-primary information for the correct and complete execution of the services offered to Users through the University's information systems.

5. It is the task of the Privacy Officers or their Privacy Delegates to carry out and document the periodic reconnaissance of processing operations.

6. In any event, all data processing operations carried out by the University of Parma, even if not included in the above list, which fall within the scope of the University's institutional tasks or which are prescribed by a law.

ARTICLE 5 - DATA CONTROLLER

The Data Controller is the University as a whole whose legal representative is the Rector pro tempore.
The University shall adopt appropriate technical and organisational measures in order to ensure and be able to demonstrate the compliance of the processing with the EU Regulation and the Personal Data Protection Code, taking into account the nature, scope, context, legal basis and purposes of the processing, as well as the risks having different probability and severity for the rights and freedoms of natural persons. These measures shall be periodically reviewed and updated.
In the case of the transfer of personal data to a third country or to an international organisation, the University is responsible for ensuring that specific conditions are met so that the level of protection of natural persons guaranteed by the EU Regulation is not prejudiced. The University cooperates with the Data Protection Authority.
The data controller, aware of the importance of adopting policies for the protection of personal data processed in the exercise of its institutional tasks, undertakes to carry out the processing in application of the principles of lawfulness, correctness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

ARTICLE 6 - CO-OWNER

When one or more data controllers determine jointly with University the purposes and means of the processing, they are joint data controllers.
The University and the Data Controller shall determine in a transparent manner, by means of an internal agreement, their respective obligations with regard to compliance with the EU Regulation, with particular regard to the exercise of the data subject's rights, and their respective functions in communicating the information required by the Privacy Policy, without prejudice to Article 26 of the EU Regulation.
The agreement adequately reflects the respective roles and relationships of the joint owners with the interested parties, even after the termination of the joint ownership relationship. The essential content of the agreement is made available to the interested party.

The data subject may exercise his or her rights vis-à-vis each data controller.

ARTICLE 7 - THE PERSONAL DATA PROTECTION OFFICER (RPD) OR DATA PROTECTION OFFICER (DPO)

The University appoints a Data Protection Officer (hereinafter DPO/DPO).
The DPO/DPO is a specialised figure in support of the Controller and performs the function of liaison with Data Protection Supervisor and guarantor for subjects.
The DPO/DPO is identified on the basis of his or her professional qualities, specialist knowledge of data protection law and practice and ability to perform the assigned tasks.
The DPO/DPO may be an internal (university employee) or external entity, in which case he/she performs his/her duties on the basis of a service contract.
The DPO/DPO is appointed, in the case of internal subjects, by decree of the Rector.
The DPO/DPO is required to perform the following tasks (in accordance Art. 39 of the EU Regulation):

1. informing and advising the data controller as well as the employees carrying out the processing about the obligations arising from this Regulation, the EU Regulation and EU and national data protection legislation;
2. monitor compliance with this Regulation, the EU Regulation and other provisions deriving from EU and national legislation, including the allocation of responsibilities;
3. provide guidance and cooperate with the Controller on training activities for personnel involved in processing and related control activities;
4. provide, if requested, an opinion on the data protection impact assessment and monitor its implementation;
5. cooperate with the Garante per la protezione dei dati personali and act as a point of contact with that authority for matters related to the processing, including prior consultation, reports of personal data breaches, cooperating with the controller for the possible submission of mandatory personal data breach notifications under the EU Regulation;
6. provide guidance drawing up and updating processing registers;
7. draw up an annual report of its activities.

In order to perform his tasks, the DPO/DPO is assisted by a *Privacy Team* composed at least:

- one representative per Executive Area and per Department (privacy delegate pursuant to Article 10.2 of these Rules);
- a representative of the IT Security OU with coordination functions;
- a representative of the Legal and Compliance OU.

Depending on the need, the DPO/DPO may make use of in-house expertise or outside the University.
In performing his tasks, the DPO/DPO duly considers the risks inherent in the processing, taking into account the nature, scope, context and purposes of the processing.
The DPO/DPO has wide access to information and is questioned for each

data protection issues and for any activity involving data processing, right from its design. To this end, the DPO/DPO must be invited to participate in coordination meetings of heads/departments and centres dealing with data protection issues.
The University ensures that the DPO/DPO exercises his or her functions autonomously and independently and, in particular, does not assign him or her activities or tasks that are in conflict or conflict of interest.
The DPO/DPO does not receive any instructions with regard to performance of the tasks entrusted to him/her pursuant to Article 39 of the EU Regulation.
The University does not remove or penalise the DPO/DPO by reason of the performance of his/her duties.
The name and contact details of the DPO/DPO are communicated to the Garante per la protezione dei dati personali. The DPO/DPO's contact details are included in privacy notices and published on the institutional website.
In order to perform the tasks referred to in paragraph 6 above, the administration shall set up in support of the DPO/DPO a network of Privacy Delegates, each of whom shall cooperate with the DPO/DPO within the structures in which personal data are managed for institutional purposes and on the basis of the competences attributed to the organisational function or institutional office they hold.
The DPO/DPO is guaranteed autonomy and resources to effectively perform the tasks assigned to him/her, in relation to the organisational size of the entity; in particular, resources are guaranteed for the acquisition of goods and/or services functional to the performance of the tasks and adequate working time for the performance of his/her function. He and the staff working with him shall also be guaranteed ongoing training to enable them to keep abreast of developments in the field of data protection.
On the instructions of the DPO/DPO, specific working groups may be set up on compliance with data protection legislation and for specific topics.

ARTICLE 8 - RESPONSIBILITIES OF TREATMENT OF PERSONAL DATA

A Data Processor is any external party who carries out, on the basis of a contract/convention or other legal act, the processing of personal data on behalf of the University and is jointly and severally liable with the University in the event of non-compliance.
The Data Processors are appointed by a legal act in accordance with national law and provide guarantees pursuant to Article 28(3) the EU Regulation, in particular with regard to the appropriate technical and organisational measures to enable compliance with the provisions of the Regulation.
The Processor may appoint by contract or other legal act sub-processors for specific processing activities, subject to the same contractual obligations that bind him/her to the University.
Should a sub-processor fail to fulfil his or her data protection obligations, the initial External Processor retains full responsibility towards the University for the fulfilment of the other Processor's obligations.

The Data Processor shall be liable to the University for the non-performance of the sub-processor, including for compensation for any damage caused by the processing.
The information to the data subject shall indicate the recipients or categories of recipients, including internal recipients, to whom the data are disclosed for processing.

ARTICLE 9 - AUTHORISATION TO PROCESS

All those who, in the performance of their duties, **access the personal data necessary for the pursuit of the purposes assigned to the organisational unit to which they belong are** considered authorised to process **the data**. Those who process data pertaining to the organisational unit to which they belong are deemed to be authorised to process data by virtue of their documented position in the organisational unit and are therefore obliged to comply with the provisions of this Article.
Persons authorised to process data receive appropriate training/information on data processing.
The authorised person processes personal data in compliance with the security measures provided by the University, which are designed to prevent the risk of destruction, loss, unauthorised access or unauthorised processing of personal data.
The authorised person is bound:

1. to maintain secrecy and the utmost confidentiality with regard to the activity performed and all information that has come to his knowledge during the activity performed;
2. not to disclose to third parties or disseminate by electronic means or otherwise any news, information or data learned in connection with facts and circumstances of which he has become aware in his capacity as designatee;
3. to attend the information and training seminars on personal data protection and to take the relevant final tests to verify learning;
4. promptly report to their office manager and to the Privacy Contact Person any anomalies, incidents, thefts, accidental loss of data, in order to activate, in cases where there is a serious risk for the rights and freedoms of individuals, the procedures for communicating data breaches to the Privacy Guarantor and to the persons concerned (data breach institution).

The authorised person is informed and aware that accessing and remaining in the company computer systems for reasons other than those for which he has been authorised for institutional and service purposes may constitute the offence of unauthorised access to information systems and may result in disciplinary sanctions, as well as expose the administration to damages, including reputational ones.
The authorised person undertakes to comply with the instructions, policies and regulations on IT security adopted by the University.
If the conditions set out in this Article are not met, those who, in the performance of their duties, accidentally acquire knowledge of personal data for which they do not have explicit authorisation to process or which do not pertain to the organisational unit to which they pertain, shall be regarded as third parties with respect to the administration itself, and as such shall comply with the prohibition to communicate and use the data, considering any processing thereof as unlawful.
The Controller prepares and keeps up-to-date documents to establish the specific data access permissions of each individual designated in relation to his or her position in the organisational chart.

Students who**,** by reason of their membership of a course of study and in the course of the same, find themselves, by way of example but not limited to

- carry out research for the drafting of the dissertation and/or other dissertations submitted for teaching evaluation;
- act in relation to activities functionally and substantially connected with the teaching and training activities of the University.

If the student, for the purposes of writing the dissertation, collects personal data belonging to the University, he/she must also take care to provide the interested parties with the information notice for the collection of data, using the appropriate model published in the privacy section of the University portal, compiled on the basis of the particularities and references to the processing to be carried out. In any event, in order to be able to prove that the thesis student has complied with the information and consent collection obligations, he/she must also submit the information notice model used and any consents collected, if necessary, to the administrative offices when filing the thesis title.

Also to be considered as authorised to process data **are trainees, interns, 150-hour collaborating students** and related figures, who, by reason of their status, **carry out their activities within the University**. It is therefore the University's responsibility to formalise and authorise the person to process data on account of the assignment or activity that he/she is going to perform.

If, on the other hand, the student acts as a collaborator, trainee or intern in a third party organisation, by virtue of an agreement between the latter and the University, it will be the host organisation that will have to train the student in the handling of data in its structure. This aspect must be agreed with the Organisation at the time the agreement is signed, together with the qualification that is to be attributed to the student hosted by the third party organisation.

ARTICLE 10 - DATA PROCESSORS

The following categories of data processors are identified in the University pursuant to Art. 29 the EU Regulation and Article 2m of Legislative Decree 101/2018:

1. Privacy Contacts
2. Privacy Delegates
3. The Scientific Officers

ARTICLE 10.1 - PRIVACY CONTACT PERSONS

The persons in charge of the structures within which personal data are managed for institutional purposes, on the basis of the competences attributed to the organisational function or institutional office they hold, are identified as Privacy Contact Persons.
Privacy Contact Persons are identified as follows:

- for activities falling within the remit of the Rector's Office: the Rector or his expressly designated delegate;
- for **administrative and management structures**: the **Director General** for the activities falling within the remit of the Directorate General and the **heads of** the directorates for their respective

activities of competence;

- for **teaching and research activities**: the **heads** of teaching and research **departments** and centres, **school presidents**, heads of other types of structures.
- in relation to the **Service Centres of the Departments**: the **Administrative Manager** the Service Centre or its delegate.

The Privacy Referees have task assisting the Data Controller in defining the purposes, processing methods and means to ensure compliance with European and national legislation on the processing of personal data, as well as with the relevant internal policies of the University, in the performance of the tasks set out in the following paragraph.

The Privacy Contact Person collaborates functionally with the DPO/DPO, operates with managerial autonomy within the scope of the competences entrusted to him/her and may delegate to his/her own privacy delegate (see art. 10.2 of these regulations) structured, lecturer or administrative technician, the tasks listed below in relation to his/her own structure and for the areas expressly defined:

1. supervise, monitor and ensure compliance with provisions of the applicable data protection regulations;
2. comply with and apply the provisions of these Rules;
3. update the privacy policy and related forms;
4. collaborate, for the parts falling within its competence, in the mapping of processing operations, in the census of databases and outsourced data processing, and in the implementation and updating of the processing register;
5. issue appropriate instructions on privacy information and security measures to the staff designated for processing;
6. ensure compliance with the security measures aimed at avoiding the risks, even accidental, of destruction or loss of data, unauthorised access or processing that is not permitted or does not comply with the purposes of collection;
7. ensure the constant monitoring of the fulfilments and activities carried out by authorised persons with particular reference to the management of data breach notification and privacy impact assessment;
8. provide timely feedback, for the processing within its competence, in the event of requests to exercise data rights, as provided for in Articles 15-22 of the EU Regulation;
9. ensure the performance of any other operation required or necessary to comply with the obligations deriving from the provisions of the law and/or regulations in force concerning the protection of personal data and cooperate with office in charge to identify the training needs of the resources of its structure;
10. compulsory participation in information/training and awareness-raising sessions on personal data protection;
11. notify the data controller and the DPO/DPO of any organisational change that may have an impact on the way the data are processed;
12. for processing operations that have consent as their legal basis, put in place organisational measures to ensure that the copy of the consent obtained, whether on paper or electronically, is kept by the structure authorised to process the data; keep, as far as it is within its competence, and make available upon request by the Data Controller or the DPO/DPO a copy of the following documentation
    - Agreements made with external managers;
    - Privacy Impact Assessment (DPIA) reports;
    - Assessments of processing based on legitimate interest;

- Data breach notifications;
- Informing data subjects of the processing carried out.

The delegation shall be formalised by a special deed, shall contain the delegated tasks and shall be accompanied by the relevant instructions. The Rector and the Data Protection Officer shall be notified of this delegation.

ARTICLE 10.2 - PRIVACY DELEGATES

The Privacy Delegate is appointed in writing by the Privacy Contact Person who gives him/her all the instructions necessary for the performance of his/her duties and aimed at compliance with the rules. In the event of termination or revocation of the appointment, the Privacy Contact Person shall notify the DPO/DPO's support office of the new appointment.
The list of Privacy Contact Persons and their Data Protection Delegates is communicated to the Rector and the DPO/DPO.

ARTICLE 10.3 - SCIENTIFIC OFFICERS

The Scientific Managers are the owners of research, within the framework of national and international and assimilated figures.
They process the data within the scope of their research project and are the contact persons for the work carried out and supervise the processing and protection of the data with regard to compliance with the EU and international regulations on the processing of personal data for statistical and scientific purposes and in accordance with the ethical rules and regulations adopted and approved by the data protection guarantor.
The Scientific Responsible is designated to the processing by the Controller when he/she carries out research activities proper to the University of Parma, also in the framework of national and international research activities.
Subjects belonging to the research group for a particular study must be authorised to process the data by the Scientific Officer himself.

ARTICLE 11 - SYSTEM ADMINISTRATORS

System administrators are the persons in charge of the operation and maintenance of a data processing system or its components; they are also Data Processors and are specially appointed.
The Provision of the Garante Privacy of 27 November 2008 (Measures and precautions prescribed for data controllers of processing operations carried out by electronic means with regard to the attribution of system administrator functions) considers various figures as System Administrators, : administrators, network and security equipment administrators, and administrators of complex software systems; these are roles that must be duly appointed and periodically verified.
Given the technical peculiarities, the System Administrator plays an extremely delicate role: he designs, develops and manages the network infrastructure, servers, software and basic application services, often dealing with security and protection of data and resources. It also provides technical (help desk) and IT support on software and hardware. When necessary, it plays a proactive role in data security breach notifications, notifying the DPO/DPO of any detected anomalies, malfunctions or security risks.

He is also responsible for the activities carried out and the consequences resulting from a malfunctioning of the network, and supports Data Processors and Authorised Officers for technical IT aspects in normal operations.
The data controller verifies the compliance of system administrators with the organisational, technical and security measures required by law for the processing of personal data.

ARTICLE 12 - AWARENESS-RAISING AND TRAINING

For the purposes of the correct and punctual application of the rules concerning the principles, the lawfulness of processing, consent, information and, more generally, the protection of personal data, the University supports and promotes, within its own organisational structure, every awareness-raising tool aimed at consolidating the awareness of the value of personal data protection. In this respect, University promotes training activities for university staff and information activities aimed at all those who have relations with the University.
Every year, after consulting the DPO/DPO, the University prepares a training plan on the processing of personal data and the prevention of the risks of violation, in order to ensure responsible, informed and up-to-date management of processing activities. The contents of the training plan shall take into account critical issues that have arisen in the previous year in relation to the application of this regulation, incidents concerning confidentiality, data integrity and availability, respect for the rights of the data subject, and new legislation, case law and practices that have occurred in the field of personal data processing. This training is coordinated with the training in computer security.
Each training session includes, with a view to empowerment, a final learning test.
Attendance at training activities is compulsory and is considered as an element in the measurement and evaluation of organisational and individual performance.

ARTICLE 13 - DISCLOSURE

For each type of data processing, the University shall provide information to the data subject, unless the data subject is already in possession of the information (Art. 13(4) of the EU Regulation) or in other special cases provided for in Art. 14(5) of the EU Regulation. The information provided to the data subject must be concise, transparent, intelligible, easily accessible and use exemplary clear language.
The staff and anyone working under the authority of the University may process personal data only for the specific purposes indicated in the information provided to the data subject at the time the data is provided or for any other purpose provided for by law.
Where personal data are to be processed for a purpose other than that for which they were collected, the University shall provide the data subject with information about the different purpose before such further processing.
If the data are not collected from the data subject, the University reserves the right not to provide the information if the data subject already has the information or if the provision of such information proves impossible or involves a disproportionate effort.

Information may not be provided where there is a risk of making it impossible or seriously prejudicing the achievement of the purposes of the processing.
In order to comply with the information obligation, in accordance with the principles set out above and for accountability purposes, the University of Parma makes available model information notices in the web space dedicated to Privacy.

ARTICLE 14 - CONSENT

Pursuant to Article 6(1)(c), (d), (e) of the EU Regulation, the University is not to request consent for the processing of personal data for all purposes relating to the University's institutional activities, to comply with legal obligations and for reasons of public security.
For purposes that do not fall within the institutional purposes, or for which the processing is made compulsory by legal provisions or for reasons of public security, the legal basis appropriate to the specific purpose for the processing is carried out must be assessed.
The Privacy Officer and the relevant Privacy Delegates define the legal basis of the processing within the framework of the system of treatment design, in compliance with the principles of 'privacy by design' and 'privacy by default'.
If the identified legal basis is consent (Art. 6(1)(a) of the EU Regulation), this must always be provided for:

1. a method of collecting consent that is suitable for demonstrating that the data subject has given his consent to the processing of his personal data;
2. a method enabling the person concerned to revoke consent at any time.
   moment, as easily as it was granted.

ARTICLE 15 - RIGHTS OF THE DATA SUBJECT

The University guarantees respect for the rights of data subjects as set out in Articles 12 to 22 of the EU Regulation.
In particular, the data subject may:

1. obtain confirmation of the existence or non-existence of personal data concerning him/her, even if not yet recorded, and their communication in intelligible form;
2. obtain access, rectification, deletion as well as object to the processing;
3. exercise the right to restriction of processing not only in the event of a breach of the lawfulness of the processing and as an alternative to deletion of the data, but also in the event of a request by the data controller to rectify the data or to object to processing. Under conditions of limitation and with the sole exception of storage, any other processing of the data is permitted only in the presence of the consent of the data subject, or establishment of rights in court, the protection of the rights of another natural or legal person, or in the presence of a significant public interest;
4. exercise the right to oppose profiling;
5. to exercise the right to data portability only if the processing is based on consent within the meaning of Art. 6. para. 1(a) or Art. 9(2)(a) of the EU Regulation or on a contract within meaning of Art. 6(1)(b) of the EU Regulation.

EU Regulation and is carried out by automated means. This right shall not apply to processing necessary for the performance of tasks carried out in the public interest or in connection with the exercise of official authority vested in the University;

6. Exercise the right to be forgotten by requesting the deletion of one's personal data if they have been made public online. This right may be exercised in any of the following cases:
    a. personal data are no longer necessary in relation to the purposes for which they were collected;
    b. the data subject revokes the consent on which the processing is based;
    c. the data subject objects to the processing and there is no overriding legitimate reason to proceed with the processing;
    d. personal data are unlawfully processed;
    e. fulfilment of a legal obligation;
    f. the data concern minors.

The University shall inform any other data controller processing the deleted personal data, including any linking, copying or reproduction, of the request for deletion.

The data subject may exercise his or her rights by means of a written request addressed to the person charge of the structure responsible for the management of the personal data that are the subject of the request and, alternatively, to the Privacy Contact Person or his or her Privacy Delegate.

Acknowledgement of the data subject's requests is regulated by a dedicated procedure, "Procedure for the management of the data subject's rights", in compliance with the following principles: acknowledgement is provided by the Privacy Contact, without undue delay, within 30 days from the date acquisition of the request at the Protocol, even in cases of refusal. For cases of particular and proven difficulty, the 30-day period may be extended up to 3 months, which cannot be further extended. The interested party is informed of this extension within one month of the acquisition of the request at the Protocol.

The feedback provided to the interested party must be concise, transparent and easily accessible, expressed in plain and simple language.

The University facilitates, through the Privacy Contact Persons or their Privacy Delegates, the exercise of the rights by the data subject, adopting all necessary technical and organisational measures.

The exercise of rights is, in principle, free of charge for the data subject.

If requests are manifestly unfounded, excessive or repetitive in nature, the University may charge a reasonable fee taking into account the administrative costs incurred, or it may refuse to comply with the request by demonstrating the manifestly unfounded or excessive nature of the request. The Administrative Council establishes the criteria for defining the method of payment and the amount of the expense contribution by the interested parties.

The forms for exercising the above-mentioned rights are drawn up and updated by the Privacy Officers or their Data Protection Officers, who must adopt organisational solutions for the management of the requests and may rely on the support of the DPO/DPO in the most complex cases.

Requests by data subjects to exercise their rights are entered in a Register no later than 30 days after conclusion of the proceedings.

In cases of outsourced data processing, the External Manager is required to cooperate with the University.

ARTICLE 16 - TREATMENT OF SPECIAL CATEGORIES OF

PERSONAL DATA

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, as well as the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sex life or sexual orientation, (hereinafter also only 'special categories of personal data' as identified by Art. 9 EU Regulation) is prohibited, except in the following cases:

1. the data subject has given his or her explicit consent to the processing of such personal data for one or more specific purposes;
2. processing is necessary for the purposes of fulfilling the obligations and exercising the specific rights of the data controller or the data subject in the field of labour law and social security and social protection, pursuant to Article 19 of this Regulation;
3. processing is necessary to protect a vital interest of the data subject or another natural person where the data subject is physically or legally incapable of giving consent;
4. the processing concerns personal data made manifestly public by the data subject;
5. processing is necessary for the establishment, exercise or defence of legal claims;
6. processing is necessary for reasons of substantial public interest within the meaning of Article 2-sexies of the Personal Data Protection Code, if provided for by European Union law or by provisions of law, regulation or general administrative acts. Processing carried out in the following matters is considered to be of substantial public interest:
    - access to administrative documents and civic access;
    - granting, liquidation, modification and revocation of economic benefits, facilities, handouts, other emoluments and entitlements;
    - relations between public actors and third sector entities;
    - conscientious objection;
    - sanctioning and protection activities in administrative or judicial proceedings;
    - institutional relations with religious bodies, religious denominations and religious communities;
    - tasks of the National Health Service and those working in the health sector, as well as tasks relating to hygiene and safety in the workplace and the safety and health of the population, civil protection, protection of life and limb;
    - planning, management, control and evaluation of health care, including the establishment, management, planning and control of relations between the administration and entities accredited or contracted with national health service;
    - social protection of maternity and voluntary termination of pregnancy, addictions, care, social integration and rights of the disabled;
    - education and training at school, vocational, higher or university level;
    - Establishment, management and termination, of employment relationships of any kind, including unpaid or honorary, and other forms of employment, trade union material, employment and compulsory employment , social security and

assistance, protection of minorities and equal opportunities in labour relations, fulfilment of remuneration, tax and accounting obligations, protection of the University's information assets, hygiene and safety at work or health and safety of the population, ascertainment of civil, disciplinary and accounting liability, inspection activities.

Genetic, biometric and health-related data may only be processed in accordance with the safeguards laid down and adopted by order of the Data Protection Authority.
Such data may not be disseminated. may be used in compliance with the guarantees of referred to Article 2_septies of the Code.

ARTICLE 17 - PROCESSING OF PERSONAL DATA RELATING CRIMINAL CONVICTIONS AND OFFENCES

The processing of personal data relating to criminal convictions and offences or related security measures is permitted if authorised by a rule of law or, in cases provided for law, by regulation, pursuant to Article 2-octies of the Personal Data Protection Code and EU Regulation.
In particular, it is allowed in the following cases:

1. fulfilment of obligations and exercise of rights by the Data Controller or the data subject in the context of employment relationships, within the limits laid down by laws, regulations and collective agreements, in accordance with Articles 9(2)(b) and 88 of the Regulation;
2. Fulfilment of obligations under statutory or regulatory provisions concerning mediation for the settlement of civil and commercial disputes;
3. verification or ascertainment of the requirements of good repute, subjective requirements and disqualification prerequisites in cases provided for by laws or regulations;
4. ascertaining liability in connection with accidents or events affecting human life, within the limits of the relevant laws or regulations;
5. establishment, exercise or defence of a right in court;
6. Exercise of the right of access to administrative data and documents, within the limits of the relevant laws and regulations;
7. fulfilment of obligations provided for by legal provisions on anti-mafia communications and information or on the prevention of mafia-type delinquency and other serious forms of social dangerousness, in the cases provided for by laws or regulations, or for the production of the documentation required by law for participation in tenders;
8. Verification of the moral suitability of those wishing to participate in tenders, in compliance with the provisions of current procurement regulations;
9. fulfilment of obligations under current legislation on the prevention of the use of the financial system for the purpose of money laundering and the financing of terrorism.

ARTICLE 18 - ACCESS TO ADMINISTRATIVE DOCUMENTS AND ACCESS

CIVIC

The limits for the exercise of the right of access to administrative documents containing personal data and for the exercise civic access remain governed respectively by Law No. 241 of 7 August 1990, as amended, and by Legislative Decree No. 33 of 14 March 2013, as amended, and by the University's implementing regulations on the subject.
Where the processing relates to special categories of personal data, access is permitted if the legally relevant situation that is to be protected by the request for access to administrative documents is of at least equal rank to the rights of the data subject, i.e. it consists in a right of personality or another fundamental right or freedom.

ARTICLE 19 - COMMUNICATION AND DISSEMINATION OF PERSONAL DATA

The communication and dissemination of personal data, excluding data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data intended to uniquely identify a natural person, data relating to a person's health or sexual life or sexual orientation, data relating to criminal convictions and offences, are permitted when

1. are provided for by law, or, in the cases provided for law, regulation or general administrative acts, pursuant to Article 2-ter of the Privacy Code, or, when it is in any case necessary for the performance of a task carried out in the public interest or for the exercise of public powers vested in the University;
2. are necessary for scientific research or statistical purposes and the data are anonymous or aggregated;
3. are required for purposes of defence or state security or for the prevention, detection or prosecution of criminal offences, subject to compliance with the rules governing the matter;
4. are necessary for the fulfilment of access requests to Article 18 of these regulations.

Requests by private persons and public economic entities for the disclosure of data must be made in writing and must state the reasons for the request and must contain

1. the name, denomination or company name of the applicant;
2. an undertaking to use the data exclusively for the purposes for which they were requested and in the manner indicated.

The University, in the person of Privacy Contact Person or his/her Privacy Delegate, shall assess, on the basis of the provisions of the applicable data protection regulations and of provisions of these Regulations, any requests for communication or dissemination of personal data to private parties and shall decide on the appropriateness of the communication.
The manner in which this data is communicated, for which a fee may be charged to cover the costs incurred, is decided by the University.
In order to foster institutional communication, the University may communicate to other public administrations and disseminate, also on its own websites, the names of its staff and collaborators, their roles, telephone numbers and institutional telematic addresses.

The University may communicate to public and private entities the data necessary for the management of the employment relationship, relating to personnel transferred, seconded or otherwise assigned in service to an entity other than the one to which they belong.
The University, in order to facilitate orientation, training and professional experiences and possible placement in the world of work, also abroad, may communicate, also on request of private subjects and by telematic means, data and lists concerning students, graduates, undergraduates and graduates, specialists, scholarship holders, doctoral students, assignees, and other training profiles, as well as of subjects who have passed the state exam. The purpose must declared in the request and the data may only be used for the purposes for which they were communicated and disseminated.
The university may also disclose to funders of doctoral scholarships and , including foreign ones, common data on doctoral students and post-doctoral fellows who have benefited from funding.
In view of the system of self-evaluation, accreditation and periodic evaluation of study courses defined by the MIUR, the University may process and/or communicate students' opinions on teaching to the bodies appointed to carry out checks on the quality of teaching such as the Evaluation Board or the Quality Presidium. These data are processed for the purpose of defining actions aimed at improving the quality of teaching.
The University may communicate, to the Hospital Agencies in agreement, data concerning the University's personnel working within the framework of the agreement with these Agencies.

ARTICLE 20 - TREATMENT WITHIN THE EMPLOYMENT RELATIONSHIP

The University processes employees' personal data in the context of the employment relationship by adopting appropriate safeguards to ensure the protection of the fundamental rights and freedoms of individuals and in compliance with the law and collective agreements.
The processing of employee data by the University does not require explicit consent as the processing is necessary to fulfil the obligations and exercise the specific rights of the data controller or data subject in the field of labour law and social security and social protection.
The University guarantees employees the exercise of the rights provided for in Articles 2 to 22 of the EU Regulation, including the right of access to evaluation data of a subjective nature, as well as the right to information.
The University adopts appropriate technical and organisational measures to ensure the protection of individuals' fundamental rights and freedoms, including individual and trade union prerogatives as provided for by Italian law, in particular by the Workers' Statute and by the rules that refer to it, as well as by the deontological rules promoted by the Garante for the protection of personal data.
The university may communicate to public and private entities common data of personnel who, due to a specific professional quality, benefit from training courses fomented in agreement with other public entities, with the aim of improving the usability and ensuring the quality and effectiveness of training in the country.
The University communicates the data of the personnel in charge of safety at work to

public and private entities that contribute to training on these issues.
In cases of receipt of curricula spontaneously transmitted by interested parties for the purpose of establishing an employment relationship, information is provided to the interested party at the time of the first useful contact, following the sending of the curriculum.
Consent to the processing of personal data in curricula is not required when the processing is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at the data subject'request.

ARTICLE 21 - COMMUNICATION AND DISSEMINATION OF DATA RELATED TO STUDY AND RESEARCH ACTIVITIES

In order to promote and support research and collaboration in science and technology, the University may communicate and disseminate, including to private individuals and by telematic means, data (with the exception of the data referred to in Articles 16 and 17 of these Rules) graduates, PhDs, technicians and technologists, researchers, lecturers, experts and scholars participating in study and research activities.
The data referred to in the preceding article do not constitute administrative documents within the meaning of Law No. 241 of 7 August 1990 and may be processed only for the purposes for they are communicated or disseminated.
The University may disclose any information concerning scientific productivity, awards and funds acquired by individuals, groups or specific scientific-disciplinary fields, including within the framework of procedures for assessing applications funding or research projects, in order to

1. Promote models for programming research activities and allocating resources according to mechanisms that ensure transparency in the definition of priorities, make appropriate use of the capacities of individuals and groups, and respect the principles of transparency and fair treatment;
2. fostering cooperation between individuals and groups through precise knowledge of achievements, in order to improve the ability to attract external funding or to establish structured collaboration with third parties;
3. provide guidance and support for the development of organisational models to support research, including benchmarking and the sharing of good practices.

The university may disclose personal data to public entities that have provided research funding, for reporting purposes and to enable statistical processing.

ARTICLE 22 - DISSEMINATION OF EXAMINATION ASSESSMENTS

In compliance with the principles of transparency by which the University is inspired and in order to improve the effectiveness and efficiency of administrative action, the publication of data concerning examination assessments is also allowed on the University websites.
The publication of data on websites is only permitted through the dissemination of the student's matriculation number and grade obtained, while respecting fundamental rights and freedoms, the dignity of the person concerned and the right to protection of personal data.

Evaluations are made available for a period of time not exceeding three months.

ARTICLE 23 - CIRCULATION OF RESULTS OF COMPETITIONS AND SELECTIONS

In compliance with the principles of transparency by which the University is inspired, the publication of the results of competitive and selective tests, as well as the relevant rankings, is also allowed on the University websites.
The publication of data on websites is carried out in compliance with the principle of data minimisation, by disseminating only the data strictly necessary to achieve the purposes for which they are published.
In the case of the dissemination of evaluations on the University websites, this information is published for a period of time not exceeding six months.

ARTICLE 24 - PROCESSING FOR THE PURPOSE OF ARCHIVING IN THE PUBLIC INTEREST OR HISTORICAL RESEARCH

Documents containing personal data that are processed for archiving purposes in the public interest or for historical research may only be used, taking into account their nature, if they are relevant and indispensable for the pursuit of those purposes.
The processing of personal data for the purpose of archiving in the public interest or historical research is carried out by ensuring compliance with the principle of data minimisation.
Where possible and without jeopardising the achievement of the purposes of the processing, the data must be processed using technical measures that no longer allow the data subject to be identified.
Personal data collected for archiving purposes in the public interest or for historical research may not be used to adopt administrative acts or measures unfavourable to the data subject, unless they are also used for other purposes in accordance with the principles laid down in Article 5 of the EU Regulation.
The processing of personal data for the purposes of archiving in the public interest or historical research is carried out in compliance with the relevant deontological rules approved by the Garante per la protezione dei dati personali.
Consultation of documents of historical interest kept in the University archives is governed by legislative decree no. 42 of 22 January 2004, by the relevant deontological rules and by the relevant University Regulations.

ARTICLE 25 - PROCESSING FOR STATISTICAL OR SCIENTIFIC RESEARCH PURPOSES

The processing of personal data for statistical or scientific research purposes by anyone working within University offices and structures or on behalf of the University itself must be carried out in compliance with the following principles:

1. Personal data processed for statistical or scientific research purposes may not be used to take decisions or measures concerning the data subject, nor processed for other purposes;

2. the data subject must be provided with timely information regarding the statistical or scientific research purposes of the processing pursuant to Article 13 of these Rules, unless this requires a disproportionate effort compared to right protected and provided that the appropriate forms of publicity identified by the relevant deontological rules, promoted by the Garante, are adopted.

Outside the cases of special surveys for statistical or scientific research purposes provided for by law, the data subject's consent to the processing of special categories of personal data, when required, may be given in a simplified manner, identified by the deontological rules referred to Article 106 or by the measures referred to Article 2-septies of the Personal Data Protection Code.

ARTICLE 26 - TREATMENT FOR MEDICAL, BIOMEDICAL AND EPIDEMIOLOGICAL RESEARCH PURPOSES

The consent of the data subject is not required for the processing of data relating to health, for the purposes of scientific research in the medical, biomedical or epidemiological fields, when the research is carried out on the basis of provisions of law or regulation law, including when the research forms part of a biomedical or health research programme provided for under Article 12-bis of Legislative Decree No 502 of 30 December 1992, and an impact assessment is conducted and made public pursuant to Articles 35 and 36 of the EU Regulation. Consent is also not required where, for special reasons, informing the data subject would be impossible or would involve a disproportionate effort, or where there is a real risk of making it impossible or seriously prejudicing the attainment of the research objectives. In such cases, the Scientific Research Manager takes appropriate measures to protect the rights, freedoms and legitimate interests of the data subject. The research project must be subject to prior consultation with the Data Protection Supervisor.

In the event of the data subject exercising his or her right to rectification and supplementation of personal data, the rectification and supplementation of the data shall be noted without changing the data, where the result of such operations does not significantly affect the result of the search.

For the further processing by third parties of personal data for scientific research or statistical purposes, the provisions of Article 110-bis of the Personal Data Protection Code apply.

ARTICLE 27 - SAFETY

The University implements appropriate technical and organisational measures to ensure a level of security appropriate to the likely risk to the rights and freedoms of natural persons arising from the processing of personal data.

In assessing the appropriate level of security, the University shall take into account the risks arising in particular from the destruction, loss, alteration, unauthorised disclosure of or access, whether accidental or unlawful, to personal data transmitted, stored or otherwise processed.

Each Privacy Officer (in relation to the processing operations falling within his or her competence), before starting a new processing operation or modifying an one, carries out the

assessment of the risks associated with the processing itself and submits it for evaluation by the DPO/DPO staff, who provide an opinion and suggest possible corrective measures.
The Privacy Officer then takes appropriate security measures to reduce the risks identified.
The main measures include:

1. pseudonymisation and encryption of data;
2. data minimisation;
3. the implementing measures of confidentiality, integrity, availability of information;
4. the resilience of processing systems and applications and their timely recovery in the event of a physical or technical incident;
5. a procedure for regularly testing, verifying and evaluating the effectiveness of technical and organisational measures to ensure the security of processing;
6. the correct management of authorisations and access credentials;
7. tools to verify the security of the devices on which the data are processed.

The technical measures are periodically reviewed through audits by the IT Security Organisational Unit and are explained in training sessions.
The University considers the transport of personal data on any medium (laptops, hard copies, pendrives, etc.) to be risky. This applies primarily to special categories of data, large volumes of personal data and information that entail particular risks for the data subject in the event of loss or destruction. Only in exceptional circumstances may such data be transported outside university premises and under direct responsibility of authorised personnel. In particular, authorised personnel are required to:

1. where possible make use of remote access via login and password to the information stored on secure systems identified by the University;
2. transport only the minimum amount of personal data;
3. ensure that mobile devices (e.g. laptops, tablets, etc.) and external storage devices used for transporting personal data outside university premises are equipped with encryption systems.

Any loss and/or theft of data must be promptly reported and dealt with in accordance with the data breach management procedure set out in Article 30 of these regulations.
For all matters not expressly regulated by this article on security, reference is made to the provisions of the sectoral University regulations, in particular those issued in compliance with the provisions of the Programmatic Security Document and the "Minimum ICT Security Measures for Public Administrations" prepared by AgID, Agenzia per l'Italia Digitale.

ARTICLE 28 - REGISTER OF PROCESSING ACTIVITIES

The University shall establish and update a register of processing activities carried out its responsibility.
The Register records the processing activities carried out by the offices and structures of the University and the main features of the processing operations. The Register is constantly managed and updated by the Privacy Referents and/or Delegates and, upon request, made available to the Data Protection Authority.
In addition to the register, documentation supporting the decision-making process for each individual treatment is filed and managed by the Privacy Referees and/or Privacy Delegates.

The Register lists and describes both the processing operations of which the University is the Controller and the processing operations that the University carries out as the External Manager of other Controllers.

The Register of Processing Operations for which the University is the Controller contains the following information:

1. the name and contact details of the University, DPO/DPO, the Privacy Contact Persons and their Privacy Delegates;
2. the structures responsible for treatment;
3. the purposes of the processing;
4. the legal bases of the processing;
5. the description of the categories of data subjects, as well as the categories of personal data;
6. the categories of recipients to whom the personal data have been or will be disclosed;
7. the possible transfer of personal data to third country or international organisation;
8. the time criteria for data retention;
9. where possible a reference to the technical and organisational security measures adopted for the processing.

The Register of processing operations carried out by the University on behalf of other Data Controllers and for which the University as Data Controller contains the following information:

1. the name and contact details of the University and the DPO/DPO;
2. the categories of processing carried out on behalf of each data controller;
3. transfers of personal data to a third country or international organisation, including identification of the third country or international organisation and, for transfers referred to in the second paragraph of Article 49 of the EU Regulation, documentation of appropriate safeguards;
4. a reference to the technical and organisational security measures adopted for the processing.

ARTICLE 29 - PRIVACY BY DESIGN, PRIVACY BY DEFAULT PRIVACY IMPACT ASSESSMENT

On the occasion of organisational and technological changes involving the processing of personal data - both in the case of processing already in place and in the case of new processing, as better described in the following paragraphs - the application of the principles of 'privacy by design' and 'privacy by default' (ex Article 25 of the EU Regulation) must be verified. This verification will proceed, first and foremost, by considering the nature, object, context and purpose of the processing and the use of new technologies. The DPO's staff will provide a specific methodology to carry out the aforementioned analysis and design of the processing tools. If the analysis shows that such profiles determine a high risk for the rights and freedoms of natural persons, before designing the processing tools, the Privacy Officer or his Privacy Delegate, in cooperation with the DPO staff and after consultation with the DPO/DPO, carries out, before proceeding with the processing, a personal data protection impact assessment (ex art. 35 of the EU Regulation). The assessment is conducted by applying a specific procedure, adopted by the DPO's staff, the results of which will be evaluated by the DPO himself. Subsequently, the design of the tools will take into account the results of the impact assessment. A single impact assessment may be conducted for a set of similar processing operations presenting similar high risks.

In particular, the Privacy Officer or his Privacy Delegate must take into account that a data protection impact assessment is mandatory in the following cases:

1. a systematic and comprehensive assessment of personal aspects relating natural persons, which is based on automated processing, including profiling, and on which decisions based that have legal effects or significantly affect them in a similar way;
2. the processing, on a large scale, of special categories of personal data such asracial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data intended to uniquely identify a natural person, data concerning a person's health or sexual life or sexual orientation, data relating to criminal convictions and offences;
3. large-scale systematic surveillance of an area accessible to the public (video surveillance);
4. the processing of data for the purposes of medical, biomedical or epidemiological scientific research;
5. or if two of the conditions set out in the EDPS Impact Assessment Guidelines are met.

The Privacy Officer or his/her Privacy Delegate shall also consult with the DPO/DPO and his/her staff to take the decision whether or not to carry out the impact assessment. This consultation and the consequent decisions taken by the Privacy Officer or his/her Privacy Delegate must be documented in the Impact Assessment. The Privacy Officer or his/her Privacy Delegate, in cooperation with the DPO's staff, is required to document the reasons in the event he/she adopts conduct that differs from that recommended by the DPO. In the event that, after the DPIA has been carried out, the Privacy Contact Person decides to carry out the processing, notwithstanding the DPO's negative opinion, the authorisation to process must be assumed by the Data Controller.

The Chief Digital Transition Officer provides support to the Privacy Contact Persons or their Privacy Delegates and the DPO/DPO in conducting the privacy impact assessment.

Privacy Delegates must cooperate in conducting the impact assessment by providing any necessary information and documentation.

The University, through the DPO/DPO, consults the Data Protection Authority before processing if the findings of the impact assessment (DPIA) conducted indicate the existence of a high residual risk.

The University, through the DPO/DPO, consults the Garante per la Protezione dei dati personali (Data Protection Authority) also in those cases where the legislation in force establishes the obligation to consult and/or obtain the prior authorisation of the same authority, for processing carried out for the performance of public interest tasks, including processing related to social protection and public health. In particular, consultation is mandatory where consent is not required for the processing of data relating to health, for purposes of medical, biomedical or epidemiological scientific research.

ARTICLE 30 DATA BREACH

A personal data breach is defined as a security breach that accidentally or unlawfully results in the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. A personal data breach may compromise the confidentiality, integrity or

availability of personal data.
The main risks to the rights and freedoms of natural persons resulting from a breach, in accordance with recital 75 of the EU Regulation, are:

1. physical, material or immaterial damage;
2. limitations of rights;
3. discrimination;
4. identity theft or usurpation;
5. financial losses;
6. damage to reputation;
7. loss of confidentiality of personal data protected by professional secrecy;
8. unauthorised decryption of pseudonymisation.

In order to protect people, data and information and to document the flows for the management of breaches of processed personal data, the University as Data Controller defines a procedure for the management of personal data breaches (*Annex Data Breach Management Procedure)*.
This procedure applies to any activity carried out by the University with particular reference to all archives and/or paper documents and to all information systems through which personal data are processed, even with the support of external suppliers.
The procedure defines the methods for identifying the breach, analysing the causes of the breach, defining the measures to be taken to remedy the personal data breach, mitigating its possible negative effects, recording information on the breach, identifying corrective actions and assessing their effectiveness, notifying the personal data breach to the EDPS if the breach poses a risk to the rights and freedoms of natural persons, and communicating a personal data breach to the data subject if the risk is high.
The procedure is made available via the University intranet.
The procedure is one of the subjects covered by the staff training referred to in Article 12 of these regulations.
Anyone who becomes aware, directly and/or indirectly (on the indication of an appointee, a University employee and/or a third party) of a possible personal data breach (even if only suspected) - regardless of the possible source/origin of such breach (third party, University staff, unidentified source, accidental event) - must immediately notify the RDP/DPO and the Privacy Contact Person of such possible breach through the channels indicated in the *Data Protection Management Procedure*.
The DPO/DPO requests from the Information Systems Area a technical report concerning the breach, which must be received within 36 hours from the request signed by the Privacy Contact or his Privacy Delegate. Any delays must be justified.
The DPO/DPO carries out the investigation of the breach taking into account the technical report provided and proposes to the controller to notify the personal data breach to the Garante if the breach entails a risk for the rights and freedoms of natural persons, and to notify a personal data breach to the data subject if the risk is high.
If technically possible, the technical report must be accompanied by the crystallisation of the data relating to the attack, if this constitutes a data breach, in order to be able to extract it for evidentiary purposes for the possible filing of a complaint with the competent authorities.
Compliance with the procedure is compulsory for all those involved and failure to comply with the rules of conduct laid down in the procedure may result in disciplinary measures being taken the offending employee or in the termination of the contract.

existing contracts with defaulting third parties, in accordance with the relevant regulations.

ARTICLE 31 - VIDEO SURVEILLANCE

The processing of personal data carried out through the activation of video-surveillance systems in the University's premises is carried out with respect for the rights, fundamental freedoms and dignity of natural persons, with particular reference to confidentiality and personal identity, also guaranteeing the rights legal persons and any other body or association involved in the processing.
Images and data collected through video-surveillance systems may not be used for purposes other than those indicated in the University regulations on video-surveillance and not be disseminated or communicated to third parties, except in the case of judicial police investigations.
The University guarantees the protection and security of personal data collected through video surveillance systems.
In particular:

1. all personnel involved in the recording, viewing and recording of images, as well as the personnel in charge of maintaining the installations and cleaning the premises, receive adequate training on the behaviour to be adopted in accordance with the provisions of current legislation on the protection of personal data;
2. only authorised personnel may have access to the images;
3. authorised personnel are bound by professional secrecy;
4. images may not be stored for longer than necessary in accordance with the principles applicable to the processing of personal data.

If the images are stored for a longer period than provided for in the relevant regulation, they must be kept in a secure place with controlled access and deleted as soon as their storage is no longer necessary.
It is the responsibility of the person in charge of the facility in which electronic image detection tools, including video recording, are installed for the protection of employees, visitors and property:

1. adopt the guarantees provided for in Article 4 of Law No. 300 of 20 May 1970;
2. ensure compliance with the principles of necessity, purpose and proportionality of data processing;
3. ensure compliance with this Regulation, with the requirements imposed by the Guarantor and with current legislation, also in relation to the use of particular technologies and/or equipment;
4. draw up a document stating the reasons for the installation of such systems, also the purpose of possible exhibition during inspection visits, or for the exercise of the data subject's rights or litigation.

This is without prejudice to the need to carry out an impact assessment (DPIA), in accordance with Article 35(3)(c) of the EU Regulation, whenever video surveillance equipment is installed in environments or areas accessible to the public.
In full compliance with the Workers' Statute, the use of plant and equipment for the purpose of remote control of workers' activities is not permitted.

ARTICLE 32 - ADMINISTRATIVE SANCTIONS

Without prejudice to the provisions of Articles 58, 82, 83 and 84 of the EU Regulation and of the Personal Data Protection Code, the disciplinary and administrative sanctions to be imposed on staff in the event of violation of the laws and procedures on personal data protection will be defined by the University also on the basis of provisions of the CCNLL, the Code of Ethics and the Codes of Conduct.

ARTICLE 33 - DATA PROCESSING IN THE MEETINGS OF UNIVERSITY GOVERNING BODIES

In the context of the activities related to the functioning of collegiate bodies, personal data is processed accordance with these Rules and Regulations and for the sole purpose of the proper management of the deliberation process.

ARTICLE 34 - FINAL PROVISIONS

For anything not expressly provided for in these Regulations, please refer to the provisions of the EU Regulation and Legislative Decree 196/2013 Personal Data Protection Code and ss.mm.ii., in addition to the provisions of the Guidelines and the Deontological Rules adopted and approved by the Guarantor.
The annexes that refer to it insofar as they relate to specific areas governed by these Rules and Regulations, including any annexes that are amended, updated or supplemented on the basis of specific regulations, shall constitute an integral and substantial part of these Rules and Regulations. Any amendments, additions or updates to the annexes to these Rules and Regulations shall be acknowledged by means of a Titulus annotation on the protocol registration of the Rectoral Decree issuing these Rules and Regulations.

ARTICLE 35 - TIME AND PUBLICITY

These Rules enter into force on the day following their publication on the University website and their posting on the online notice board.
The University shall publicise these Rules and Regulations and subsequent amendments and additions by publication in the Official Bulletin of the University and by internal distribution through institutional distribution lists.