UNIVERSITÀ DI FOGGIA

HR EXCELLENCE IN RESEARCH

REGULATIONS ON THE PROTECTION OF PERSONAL DATA OF THE UNIVERSITY OF FOGGIA

INDEX

PART I
GENERAL DISPOSITIONS

ART. 1
SCOPE OF APPLICATION

1. These rules, adopted in implementation of the Regulations (EU) No. 679 of 27 April 2016 (also known as the "GDPR") and the Legislative Decree No. 196/2003 as emended by Legislative Decree No. 101/2018 (known as the "Privacy Code") and subsequent emendments and additions, governs the protection of natural persons with regard to the processing of personal data and the free movement of such data carried out by the University of Foggia.
2. The University of Foggia (referred to as the University), as a Public Administration pursuant to the Article 1, paragraph 2 of Legislative Decree No. 165/2001 and subsequent emendments, pursues objectives of public interest as defined by law and by its own Statute.
3. The University, as the Data Controller, processes the personal data of data subjects in the pursuit of its institutional purposes, respecting every rights and freedom, human dignity, and the right to the protection of personal data, in order to establish a relationship of trust with students, teaching and research stuff, technical and administrative stuff, and all those who, in every way, come into contact with the University.
4. The University processes personal data respecting the current European and National Legislation on personal data protection.
5. The processing of personal data is carried out in respect of the current legislation, based on the lawful conditions set out in the GDPR and the Privacy Code, as was said in the art. 4 of these present Regulations.

ART. 2
DEFINITIONS

1. For the purposes of these Regulations, and in accordance with the National and European Legislation on personal data protection, the following definitions shall apply:

a) "Processing": any operation or a set of operations which is performed on personal data or on a set of personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by trasmission, disseminations or otherwise making available, alignment or combination, restriction, erasure or destruction (art. 2, point 2 of the GDPR general data protection Regulations);

b) "Personal data": any information relating to an identified or identifible natural person (data subject); an identifible natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (art. 4, point 1 of the GDPR);

c) "Special categories of personal data": 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 for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation (Article 9, paragraph 1 of the GDPR);

d) “Genetic data”: personal data relating to the inherited or acquired genetic features of a natural person which provide unique information about the physiology or the health of that person, and which result, in particular, from the analysis of a biological sample from the natural person in question (Art. 4 No 13 of the GDPR);

e) “Biometric data”: personal data resulting from specific technical processing relating to the physical, physiological or behavioural features of a natural person, which allow or confirm the unique identification of that natural person, such as face ID or dactyloscopic data (Art. 4, No 14 of the GDPR);
f) “Data concerning health”: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person personal health (Art 4 No 15 of the GDPR);
g) “Personal data relating to criminal convictions and offences”: personal data relating to criminal convictions and offences or related security measures (Art. 10 of the GDPR);
h) “Consent of the data subject”: any freely given, specific, informed and anambiguous indication of the data subject’s wishes by which the person, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to that person;
i) “Controller”: the natural, or legal person, public authority, agency or other body which, alone or with others, determines the puposes and means of the processing of personal data: where the purposes and means of such processing are determinated by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law (Art 4 No 7 of the GDPR);
j) “Joint controller”: the controller who, jointly with one or more Controllers, determines the purposes and means of the processing of personal data;
k) “Processor”: a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller (Art. 4 No 8 of the GDPR);
l) “Data protection officer” (DPO): a professional figure expert in data protection tasked with ensuring the correct application of European and national data protection law within each organization where they are appointed (Arts. 37,38 and 39 of the GDPR);
m) “Digital transition officier” (DTO): a figure established within public administrations to ensure the transition to digital operational modes and the consequent reorganization processes aimed at creating a digital and open administration, providing services that are easy to use and of high quality, through greater efficiency and cost-effectiveness (Art. 17 of the Digital Administration Code);
o) “System administrator”: within the scope of the Italian Data Protection Authority’s provision of November 27, 2008, System Administrators are identified as a professional figure dedicated to the management and maintenance of processing systems used for the processing of personal data, including database management systems, complex software systems such as ERP (Enterprise Resource Planning) systems used in large companies and organizations, local networks, and security devices, insofar as they allow intervention on personal data;
p) “Communication”: making personal data known to one or more specific recipients other than the data subject, the controller’s representative within the territory of the State, the processor, and those authorized, by any means, including by making the data available, consulting it, or through interconnection;
q) “Disclosure”: making personal data known to an indefinite number of subjects, by any means, including by making the data available or by consultation;

r) “Anonymous information”: information that does not relate to an identified or identifiable natural person or personal data rendered sufficiently anonymous so as to prevent or no longer allow the identification of the data subject;

For all the other information relating the processing of personal data that are not included in this article, reference is made to the European and national legislation on the personal data protection, as well as, to the guidelines issued by the Italian data protection authority and the European data protection board.

ART. 3
PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA

1. The University of Foggia processes personal data following the principles set out in Articles 5 and 25 of the GDPR.

2. Personal data are:

a) Processed lawfully, fairly and transparently (lawfulness, fairness, and transparency);
b) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purposes limitation). Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered incompatible with the initial purposes;
c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
d) Accurate and, if necessery, kept up on date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);
e) Kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the personal data are processed: personal data may be stored for longer periods of time but they have to be processed only for archiving purposes in the public interest, scientific, or historical research pourposes, or statistical pourposes, subject to the implementation of appropiate technical and organisational measures required by the GDPR (storage limitation);
f) Processed ansuring appropiate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality);
g) Processed to the extent necessary for the pourposes for which they are collected (necessity).

3. The University adopts appropiate technical and organisational measures to demostrate compliance with the principles referred to in the previous paragraph (accountability), considering the state of the art, the cost of implementation, and the nature, scope, context and pourposes of the processing.

4. In case of transfer of personal data to a third country or an international organization, the specific conditions laid down in Articles 44 and et. Seq. of Regulations (EU) 2016/679 shall apply, in order to ensure that the level of protection of the natural persons guaranteed by European legislation is not undermined.

ART. 4
GIURIDIC BASE

1. The University is a public administration pursuant to Article 1, paragraph 2 of the legislative Decree no. 165/2001. It pursues objectives of general interest, operates under administrative law, and exercises public authority. The University may process personal data when one of the conditions provided in Art. 6 par. 1 and Art. 9 par. 2 of the RGPD applies.
2. The processing of personal data carried out by the University for institutional purposes and related tasks is based on the legal basis provided in Art. 6, par. 1, letter e) of the RGPD.

2.1 As provided in the Art. 2- ter of the legislative Decree 196/2003 and subsequent emendaments, the legal basis for the processing of personal data used for the performance of a task in the public interest or in connection with the exercise of public authority is established by a legal or regulatory provision or by general administrative acts.

2.2 Based on par. 1-bis of Art. 2-ter of the legislative decree 196/2003 and subsequent emendamments, following any other obligation provided in the RGPD and in the Privacy Code (in its updated version), the processing of personal data by a public administration is allowed when necessary for the performance of a tasks carried out in the public interest or for the exercise of official authority vested in it.

PART II
DATA CIRCULATION

ART. 5
DATA CIRCULATION IN THE UNIVERSITY

1. Access to personal data by administrative, service, educational, and scientific structures, but also by the employees of the University, is permitted only when they are used for institutuinal purposes. Such access is guided by the principles of the free flow of information in a single departement of the University, according to which the University organizes the information and data at its disposal through tools, including digital systems.
2. Any request for access to personal data by any University structures or its employees, duly justified and related to the performance of activities within their specific functions, will be granted directly without any other formalities, to the extent that it is necessary, relevant, and not excessive for the pursuit of institutional interests. If the request is intended for a further and/or different use of data, the requester must explicity and formally indicate this in the request and the nit will be evaluated by the data Repository Manager, and authorization will be granted or denied depending on whether or not the purpose falls within the University's institutional activities.
3. For the purposes of data access, bodies with control and evaulation functions such as the Broad of Auditor, the Evaluation Unit, and many other bodies with such power are considered equivalent to University structures.

ART. 6
CIRCULATION, COMMUNICATION AND DISSEMINATION OF DATA TO THIRD PARTIES

1. The communication of personal data between entities that carry out data processing, other than special categories of data referred to in Arts. 9 and 10 of the GDPR, for the performance of a task carried out in the public interest or in the exercise of official authority, is permitted only if provided by a legal provision or, in cases provided by law, by a regulatory provision.

2. The dissemination and the communication of personal data, processed for the performation of a task of public interest or connected with the exercise of official authority, to entities that will process personal data for other purposes it will be allowed only if provided in par. 1.
3. For the purpose of facilitating guidance, training, and profesional placement, including abroad, of students or recent graduates, the University may, upon the data subject's explicit request or consent, communicate or disclose to private entities, also via eletronic means, personal data relating to academic achivements, both interim and final, as well as personal data including special categories of personal data as defined in Articles 9 and 10 of the GDPR insofar as such data are relevant to the aforementioned purposes and the tasks connected thereto.
4. The transfer of personal data in countries outside the EU is carried out under the conditions laid down in Art. 44 and following the GDPR.

ART. 7
PUBLICATION OF THE RESULTS OF COMPETITIONS AND SELECTION PROCEDURES FOR TEACHING AND NON-TEACHING STAFF

1. In accordance with the transparecy regulations, is allowed the publication, also in the University's websites, of public notices for the recruitment, in any capacity, of academic and non- academic staff, along with the evalutation criteria adopted by the Selection Commitee, the topics, and the final rankings, including the names of the successful candidates or those deemed eligible.
2. The publication of documents on the websites is carried out in compliance with the principle of data minimisation, by disclosing only the data strictly necessary to achive the purposes for which they are published. The documents are published for the period established by the law; once this period has expired, they are removed from the website.
3. Information relating to the health condition or socio-economic difficulties of the data subjects is not subject to publication.
4. In order to balance the requirement for transperancy with the need to protect personal data, the publication of ranking list is permitted with the names of successful or eligible candidates only. The names of candidates who were not eligible or did not pass the selection process must not be published.

PART III
ENTITIES RESPONSIBLE FOR DATA PROCESSING AND PRIVACY ORGANIZATIONAL CHART

ART. 8
DATA CONTROLLER

Pursuant to the applicable National and European Regulations, the University, represented by the acting Rector, is the data controller.
1. The data controller is responsible for decisions regarding the purposes and methods of the personal data processing, as well as the tools used.
2. The data controller, in accordance with the National and European Data Protection Legislation, fulfills the obligations related to the data protection and, in particular, implements appropiate technical and organizational measures to ensure a level of security appropiate to the risk.
3. The data controller, within the scope of the powers conferred by the Statute, may delegate the head of the Departement to which the Privacy Office reports to sign documents relating to the exercise of the data subject's rights as set out in Art. 25 of these present regulations.

ART. 9
DATA PROCESSOR

1. If the University, for the purpose of achieving its institutional objectives, use a third party to carry out specific activities involving the processing of personal data, the data controller shall appoint that party as data processor pursuant Art. 28 of the GDPR.
2. The data processor is selected among entities that provide sufficient garantees to implement appropriate technical and organizational measures, so that the processing complies with the data protection regulations and ensures the protection of the rights of the data subject.
3. The appointment of the data processor is made by means of a contract, or any other legal acts in a written form, which specifies the nature, purposes, and duration of the processing, the type of personal data processed, and the categories of data subjects, defining the obligations of the processor following Art. 28 par. 3 of the GDPR.
4. The data processor may be authorized to work with another processor (sub-processor) for the performance of specific activities of processing, but the same obligations imposed on the processor are also imposed on the sub-processor. In any case, the data processor remains fully liable to the data controller for the fulfillement of the obligations by the sub-processor.
5. The University may be appointment as data processor, when, on the basis of a contract or other legal acts in a written form, it carries out personal data processing on behalf of another data controller.

ART. 10
AUTHORIZED DATA HANDLERS – DATA PROCESSOR

The subjects authorized to the data processing are natural persons who have been instructed and trained by the data controller to carry out data processing operations under their authority and in accordance with the instructions received.

1. The natural persons that are responsible for the processing of personal data in the University are:
   a) Teaching stuff, researches, and technical-administrative personnel;
   b) Collaborators affiliated with administrative and service structures, as well as those involved in teaching and research;
   c) The members of the central governing bodies of the University, as defined by Art. 3 of the Statute, as well as other bodies and commitees operating within it;
   d) All other individuals who process personal data within the organization, including students, PhD candidates, reseach fellows, interns, and trainees (for thesisi work, collaborations, research activities, internships, or traineeships).
2. The authorization for the processing of personal data may be granted, by eletronic means through general measures and/or specific acts, depending on the type of processing and the nature of the data processed. It may also be granted through the documented assignment of a natural person to a structure/office for which the scope of the processing permitted and authorized for the members of that structure/office is identified in writing.
3. Authorized persons for the data processing undertake to maintain the confidentiality of the information and data they become awere of and, in any case, not to disclose and/or disseminate such data without authorization. They are also required to promptly report to the data controller any breach concerning personal data protection.

ART. 11
DATA PROTECTION OFFICER

1. The University, as a public administration, designates a data protection officier (DPO) pursuant to Art. 37 lett. A) of the GDPR.
2. The DPO is selected on the basis of professional qualities, expert knowledge of data protection law and pactices, both at European and National level, and the ability to fulfill the tasks required by the legislation.
3. The DPO is required to perform the following tasks:
   a) To inform and advise the data controller, as well as employees and collaborators who carry out processing activities, regarding their obligations under the GDPR and National data protection legislation;
   b) To ensure compliance with the GDPR and with other provisions stemming from EU and National legislation, including the assignment of responsibility, and to verify the training of personnel involved in processing activities and related control tasks;
   c) Share, if request, advice on the data protection impact assessment and manitor its performance;
   d) To cooperate with the Supervisory authority;
   e) Act as the point of contact for the data protection authority on metters relating to processing, including the prior consultation referred to in Art. 36 of the GDPR, and where appropriate, carry out consultations regarding any other metter.
4. The DPO prepares an annual report on the activities carried out.
5. The DPO is provided with adequate resources and sufficient working time to perform their duties, including the possibility of relying on specific working groups.
6. The DPO has access to the necessary informations to perform their tasks and is consulted on issues related to data protection and on activities involving data processing from the earliest stage of design and by default.
7. The data controller ensures that the DPO performs their tasks with autonomy and indipendance, and also commits not to remove or penalize them for carrying out their tasks. In particular, the DPO cannot hold roles that involve determinating the means and puposes of the processing, nor can they rapresent the data controller or the data processor.

ART. 12
TEAM PRIVACY AND PRIVACY STUDY GROUP

1. The Privacy team, nominated with decree by the Rector, is composed of:
   - The Rector's delegate for Confidentiality/Privacy or, in the absence thereof, a faculty member with expertise in privacy matters;
   - A member with managerial qualification designated by the General Director;
   - A member of the technical-administrative staff with expertise in Privacy.
2. By request of the privacy team, privacy reoresentatives can be naminated in every University's departements.
3. The team meets periodically, and in any case once a month with the data protection officier.
4. The role of the Privacy team is to support the data protection officier (DPO): facilitating coordination between the data controller and the data protection officier.
5. The Privacy team, always in collaboration with the DPO, proposes and promotes training activities and seminars for the University's stuff.
6. The Rector may nominate with its own decree, on the team Privacy request, a privacy study group. The group is chaired by the a delegate of the Rector (privacy delegate/Confidentiality and is composed of faculty members in law, philosophy, and computer science disciplines, with experitise in privacy, data protection and cybersecurity. The role of the group, purely advisory

and research based, is to analyse and enhance data protection practices. Any request coming from the group is shared with the Privacy team and then with the DPO.

ART. 13
SYSTEM ADMINISTRATORS

1. System administrators are the individuals responsible for the management and maintenance of data processing systems and their components, used in relation to the processing of personal data within the University of Foggia. The "system administrators" are essential figures for the security of database and the proper management of the telecommunication networks. They are experts tasked with performing sensitive functions that involve the practical ability to access all data transmitted across institutional and organizational networks.
2. For the purposes of these present Regulations, system administration are considered the professional figures who operate in the University for the administration of databases, nateworks, and complex software systems.
3. The data controller selects the system administrators through a formal act of individual designation, in which the tasks and permitted areas of operation in detail, based on the assigned authorization profile.
4. In case of notification of data protection violation, the system administrator shall report to the data controller and the DPO any detected anomalies, malfunctions, or security risks.
5. The system administrator supports the authorized users with technical and IT-related aspects in the performance of their institutional operational activities.

PART IV
TYPES OF PROCESSING

ART 14
PROCESSING OF PERSONAL DATA

1 The University carries out personal data processing for the pursuit of its public interest purposes, as identified by legal, statutory, and regulatory provisions, using appropiate measures and taking into account the state of the art, implementation costs, as well as the nature, scope, context, and purposes of the processing. Always in compliance with the GDPR, the italian privacy code, and the guidelines and provisions issued by the data protection authority.

2 The University carries out the processing of personal data, including special categories of data, provided by legislation and regulations concerning, by way of exemple but not limited to the following areas:

a) The management of work relationships involved in the teaching and research stuff, executives and technical-administrative stuff, external collaborators, and other individuals engaged with the University through para-subordinate contracts, including those whose employment relationship has terminated;
b) Teaching activities, including the management of students careers, interpreted as graduates, doctoral candidates, and interns;
c) Reseach activities, including medical research, as well as teaching and healthcare services related to research, and healthcare services provided within affiliated healthcare facilities;
d) Managerial and contractual activities, carried out on behalf of third parties and/or related to cross-functional operations, including technology transfer.

ART. 15
SPECIAL CATEGORIES OF DATA

1. The processing of personal data that will disclose racial or ethnic origin, political opinions, philosophical or religious beliefs or the union affiliation, as well as any genetic data, biometric data intended to uniquely identify a natural persoan, data related to personal health or to sexual life or sexual orientation (cd. Particular category of data) is forbidden. The processing may be allowed if one of this conditions will accurs (art. 9, par. 2 of the GDPR):
   a) The data subject has presented explicit consent for one or more specific pourposes;
   b) The processing is necessary for the puposes of fulfilling the obligation and the rights of the University or the data subject in the field of employment law and social securety and social protection, to the extent that it is authorized by Union or National law or by a collective agreement, subject to appropriate safeguards for the fundamental rights and interests of the data subject;
   c) The processing is necessary for the sefety of the interest of the data subject or of another natural person when the data subject can't give the consent due to its personal or giuridic position;
   d) The processing concerns personal data that has been manifestly public by the data subject;
   e) The processing is necessary to establish, exercise or defend a right in a legal proceeding or whenever judical authorities are exercising their judical functions;
   f) The processing is necessary for preventice medicine pourposes or occupational health, valutation of the work capacity of the employee, diagnosis, assistence or sanitary or social therapy which means the management of sanitary or social servives based on Union or National law or pursuant to a contract with a healthcare professional, and the data is processed by or under the responsability of a professional subject to an obligation of professional secrecy;
   g) The processing is necessary for archiving purposes in the public interest, scientific or historical reaserch purposes, in accordance with art. 89 of the EU Regulations;
   h) The processing is necessary for public interest, if provided by Union law or by National law, by provisions of law or regulation, or by general administrative acts specifying the types of data that may be processed, the operations that may be carried out, and the reasons of substantial public interest, as well as ensuring that the processing is proportionate to the pursued purpose, respects the essence of the right to data protection, and provides appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.
2. For the puposes of the previsions referred to in the precedeting par. h), processing activities carried out in the areas specified in the art. 2-sexies of the Privacy Code are considered to be of significant public interest.
3. Genetic, biometric data relating to the health can't be shared and can be processed only if one of the conditions in the par. 1 accurs and in compliance with the protective measures issued by the data protection authority.

ART. 16
DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES – JUDICAL DATA

1. The processing of personal data relating to criminal convictions or offences, or connected with preventive measures is allowed only if authorized by the Union law or by the National law that provides appropriate safeguards for the rights and freedoms of the data subject.

2. The processing of personal data referred to in par. 1 is permitted, in particular, in the following casess as provided for in Art. 2-octies of the Privacy Code:
   a) Fulfilment of obligations and exercise of rights by the data Controller or the data subject in the contex of employment relationships, within the limits established by laws, regulations and collective agreements, as provided by Art. 9 and 88 of the GDPR;
   b) Fulfilment of obligations provided by provisions of law or regulations concerning mediation aimed at the settlement of civil and commercial disputes;
   c) Verification or assessment of integrity requirements, subjective requirements, and disqualifying conditions in the cases provided for by law or regulations;
   d) Assessment of liability in relation to accidents or events concerning human life, within the limits established by applicable laws or by the 11 regulations;
   e) Assessment, exercise or difence of a right in a court of law;
   f) Exercise of the right to access to the data and to administrative documents, within the limits established by laws or by the regulations;
   g) Fulfilment of obligations provided by provisions of law concerning communication and anti-mafia reports or concerning the prevention of mafia-type criminality and other serious forms of social danger, in the cases provided by laws or by regulations, or for the preparations of documentation required by law for partecipation in public procurement procedures;
   h) Assessment of the moral suitability requirement of those intending to partecipate in public procurement procedures, in compliance with the applicable procurement regulations;
   i) Fulfilment of the obligations provided by laws concerning the prevention of the use of the financials system for the purpose of laundering the proceeds of criminal activities and financing terrorism.

ART. 17
PROCESSING OF PERSONAL DATA IN THE CONTEXT OF EMPLOYMENT

1. The University processes the personal data of the teaching and researching stuff, of the managerial and technical-administrative sfuff, as well as individuals engaged in other forms of employment relationships different from subordinate employment, adopting appropriate safeguards to ensure the protection of the fundamental rights and freedoms of individuals, in compliance with the law and applicable collective agreements.
2. The processing of personal data relating to the stuff, is necessary, may be effectuated for public interests as definited in Art. 2 sexies of the Privacy Code; to fulfil the obligations and exercise the specific rights of the data controller or the data subject concerning employment rights and social securety and social protection; to assessment, exercise or defend a right in the court of law; For purposes of archiving in the public interest, scientific or historical research, or statistical purposes, in accordance with Article 89(1) of the GDPR (Article 9(2)(g), (b), (f), (j) of the GDPR).
3. The stuff members follows technical and organizational measures indicated by the University to garantee security in the processing of personal data, also remotely or in smart working mode.
4. Stuff members shall maintain the confidentiality of all personal data processed in the course of their duties.

ART. 18
STUDENT RECORDS AND EDUCATIONAL ACTIVITIES

1. The University of Foggia proccess student's personal data, interpreted in their broadest meaning, for the purpose of carrying out admission and enrollment procedures for undergratuates and postgraduate courses and intership, as well as all activities related to management of students and student records.
2. The student's right to privacy remains safeguarded persuant to Art. 2, par. 2, of Presidencial Decree No. 249 of June 24, 1998.

ART. 19
PROCESSING OF PERSONAL DATA FOR SCIENTIFIC, HISTORICAL OR STATISTICAL PURPOSES

1. The processing of personal data for archiving purposes in the public interest or for historical research is effettuated from whoever works in the University's structures ensuring compliance with the principle of data minimization and with the data protection principles enshrined in the GDPR and in the Privacy Code (upgraded version).
2. where is possible and without compromising the achievement of the puposes of the data processing, the 12 data will be processed with technical measures and will not allow the identification of the data subject anymore.
3. The personal data collected for archiving purposes in the public interest or of historical research cannot be used to adopt decisions or administrative measures detrimental to the data subject, unless they are processed for other purposes following the principles in the Art. 5 of the GDPR.
4. The documents that contains personal data, processed for archiving purposes in the public interest or for historical research, may be used, following their nature, only if they are relevant and necessary for the archivement of such purposes.
5. The consultation of historically significant documents preserved in the University archives is governed by Legislative Decree n. 42 of Genuary 22 2004 the related codes of conduct and by University's departements regulations.
6. The processing of personal data for archiving purposes of public interest or for historical research is effettuated rispetting the codes of conduct approved by the data protection authority.
7. The processing of personal data for statistic or scientific purposes from whoever works in the offices and University's structures or on behalf of the University itself, has to respect the following principles:
   a) The personal data processed for statistic or scientific purposes cannot be used to take decisions or measures on the data subject, and either processed for other purposes;
   b) The data subject must be provided with information relating the statistical or scientific research purposes of the processing, unless this would require a disproportionate effort in relation to the right being protected, and provided that appropriate forms of public disclosure are adopted, as identified by the relevant codes of conduct promoted by the data protection authority.

PART V
DATA PROTECTION AND DATA SECURITY

ART. 20
RECORD OF PROCESSING ACTIVITIES

1. The University, as the Data Controller, has a Record of processing activities carried out under its own responsibility and is responsible for the corresponding update.
2. The Record contains the following informations;

a) The competent body in charge of the processing;
b) Where applicable, the names and contact details of the Joint Controller and Processor;
c) The purposes of the processing;
d) A description of the categories of data subject and the categories of personal data;
e) The categories of recipients to whom the personal data have been or will be disclosed;
f) Any transfer of personal data to a third country or an international organization, with the indication of the third country or the international organization and the adeguate documentation of guarantees;
g) Where applicable, the final deadlines provided for the deletion of the different categories of data;
h) Where applicable, a general description of the technical and organizational security measures adopted.

3. The Record of the processing is unitary, but every University's area/departement tekes care of the compilation within its own areas of responsability.
4. The University keeps a Record of every category of processing carried out as the Data Processor on behalf of other Data Controllers, containing:
   a) The department responsible for the processing;
   b) The name and contact details of the Data Controller on whose behalf the University acts, and the Data Protection officier;
   c) The 13 categories of the data processing carried out on behalf of the Data Controller;
   d) Any transfer of personal data to a third country or an international organization, with the indication of the third country or the international organization and the adeguate documentation of guarantees;
   e) Where applicable, a general description of the technical and organizational security measures adopted.

ART. 21
STAFF TRAINING

1. To ensure the correct and timely implementation of regulations regarding personal data protection and cybersecurity, the university supports and promotes, with the involvement of the University's institutional bodies responsible for the subject matter, awareness-raising tools, and training activities aimed at strengthening awareness of the value of personal data protection and directed at University staff.

ART. 22
DATA PROTECTION IMPACT ASSESSMENT

1. When a type of processing, when it specifically involves the use of new technologies and, considering the nature, scope, context, and purposes of the processing, it may pose a high risk to the rights and freedoms of a natural person, the university, before proceeding the processing, carry out, with the DPO, a data protection impact assessment. A single impact assessment may be conducted for a set of similar processing activities that present similar high risks.
2. Without prejudice to the types of processing identified by the data protection authority, a data protection impact assessment is carried out by the University in the following cases:
   a) Sistematic and global assessment of all the aspects relating the processing of a natural person, based on an automatic processing, including the profiling, and on which decisions

are based that produce legal effects concerning those individuals or similarly significantly affect them;
   b) Large-scale processing of special categories of personal data referred to in the preceding Article 17, or of data relating to criminal convictions and offences;
   c) Systematic large-scale monitoring of a publicly accessible area;
   d) The processing of the data relating personal health for scientific, medical, biomedic or epidemiological research.
3. The impact assessment contains the following elements:
   a) A sistematic description of the processing and their purposes;
   b) An assessment of the necessity and proportionality of the processing in relation to the purposes;
   c) An assessment of the risks for the rights and liberty of the data subject;
   d) The measures envisaged to address the risks, including safeguards, security measures, and compliance with the GDPR, taking into account the rights and legitimate interests of the data subjects and other individuals concerned.
4. If necessary, the University shall carry out a review to assess whether the processing of personal data is being carried out in accordance with the impact assessment, when changes in the risk posed by the processing activities arise.

ART. 23
TECHNICAL AND ORGANIZATIONAL MEASURES

1. The University as the data controller adopts adeguate technical and organizational measures to garantees a level of security commensurate to the risk, measures that includes among others, the ability to ensure on a permanent basis the confidentiality, integrity, availability and resilience of processing systems and services, taking into account the state and the art and implementation costs, as well as the nature, scope, context, and purposes of the processing, and the risk of variable probability and severity to the rights and freedoms of natural person.
2. In the assessment of the adeguate level of securety, particular consideration is given to the risks posed by the processing that comes from, in particular, the destruction, loss, alteration, anauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.
3. The University adopt an approach that consider the protection of personal data object of processing from the moment of the design and from the default setting also in the selection and configuration of information systems and operational procedures.
4. After the entry into force of these present Regulations, the Data Controller may entrust the privacy study group in agreement with the DPO and the privacy team with defining any strategies, guidelines, and policies.
5. Authorized personnel are instructed and trained to observe appropriate technical and organizational measures to limit the risks of destruction or loss, including accidental, and unauthorized access to personal data.

PART VI
DATA SUBJECT RIGHTS

ART. 24
EXERCISE OF THE DATA SUBJECT'S RIGHTS

1. The University respects and acknowledges the rights of the data subject as setted out in Art. 15 and 22, in accordance with the specific procedures provided therein.
2. In particular, the rights of:
   a) Access to personal data which means the right to known and obtain the confermation if there is or isn't a processsing of personal data and all the information about it;
   b) Rectification, which means, the right to correct inaccurate personal data, as well as obtain the completion of incomplete data without undue delay;
   c) Erasure, "right to be forgotten", meaning the right to have one's personal data erased without undue delay, in the cases provided for by Art. 17 of the GDPR;
   d) Limitation to the processing, which means the right to prevent the processing of a subject personal data following Art. 10 of the GDPR:
   e) Data portability, that is the right to receive the personal data provided to the data Controller in a structured, commonly used and machine-readable format, and to transmit those data to another Controller, where the processing is based on consent or on a contract and is carried out by automated means;
   f) Objection to processing, that is, the right to object, on grounds relating to the data subject's particular situation, to processing carried out for purposes of public interest or legitimate interest, or to processing for scientific or historical research purposes or statistical purposes, as well as the right to object at any time, on any grounds, to processing for direct marketing purposes;
   g) Withdrawal of consent for processing carried out on the basis of consent, at any time and with the same ease with which it was given, without affecting the lawfulness of processing based on consent before its withdrawal.
2. The exercise of the rights may be exercised from the data subjects without any formality and for free. However, all reasonable measures will be adopted to verify the identity of the data subject or their representative, such as the request for identification documents, powers of attorney, guardianship appointement acts, or letters of authorization.
3. On the University's departement official website, in the privacy section, it is indicated the mail adress where to sent the request (https://www.unifg.it/it/privacy).
4. The data Controller, in accordance with the DPO, have to give an answer to the request of exercise of the rights without undue delay and within a month from the request. However, this period may be extended for two month when the request is particularly complex, including in relation to the volume of data requested and the number of request submitted, taking into account in particular the burden their impose and their impact and cost in relation to the time required to respond.
5. Where a request is manifestly unfounded or excessive, or where the data subject provides false or misleading information when submitting the request, the Controller shall refuse the request, providing reasons for the refusal.
6. In any case, the right to lodge a complaint with the Data Protection Authority remains unaffected, pursuant to Article 77 of the GDPR, if the data subject considers that the processing of their personal data infringes data protection legislation.
7. Reference is made to the provision setted out in Article 2-undecies of the Italian Privacy Code regarding the restriction of data subject rights. In particular, it should be noted that the rights referred to from Article 15 to 22 of the GDPR may not be exercised through a request to the data controller or by lodging a complaint pursuant to Article 77 of the GDPR, where the exercise of such rights could result in actual and concrete harm to the confidentiality of the identity of the person reporting violations that they became aware of in the context of their

work-related activities or duties, pursuant to the legislative decree implementing Directive (EU) 2019/1937 of the European Parlament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, or who report breaches pursuant to Articles 52-bis and 52-ter of the relevant legislative decree.

ART. 25
THE PRIVACY POLICY

1. Every University structures carry out the obligations to inform the data subject every time they collect personal data, informing the data subject about:
   a) The purposes and the methods of the processing which the data request are destinated;
   b) The mandatory or optional nature of the provision of requested data and the consequences of a potential refusal;
   c) The subjects or the categories of subjects to whom the data may be communicated or may become aware of as responsibles or delegates and the scope of dissemination of the data itself;
   d) The rights of the code;
   e) The name, the denomination or the company and domicile, the registered adress or the holder's adress, and if requested, of the controller.
2. The privacy notice could be given in writing, in the registration form, on papers in the 16 structures, or also with mass information, such as signs posted in the places where the interested parties go to give their data (department offices, human resources office, etc…) or with notices on web pages.
3. If the personal data are not collected at the interested part's adress, the privacy notice is given when the registration of personal data is made or not later than the first communication, axcept the following cases:
   a) When they are processed based on the obligation provided by the law, from regulations or EU legislation;
   b) When they are processed to assert or defend a right in court, as long as the data are processed only for that purpose and for the time necessary to fulfill it;
   c) When the privacy notice involves the use of means that the Data Protection Authority has declared disproportionate to the right being protected.

PART VII
SANCTIONS AND DATA BREACHES

ART 26
PERSONAL DATA BREACH AND SANCTIONS

1. The University, in accordance with the DPO, notify the violation of the data protection authority without unjustfied delay and, when is possible, within 72 hours from the moment the data protection authority became aware, unless it is unlikely that the violation of personal data presents a risk for the rights and the liberties of the natural persons. In case the notice at the data protection authority is made within 72 hours, is Accompanied by the reasons of the delay.
2. The notice contains the following elements:
   a) The nature of the violation of the personal data, including, when is possible, the categories and the Approximate number of the Interested parties as well as the approximate number of the personal data involved;

b) The name and the contact informatons of the DPO or others contacts where to get more informations;
c) Probable conseguences of the violation of personal data;
d) Measures taken or proposed to be taken to address the personal data breach and, where appropriate, to mitigate its possible adverse effects.

3. When the violation of personal data is subject to present an elevate risk for the rights and the liberties of the natural persons, the university communicates the violation to the data subject without unjestfied delay.
4. The communication to the data subject is not requested when one of these conditions occurs:
   a) The University had implemented appropriate technical and organizational protection measures (in particular, those aimed at rendering personal data unintelligible to anyone not authorized to access it, such as encryption), and such measures had been applied to the personal data affected by the breach;
   b) The University subsequently adopted measures aimed at preventing the emergence of a high risk to the rights and freedoms of the data subjects;
   c) the communication would involve a disproportionate effort, in which case a public communication or similar measure shall be carried out, whereby the data subjects are informed with comparable effectiveness.
5. If the University did not communicate the violation of personal data to the data subject, the data protection authority, after the valutation the probability that the violation presents an elevate risk, it may request that appropriate action be taken, or may decide that one of the conditions referred to in paragraph 5 has been met.
6. The university documents any violation of personal data, the circumstances, conseguences and the measures taken to fix it.
7. The ICT sector supports data controller in accordance with the DPO in the management of the data breach.
8. without anjustfied delay all information related to the data breach must be sent via email to the Data Protection Officer.

PART VIII
MISCELLANEOUS

ART. 27
VIDEO MONITORING

1. The processing of personal data realized with video monitoring installations located at the university sites is regulated by the specific regulations adopted from the departement in subject.

ART. 28
ACCESS RIGHTS AND PRIVACY

1. The assumptions, the methods, the limitations for the exercise of the right to have access to administrative's documents containing personal data, and the related protection they are regulated by the law of August 7 1990, n. 241 and s.m.i. and from the Regulations governing the administrative procedure, of the right to have access to administrative's documents and the Civic access right adopted by the University.
2. In case of data capable of revealing the state of health or sexual life, access to administrative documents is permitted when the legally relevant situation intended to be protected by the

request for access to administrative documents is of a rank at least equal to the rights of the data subject highlighted in the document, or consists of a personality right or another fundamental and inviolable right or freedom.

FINAL DISPOSITION

1. For matters not expressly provided for in these present regulations, reference is made to the provisions of Regulations (EU) 2016/679 and the current Personal Data Protection Code, as well as to the guidelines and directives and the ethical rules adopted and approved by the Data Protection Authority.
2. The provisions contained in other university regulationss concerning personal data protection that conflict with or are incompatible with these Regulations shall be disregarded.