POLITECNICO
MILANO 1863

P O L I T E C N I C O D I M I L A N O

THE DIRECTOR GENERAL

HAVING REGARD TO Italian Law 09.05.1989, no. 168, entitled “Establishment of the Ministry for Universities and Scientific and Technological Research”, as amended;
HAVING REGARD TO Italian Law 07.08.1990, no. 241, entitled “New regulations on administrative procedure and right of access to administrative documents”, as amended;
HAVING REGARD TO the Italian Decree of the President of the Republic of 28.12.2000, no. 445, entitled “Consolidated Law on administrative documentation”, as amended;
HAVING REGARD TO the Italian Legislative Decree of 30.03.2001, no. 165, entitled “General rules on the structure of employment in public administrations”, as amended;
HAVING REGARD TO the Italian Legislative Decree of 27.10.2009, no. 150, entitled “Implementation of Italian Law of 4 March 2009, no. 15, on the optimisation of productivity in public works and efficiency and transparency of public administrations", as amended;
HAVING REGARD TO the Italian Law of 30.12.2010, no. 240, entitled “Rules on the organisation of universities, academic staff and recruitment, and authority granted to the Government to incentivise the quality and efficiency of the university system”, as amended;
HAVING REGARD TO the (EU) Regulation 27.04.2016, no. 679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
HAVING REGARD TO the Italian Legislative Decree 10.08.2018, no. 101 "Provisions for the adaptation of domestic laws to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to personal data processing and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”;
HAVING REGARD TO the implementing provisions of Regulation (EU) 2016/676 issued by the Italian Data Protection Authority;
GIVEN THAT pursuant to Chapter III - Data controller and data processor - Section I - General Obligations of Legislative Decree of 18.05.2018, no. 51 "Implementation of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, ascertainment and prosecution of criminal offences or the enforcement of criminal penalties, and on the free movement of such data, and which repeals the Framework Decision 2008/977/JHA of the Council", and specifically Article 15 "Obligations of the data controller", the data controller is required - taking into account the nature, scope, context and purposes of the data processing and also the risks to the rights and freedoms of individuals - to implement appropriate technical and organisational measures to ensure that the data processing is carried out in conformity with the provisions of the measure in question;
HAVING REGARD TO the existing Charter of Politecnico di Milano;
HAVING REGARD TO the existing General University Regulations;
HAVING REGARD TO the Rectorial Decree Index No. 8269 of 20.12.2017 appointing Dr. Vincenzo Del Core as Data Protection Officer (DPO) for Politecnico di Milano, in compliance with the provisions of Regulation (EU) 2016/679;

HAVING REGARD TO Rectorial Decree no. 4012 of 06.06.2018 by which the pro-tempore Rector of Politecnico di Milano delegated to the General Manager, Mr Graziano Dragoni, the task of organising the University data privacy system;
HAVING REGARD TO its operative Decisions on the administrative structure of Politecnico di Milano;
HAVING REGARD TO Rectorial Decree Index No. 6761 of 06.10.2020 adopting Politecnico di Milano's Regulations on personal data protection and ICT security, with particular reference to Article 2 "Acts of Politecnico di Milano on personal data protection and ICT security";
IN CONSIDERATION OF the need to define adequate operating instructions for the processing and protection of personal data, i.e. an operational mechanism available to the various University stakeholders who occupy the specific roles provided for by applicable rules on personal data management activities;

DECREES AS FOLLOWS

Article 1

For the reasons mentioned in the Recital, the "Operating instructions for the processing of personal data" are adopted, the text of which is an integral part of this official measure.

Operating instructions for the processing and protection of personal data

1. SCOPE

These operating instructions are drafted by reference to the Regulations of Politecnico di Milano on the processing of personal data and ICT security, adopted by Rectorial Decree Index No. 6761/STSAG, Folder No. 0145524 of 06.10.2020, which incorporates the most important principles and obligations provided for by EU Regulation 2016/679 and associated domestic rules on the processing and protection of personal data, with particular reference to Legislative Decree 196/2003, as amended by Legislative Decree 101/2018.

These instructions contain, in particular, operating procedures to be followed for the correct processing of personal data, and also concrete solutions to potential problems that could face internal Data Processors, data privacy officers and Authorised Persons in the course of their duties.

Accordingly, these operating instructions are also intended to assist internal Data Processors, data privacy officers and Authorised Persons who work in the University in any capacity.

They consist of a general part, which aims to explain aspects that need to be taken into account when processing personal data, and a special part, in which data processing operations that are subject to additional rules are described, e.g. research areas and other instances where data disclosure requests arise at meetings with the individual functions.

The instructions may be updated at least once a year, also in order to keep abreast of regulatory changes in the personal data protection field.

2. LEGISLATIVE AND REGULATORY SOURCES

The regulatory framework on personal data protection (or "privacy") is particularly complex and consists of provisions at both European and domestic level. Accordingly, the regulatory sources on personal data protection are listed in the following order:

a) EU Regulation 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

b) Legislative Decree 196/2003 (Personal Data Protection Code), as amended by Legislative Decree No. 101/2018.

c) Official Provision setting forth mandatory requirements in relation to the processing of special categories of data, pursuant to Article 21.1 of Legislative Decree No. 101 of 10 August 2018 (Published in the Official Gazette General Series No. 176 of 29 July 2019), which sets out the requirements to be observed for specific data processing operations. For Politecnico di Milano, the most relevant requirements involve:

1. Requirements for the processing of special categories of data in employment (General Authorisation no. 1/2016);
2. Requirements for the processing of genetic data (General Authorisation no. 8/2016);
3. Requirements for the processing of personal data for scientific research purposes (General Authorisation no. 9/2016).

d) Ethical rules for data processing for statistical or scientific research purposes, published pursuant to Article 20.4 of Legislative Decree No. 101 of 10 August 2018 - 19 December 2018 (published in Official Gazette No. 11 of 14 January 2019).

e) Regulations of Politecnico di Milano on the processing of personal data and ICT security, adopted by Rectorial Decree Index No. 6761/STSAG, Index No. 0145524 of 06.10.2020.

Additional sources on personal data processing are provided by the guidelines published by the European Data Protection Authority and by the Italian Data Protection Authority, which provide useful standards of conduct that the Data Controller and/or Data Processor should adhere to in the context of individual data processing operations and the methods for disseminating and disclosing personal data.[1].

3. ACCOUNTABILITY

This is the foundational principle of the entire data protection area, and it consists of a set of actions and procedures that must be taken into account in order to ensure that personal data are properly protected in compliance with law.

In concrete terms, this principle requires the proactive, permanent and documented adoption of measures whose purpose is to safeguard personal data in the context of data-processing activities engaged in from time to time by the Data Controller and/or by internal/external Data Processors.

Therefore attention is focused on demonstrating how **accountability** is exercised and on its **verifiability**, and also on the need to foster an integrated approach (involving each and every area of the University's organisation) that takes due account of the potential degree of risk that accompanies each data processing operation. Accountability, namely the obligation to be able to account for one's actions and operations, therefore implies:

1. The planning and implementation of obligations, measures and compliance formalities in order to ensure conformity with applicable rules, from the planning stages of the data processing onwards (privacy by design) and by default;
2. The importance of tracking data processing activities by keeping suitable records and documenting their compliance with applicable rules;

1 The list of guidelines published at European level is available at the link: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_it .

3. The implementation of data protection impact assessments where data processing operations involve significant risks to the rights and freedoms of the data subject(s);
4. The provision of clear and satisfactory mechanisms and procedures for data subject(s) to exercise their rights;
5. The readiness to submit/communicate associated documents and objective evidence to the Supervisory Authority (and other stakeholders, as appropriate).

All of this will facilitate full compliance with the provisions of EU Regulation 2016/679, in conformity with the principles already set out in detail in the Privacy Organisational Model of Politecnico di Milano, on pages 5 and 6, namely:

- **the principle of lawfulness, fairness and transparency:** *the data* should be *processed lawfully, fairly and transparently* in relation to the data subject;
- **the principle of purpose limitation:** *the data should be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the initial purposes;*
- **the principle of data minimisation:** *the data should be adequate, relevant and strictly limited to what is necessary in order to facilitate the purposes for which they are processed;*
- **the principle of accuracy:** *the data should be accurate and, where necessary, kept up to date; specific criteria should be applied to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are promptly erased or rectified;*
- **the principle of limitation of data retention:** *the data should be kept in a form that enables data subjects to be identified for a period of time no longer than necessary for the purposes for which the data are processed; personal data may be stored for longer periods provided that such data will be processed solely for archiving purposes in the public interest, or for scientific or historical research or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the European GDPR;*
- **the principle of integrity and confidentiality:** *the data should be processed in a manner that ensures adequate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures.*

4. LEGAL BASIS OF THE DATA PROCESSING

Article 6 of EU Regulation 2016/679 specifies the legal conditions on which a processing of personal data may be deemed legitimate.

Without prejudice to the requirement to provide the data subject with a privacy notice pursuant to Articles 13 and 14 of EU Regulation 2016/679, the following cases provided for by Article 6 of EU Regulation 2016/679 provide various legal bases for a data-processing:

- **The data subject has given his/her consent** (e.g. the legal basis for the data-processing may be provided e.g. by the data subject's participation in events);
- **Performance of a contract and related obligations to which the data subject as a natural person is party** (e.g. a donation contract, the natural person must be informed of the data processing, participation in paid conferences);
- **Compliance with a legal obligation;**
- **To protect the vital interests of the data subject or of third parties;**
- **Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority** (this is the legal basis underpinning Politecnico di Milano's institutional activities e.g. for student careers and or other services described in second level privacy notices);
- **Legitimate interest** (note: in the case of Politecnico di Milano, only when not performing functions/tasks carried out in the public interest or in the exercise of official authority vested in the Data Controller. Where a data processing is considered to fall within the legitimate interest criterion, the Data Protection Officer should be contacted in order to assess its fairness. This criterion should not, in principle, be used as a legal basis for personal data processing activities in the case of a public administration, and should only be considered in residual cases where the University is not acting as an entity with public powers.

In the context of the relevant activities, it is always necessary to ensure that one of these preconditions is satisfied, as the collection and processing of, and access to, personal data can proceed exclusively on the basis of one of these conditions.

Note, too, that it is considered exceptional for a public administration to seek the consent of a data subject to the processing of personal data for its institutional purposes. Indeed, Recital 43 of EU Regulation 2016/679 states that: "In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the Controller, in particular where the Controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the

consent despite such consent not being necessary for such performance."

Accordingly, public entities are not entitled to rely on the precondition of Article 6.1(a) (consent of the data subject), except where there is a level playing field between the data Controller and the data subject, which should be carefully assessed (e.g. participation in events or conferences, or in exceptional cases when personal data are to be transferred to a country without any systematic adequacy decision procedures).

As stated in Article 1 of the Politecnico Regulations on personal data processing and ICT security, Politecnico di Milano is a public administration within the meaning of Article 1.2 of Legislative Decree 165/2001, as amended, and as such pursues general interest purposes, operating under administrative law and exercising public powers. Therefore, the processing of personal data in the exercise of its institutional functions and tasks, such as e.g. teaching, research and third mission activities, is legally justified primarily based on the condition provided for by Article 6.1(e) of the EU Regulation.

5. TRAINING

Recent regulatory developments and, more generally, the need to ensure the protection of personal data, understood as an effective fundamental right of the individual (Article 8 of the ECHR), require adequate and accurate knowledge levels within an organisation. Accordingly the Data Controller, with the assistance of the Data Protection Officer, organises the training and refresher training of all University personnel in the field of Privacy.

The following minimum contents are anticipated for Privacy training:

- initial training of at least 4 hours provided to senior and non-senior management personnel on the organisational model adopted by the University;
- continuous training of at least 4 hours per training year provided to all University personnel on updates to the Privacy organisational system and on the results of Privacy audits in the reference period.

The provision of effective and continuous training courses is also instrumental in mitigating risks associated with and deriving from the various stages of data processing.

Politecnico di Milano has prepared a special personal data protection course on its website: https://servizionline.polimi.it/portaleservizi/portaleservizi/controller/Portale.do?jaf_currentWFID=main&EVN_SHOW_PORTALE=evento

6. HOW TO MAP A DATA PROCESSING

Data-processing operations may be summarised in 5 stages, which may correspond to the life cycle of personal data:

COLLECTION → USE/MANAGEMENT → TRANSFER → STORAGE → ERASURE

"COLLECTION" means the initial phase of acquisition of personal data, i.e. the moment when and the procedures (which should be legitimate, as section 4 of these Instructions indicate) by which personal data released by the data subject is first acquired. This leads to the phase of **"USE"** of such data, namely the activity of accessing, processing and using them in order to achieve the anticipated purposes for which the personal data were in the first place collected. During these phases, the data may be **"TRANSFERRED"** to other parties (e.g. authorities, public or private research bodies, project partners, entities, associations, etc.) who are identified as "Recipients" and carry out functions related to the purposes anticipated. After the data have passed through the stages of use and possible transfer, they are likely to require **"STORAGE"** for a specific period of time which must always be a clearly defined interval, based on the specific purposes of the data processing, except in special cases where the data are archived or where it is not feasible to define an adequate and specific period of time. Once the deadlines for data storage and processing have expired, i.e. when the personal data initially collected no longer need to be kept for any purpose/reason, the stage of "ERASURE" arrives: this refers to any technique and expedient that leads to the destruction, inaccessibility and non-readability of the data initially collected.

All of this defines and constitutes the "Personal Data Lifecycle", which is useful in order to reconstruct and clarify the various properties and stages of the data-processing to be carried out To demonstrate compliance with the provisions of EU Regulation 2016/679 and in order to have a clear understanding of the various figures involved as well as the various roles, data categories, procedures and other aspects (Privacy by design), the entire process needs to be mapped out by reference to a detailed flowchart that can describe the entire life cycle of the personal data collected and processed (as applicable). The mapping should therefore cover the following contents:

1. Figures involved and their respective roles, namely:

Data Controller, internal Data Supervisors, external Data Supervisors, Recipients, Authorised Persons, Data Subjects and other parties who may have access to data collected and processed (for further details see the Privacy Organisational Model of Politecnico di Milano, chapter 5).

2. Type of personal data, namely:

Personal data is any information (e.g. the name) related to a natural person who is identified or identifiable directly or indirectly (Article 4 of EU Regulation 2016/679), or information (e.g. tax code, fingerprint, telephone traffic, image, voice data) about a person whose identity can be ascertained by reference to additional information. The person to whom the processed data refer is known as the "data subject". It is important to note that the data subject can only be a natural person (i.e. an individual) and not a legal entity (e.g. company, foundation or association). Data is considered personal if it enables the person to be identified or if it describes the individual in such a way that enables him or her to be identified by means of other data. Both types of data are protected in the same way. Identification, therefore, means the ability to distinguish the person from any other person or within a category. A person cannot be considered identifiable if the identification would require further data to be obtained for unreasonable costs and times.

A person is identifiable also if he or she can be identified by reference to additional elements. Personal data is a dynamic concept, which always depends on the context, in the sense that even if an isolated piece of information cannot result in an individual being identified, the fact that such information can be used for identification purposes by cross-referencing it with other data nevertheless characterises it as personal data. In addition, for information to constitute personal data, it is not necessary that it should be able to physically identify the person.

Generic Personal Data	**Special Personal Data[2]**
First name and last name	Health data (one of many examples would be blood group)
Registration number / Badge / Personal ID code	Data on criminal convictions and offences committed
Tax code	Data on racial or ethnic origin
Date and place of birth	Data on nationality and/or citizenship
Blood or in-law relationships (grade)	Data on political opinions
Telephone number	Data on personal interests and/or preferences
E-mail address	Data on personal movements and/or location
Physical address (residence and/or domicile)	Data on court or disciplinary proceedings (unrelated to criminal convictions and offences committed)

[2] In comparison with Article 9 of EU Regulation 2016/679, which identifies a list of special personal data, a broader list of “semi-special” data is provided here since, although not directly referred to, such data may entail a connection with special personal data. It is recommended in that case to consult the Data Protection Officer.

No. of registered movable property	Data on gifts/donations made
data on bank accounts and/or insurance contracts	Data on marital status/personal relationships
Data on education and/or vocational training	Data on lifestyle and/or sexual orientation
Data on awards and/or prizes	Data on behaviour/conduct
Data on employment status and/or position	Data on professional performance
	Data on trade union membership
	Data on reliability (economic, personal, etc.)
	Data on religious or philosophical beliefs
	Genetic data
	Biometric data
	Fingerprint data
	Images
	Voice recordings

3. Methods of collection and transfer between the various parties involved in the intended data processing; format in which the data is collected and means used to transfer them from one party to another.

4. How personal data are communicated and disseminated:

- Communication or transfer, which means making personal data known to one or more specific persons other than the data subject, the Data Controller's representative, the Data Processor and the data processing operators (i.e. those in charge of actual data processing operations). If communicated, the data is transferred to third parties.

- Dissemination, which means making personal data known to unspecified persons, in any form, including by making them available, also for consultation. Thus, dissemination also occurs e.g. if a photograph is published on a social network. Without a lawful legal basis, this activity must be considered unlawful.

NOTE

The publication of participants' grades in an examination on the platform Beep, in the reserved area,constitutes a communication for data-processing purposes.

Where a student's grades are published online in clear text with the student's name and surname, this constitutes a dissemination of data. In this case, it is crucially important how the publication is carried

In the exceptional case that confidential access channels are not used, it is good practice to operate as follows:

MATRICULATION of the student (only) → grade/examination result.

The following formulations are either **NOT** recommended or prohibited:

- Person code → grade; (not recommended);
- Person code → name and surname → grade; (prohibited);
- Name and surname → grade; (prohibited);
- Matriculation → person code → name and surname → grade; (prohibited).

5. **Other rules involved,** in addition to those relating to privacy, copyright, compliance standards, labour law, etc.

In the context of research projects, a dedicated analysis form should be compiled, available in Italian and in English in the University repository "Privacy and GDPR: legislation and background information"[3].

7. CATEGORIES OF SPECIAL DATA

It is prohibited to process special data pursuant to Article 9 of EU Regulation 2016/679. This prohibition is lifted if the conditions set forth in Article 9(2) of EU Regulation 2016/679 are present.

The following are the conditions for the legitimate processing of special data:

a) the data subject has expressly consented to the processing of such personal data for one or more specific purposes;
b) processing is necessary in order to implement the obligations and exercise the specific rights of the Data Controller or of the data subject in the field of employment law, social security and social protection, in so far as it is authorised by Union or Member State law or collective agreements;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

[3] The document mentioned is available on the repository at the following link: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?viewid=5aec781e%2Dc4c2%2D487c%2Db0af%2Dba781f7fb0bf&id=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2Fdocumentazione%20ricerca%20scientifica .

.

e) processing involves personal data made manifestly public by the data subject (e.g. published on social networks or disseminated to personnel by email);

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) processing is necessary for reasons of substantial public interest on the basis of Union or Member State law, providing for appropriate measures to safeguard the data subject's fundamental rights;

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, based on Union or Member State law providing for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes.

Processing of special data within the Public Administration.

Where the processing of special data is authorised, special consideration should be given to the provisions of Article 9.2(g) of EU Regulation 2016/679, which permits the processing of "special" data if the processing is necessary for reasons of substantial public interest on the basis of Union or Member State law, which should be proportionate to the aim pursued, should respect the essence of the right to data protection and should provide for suitable and specific measures to protect the fundamental rights and interests of the data subject.

Accordingly, Article 2-sexies of Legislative Decree 196/2003, establishes that the processing of the special categories of personal data referred to in Article 9.1 of the Regulation, required for reasons of substantial public interest within the meaning of paragraph 2(g) of the same Article, is permitted if provided for by EU law or by the provisions of domestic Member State law (or, where legally provided for, of domestic regulations) which specify the types of data that may be processed, the operations that may be carried out and the substantial public interest justification involved, and also the suitable specific measures to protect the fundamental rights and interests of the data subject. Subject to the provisions of further legislative enactments, substantial public interest purposes are those referred to in Article 2-sexies (2) of the aforementioned Legislative Decree no.196/2003, and are listed below:

a) access to administrative documents and civic access;

b) keeping of documents and of registers of civil status, of records of the population resident in Italy and of Italian citizens resident abroad, and of electoral rolls, and the issuance of identification or travel documents or documents amending personal particulars;

c) keeping of public registers for immovable or movable property;

d) keeping of the national register of driving licence holders and of the national vehicle register;

e) citizenship, immigration, asylum, status as foreigner or displaced person, refugee;

f) election franchise and eligibility, and the exercise of other political rights, diplomatic and consular protection rights, and the requirement to document the institutional activities of public bodies, particularly the drafting of minutes and reports of the proceedings of representative assemblies, committees and other collegial or assembly bodies;

g) exercise of the mandate of representative bodies, including their suspension or dissolution, and the requirement to determine causes of ineligibility, incompatibility or disqualification, or removal or suspension from public office;

h) the performance of control, political policy, parliamentary enquiry or inspection functions, and access to documents recognised by law and by the rules of relevant bodies for exclusive purposes associated directly with the implementation of an elective office;

i) activities of public entities which concern the application - also through their assignees - of customs and tax provisions in force;

l) control and inspection activities;

m) the grant, payment, modification and revocation of economic benefits, facilities, handouts, other emoluments and entitlements;

n) the grant of honours and awards, the granting of legal status of associations, foundations and bodies, including those of a religious nature, ascertaining the integrity and professionalism requirements for appointments (for the competency profiles of public bodies) to offices including religious offices and to managerial positions in legal entities, companies and non-state educational institutions, and also the granting and revocation of authorisations or qualifications, the granting of patronage, sponsorship and institutional awards, membership of committees of honour and admission to institutional ceremonies and meetings;

o) relations between public and third sector entities;

p) conscientious objection;

q) protective and sanctions activities in the administrative or judicial field;

r) institutional dealings with religious bodies, religious denominations and religious communities;

s) social welfare activities for the protection of minors as well as the needy, dependent and incapacitated;

t) administrative and certification activities related to activities of diagnosis, healthcare, therapy or welfare, including those related to organ and tissue transplantation and human blood transfusion;

u) duties and functions of the national health service and of health care workers, and duties related to workplace safety, health and hygiene and to the safety and health of the population, civil protection, protection of life and physical safety;

v) planning, management, control and evaluation of health care, including the establishment, management, planning and control of relations between the administration and entities that are accredited, approved or affiliated with the national health service;

z) supervision of trials, pharmacovigilance, marketing authorisation and importation of medicines and other health-related products;

(aa) social protection for maternity and voluntary termination of pregnancy, addictions, assistance, social integration and rights of the disabled;

(bb) education and training in school, vocational, higher or university level institutions;

(cc) data processing operations carried out for archiving purposes in the public interest or for purposes of historical research, involving the preservation, organisation and communication of documents held in State archives, in the historical archives of public bodies, or in private archives declared to be of particularly important historical interest, for purposes of scientific research and also for statistical purposes, by bodies that belong to the national statistical system (Sistan);

dd) establishment, management and termination of employment relationships of any kind, including unpaid or honorary, and of other forms of employment, trade union matters, employment and compulsory placement, social security and social welfare, protection of minorities and equal opportunities in the context of employment relationships, compliance with remunerations, tax and accounting obligations, workplace safety, health and hygiene, health and safety of the population, assessment of civil liability and disciplinary and accounting responsibility, inspection activities.

data on criminal convictions and offences are regulated by Article 10 of the Regulation, which provides that such data may be processed only under the supervision of the public authority and subject to appropriate safeguards and adequate data security measures, in order to ensure that the data subject in question is fully protected. Article 2-octies (5) of Legislative Decree 196/2003 extends the provisions of Article 2-sexies of that decree to the processing of data related to criminal convictions and offences when it is carried under the public authority's supervision.

Cases of special data processed by Politecnico di Milano

Special and judicial data, for which processing by the various facilities of the University is anticipated, are processed in accordance with Article 13 of the Politecnico di Milano Regulations on the processing of personal data and ICT security, and they are therefore traceable:

1. **Management and course of the employment relationship of personnel:**

- **health-related data** (especially when checking suitability for service, when persons from protected categories are being recruited, when disabled people are commencing work, or for maternity leave, workplace health and safety measures, fair compensation, compliance with compulsory and contractual social security and insurance procedures, social welfare benefits, social security redemptions and unifications, accident and/or incident reports, use of special exemptions or work permits);
- **data on political and trade union opinions or religious beliefs or membership of political parties, associations and organisations of a religious, philosophical, political or trade union nature** (in particular for the payment of membership fees, the grant and exercise of leave and of trade union rights, the holding of elections and consultations, request for leave on the occasion of religious holidays);
- **data revealing racial and ethnic origin** (especially when establishing and managing employment relationships with foreigners);
- **judicial data associated with disciplinary proceedings**;
- **data on sexual orientation** (particularly for possible gender reassignment).

2. **Management and course of scientific research activities:**

- **health-related data** (especially for processing data on diseases, therapies and other medical and biomedical information);
- **data on political and trade union opinions or religious beliefs or membership of political parties, associations and organisations of a religious, philosophical, political or trade unionist nature;**
- **data revealing racial and ethnic origin** (especially where foreigners and/or persons with refugee status are involved, in the humanities, economics, biomedical sciences);
- **judicial data associated with disciplinary proceedings;**
- **data on sexual orientation** (especially for research in the humanities and biomedical sciences);

3. Management and course of teaching activities, enrolments and student careers:

- **health-related data** (especially for processing data related to pregnancy or to disabled students and associated social welfare measures/grants);
- **data on political and trade union opinions or religious beliefs or membership of political parties, associations and organisations of a religious, philosophical, political or trade union nature** (especially for the carrying out electoral activities in the University);
- **data revealing racial and ethnic origin** (especially for non-EU citizens and for refugee status and associated grants);
- **judicial data associated with disciplinary proceedings** (especially for users and students held in custody in the context of disciplinary proceedings against the student);
- **data on sexual orientation** (in particular for possible gender reassignment);

Processing of data of minors

Article 8 of the European Regulation No. 2016/679 introduced specific rules for consent-based processing of children's data, in relation to information society services. The provision states that the processing of the personal data of a child shall be lawful where the child is 16 years old (in Italy the legislation has set the age limit at 14 years old: Article 2-quinquies of the Italian Personal Data Protection Code, introduced by Decree No. 101 of 10 August 2018) and has given his/her consent pursuant to Article 6.1(a) of the Regulation. However, its scope somewhat circumscribed, it and applies only to data processing operations:

1. involving generic personal data, i.e. not sensitive, judicial or genetic data;
2. for which the data subject must give his/her consent. Consequently, if the data processing has a different legal basis, the rule does not apply;
3. correlated with the direct supply of information society services: this term refers to any service that is generally provided for remuneration, remotely, by electronic means and at the individual request of a recipient of services.

The Italian provision also states that if child is below the age of 14 years, such processing shall be lawful provided that consent is given or authorised by the holder of parental responsibility over the child. This formulation is consistent with other legal provisions, which link the right to exercise an entire series of rights in specific fields, to the child's 14th year.

[4]

The signature of a parent or person exercising parental authority is also required in the case of a liability release form for photography sessions and video recordings. In this case too the mechanism of specific consent is adopted i.e. consent must be given for each anticipated involving the taking of photos and/or filming of videos.

Having said that, the main problem resulting from this regulatory framework remains the paradoxical split created between the minor's capacity to avail of online services and the minor's capacity to act in the real world context. In other words, although a minor currently requires parental consent for off-line data processing operations (e.g. to register at a gym or for a class photo), he or she can dispense with such consent and act independently in the much more complex universe of on-line data processing.

8. RISK ANALYSIS

The Data Controller and/or the Data Processor are aware of the risks that performing or initiating a data processing operation can represent to the rights and freedoms of data subjects, which may arise in the course of a data processing operation, as specifically referred to in Recital 75 of EU Regulation 2016/679.[5]

All such risks must therefore be identified, analysed and managed accordingly, particularly in order to ascertain the likelihood and seriousness of personal harm.

Risk analysis is a tool that can reveal and develop a specific knowledge and awareness of risks. It provides information on the basis of which a risk weighting assessment can be carried out, and is required in order to make decisions about the methods that can be adopted to limit and/or avoid each identified risk.

The choice of the most suitable procedures to be adopted during the processing obviously depends on the method of processing, on the type of risk encountered, and also on a careful cost-benefit analysis emerging during the phase of assessment of each individual risk.

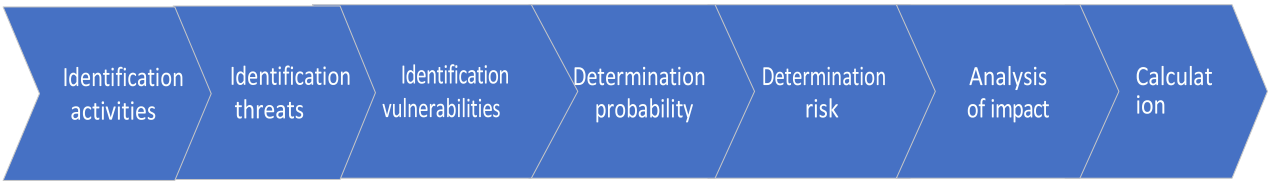
[4]The decision to identify age 14 as the watershed is in line with other legal provisions, which link to this age the entitlement to exercise a whole series of rights in certain fields established by law. First and foremost, the law on cyber-bullying (Law No. 71 of 29 May 2017), which entitles a child over 14 to request the operator of the website or social media to remove, screen or block the dissemination of harmful content concerning him/her. If the operator does not do so within 48 hours or if it has not been possible to identify him or her, this child of 14 years or over may also request the intervention of the Italian Data Protection Authority to have the harmful content removed. Above all, children over 14 may give their consent to adoption (Article 7.2 of Law No 184 of 4 May 1983). As the Italian Data Protection Authority also pointed out, it would have been inconsistent to permit the 14-year-old consent to be adopted, but not to prevent him or her from accessing information society services.

[5] The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may lead to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic detriment or social disadvantage; where data subjects may be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, as well as genetic data, health data or data related to sex life or to criminal convictions and to offences or to related security measures; where personal aspects are evaluated, in particular by analysis or prediction of aspects of work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, particularly children, are processed; or where the processing involves significant masses of personal data and a large number of data subjects.

.

The term 'procedure' means all those technical and organisational steps required to ensure adequate levels of security and integrity of personal data collected and processed.

Risk analysis step:



Step 1 - Identification of activities

This involves identifying the anticipated data processing activities which require a risk analysis. All information on the data processing to be carried out must be gathered at this stage - i.e. any and all information on the systems and tools deployed to implement the data processing, for example, whether the data processing requires PCs, laptops, tablets, the adoption of a network or email system.

Other elements that need to be taken into account when conducting a data protection risk analysis are: the number of users involved in the activity anticipated (the greater the number, the greater the risk), the type of information (the more sensitive the information, the greater the risk), the use of the information, the availability of the information, and the mobility of the information.

Step 2 - Identification of threats

Once the activities and assets have been gathered around classified, the next step is to identify threats. From an IT security point of view, **a threat is any factor that could compromise the confidentiality, integrity or availability of information or of an information system.**

To illustrate, one may describe three types of threat:

1. **acts of god** (e.g. lightning, earthquakes, hurricanes and tornadoes);
2. **human acts** (e.g. carelessness, human error, unauthorised access, identity theft; tampering; data hacking; equipment theft, external hackers and visitors, poor training);
3. **environment threats** (e.g. hardware failure, power outage, faulty air conditioner that generates overheating, breakdown of mains cable and ceiling water leakage).

The risk analysis should not focus on each and every possible threat, but on what is reasonably foreseeable in relation to the data processing.

Step 3 - Identifying vulnerabilities

A vulnerability is an inherent weakness or the absence of a safeguard which a threat can exploit. Vulnerabilities may be caused by individuals, processes or technologies. The absence of functioning controls often constitutes a vulnerability in an application or system. For example, anti-virus software is used to prevent or detect malicious code. If this control is absent, this represents a vulnerability. By contrast, controls can be present, but inadequate. Using the same example, if antivirus software is present but is not updated regularly, this also represents a vulnerability.

In general, threats are linked to vulnerabilities, although it is not necessarily a one-to-one relationship. Many threats can exploit a single vulnerability. Conversely, a single control can be deployed to address multiple threats.

Example of threats and vulnerabilities

Threat	Vulnerability
1. Theft or loss	Power-on passwords and other access control devices are not used. Security devices (physical or technical) for monitoring lost or stolen laptops are missing.
2. Malicious code (e.g. viruses, worms, Trojans, spyware)	The antivirus software is not updated regularly. Users have local administrator rights and can disable or deactivate anti-virus software and download executable programs.

Step 4 - Determination of probability

The next step in the risk analysis process is to determine the likelihood that a potential threat could succeed in exploiting the vulnerabilities.

This determination of probability must be implemented while taking into account existing data security safeguards and controls. Exemplary definitions of probability classifications are described in the figure below.

Definition of probability

Level of probability	Definition of probability
Very high	The threat source is highly motivated and sufficiently capable, and controls are ineffective to prevent the vulnerability from being exploited.
High	The threat source is motivated and sufficiently capable, and controls are ineffective to prevent the vulnerability from being exploited.
Medium	The threat source is motivated and capable, but controls are in place that may prevent the vulnerability from being exploited.
Low	The threat source is ineffective, or controls are in place that may prevent, or at least significantly hinder, the vulnerability from being exploited.

Step 5 - Impact analysis

The next step in the process is to determine the potential impact of threats that successfully exploit vulnerabilities.

Step 6 - Risk calculation

The purpose of this step is to assign a risk score based on the probability that the threat will be realised, given the current controls in place and the impact to the organisation if the threat succeeds in exploiting a vulnerability. The risk score enables resources to be prioritised, and enables the areas of greatest risk to be focused on.

Irrespective of the method used, the main aim of conducting a risk analysis is to prioritise risks. This prioritisation guarantees that limited resources (e.g. financial resources, people and time) can be deployed to the highest risk areas so that vulnerabilities can be addressed and reduced.

Step 7 - Documentation of results (*STRONGLY RECOMMENDED)*

The final step in the risk analysis process is to document the results, which the organisation's functions can display by using and archiving a spreadsheet or report summarising the entire analysis.

In order to facilitate and accurately handle this step, a file is available in Excel format in the University repository, entitled "Personal data risk analysis"[6]. This file consists of 7 sheets: the first sheet "Impact and Threat Values" describes risk levels that could implicate a personal data processing operation. In the following sheets - "Impact Determination", "Assessment Questionnaire", "Threat Likelihood", "Risk Calculation", "Suggested Measures" and "Risk Weighting" - details and steps are requested which, depending on the responses, will need to a final calculation of the risk and its classification by level of severity.[7]

If the final outcome points to high severity and risk levels, then a more in-depth Data Protection Impact Assessment (DPIA) must be carried out, as described below.

It is also necessary to fill in a "Personal Data Processing Analysis Form"[8] in the context of research projects or any activities involving the processing of personal data: this Form is useful to initially map the data processing and makes it possible to certify how the intended data processing will be carried out; it is also valid as an initial self-certification in relation to the risks involved.

Risk analysis is recommended for new data processing operations or in the context of new research projects or lines of research, so that it will be possible to understand how relevant personal data will be processed.

The analysis is not a static document and can be repeated if the need arises in view of organisational or technological changes.

9. RECORD OF PROCESSING ACTIVITIES

The first summary mapping of data processing described above, also with the adoption of the Personal Data Processing Analysis Form, is followed by the compliance obligation on the Data Controller and Data Processors provided for by Article 30 of EU Regulation 2016/679: the Record of Processing Activities.

[6] The document mentioned is available in the repository at the following link:https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=8du3uH .

[7] Other risk analysis tools are available from ENISA https://www.enisa.europa.eu/risk-level-tool/ or the Spanish Data Protection Authority, https://gestiona.aepd.es/.

[8] For more details on the research projects, see paragraph 21 of this document.

It is in fact necessary, on an ongoing basis, to fill in a template in table format[9] or a special application with the information that is specifically required by the EU Regulation and also listed on page 16 of the Privacy Organisational Model of Politecnico di Milano.

The Record of Processing Activities is mandatory and not optional. The supervisory authorities must have access to these Records if they so request, particularly during inspections and when documentation is requested of data processing operations carried out.

The Data Controller and Data Processors must therefore ensure that the Record is continuously updated, and they guarantee that it will be made available if a request for access is made. The Record is regularly updated at pre-determined intervals, as the Data Controller is specifically obligated to ensure that the data processing forms which comprise the Record realistically and dynamically represent the University's data processing operations. It will be necessary, in particular, to update the Record in the event of any significant organisational, operational or technological change that could influence the management of personal data.

General notes for compiling a Data Controller/Data Processor Record

The Record is completed by entering the following information:

Data Controller's Record	**Data Processor's Record**
▪ **NAME** and **CONTACT DETAILS** of the Controller and, where applicable, of the Controller's representative and of the Data Protection Officer.	▪ **NAME** and **CONTACT DETAILS** of the Data Processor, of each Controller through which it acts, of the representative of the Controller or of the Data Processor and, where applicable, of the Data Protection Officer.
▪ **PURPOSE OF THE DATA PROCESSING**	▪ categories of **DATA PROCESSING ACTIVITIES CARRIED OUT** on the Controller's behalf.
▪ **CATEGORIES OF DATA SUBJECTS AND OF PERSONAL DATA**	▪ (where applicable) **TRANSFERS OF DATA TO NON-EU COUNTRIES and/or INTERNATIONAL ORGANISATIONS** and, for transfers referred to in Article 49.2, the documentation of adequate guarantees.

[9] The cited document is available on the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=pu1iq0 .

	.
▪ **CATEGORIES OF RECIPIENTS** (including those from non-EU countries and international organisations).	▪ (where possible) general description of the technical and organisational **SAFETY MEASURES** referred to in Article 32.
▪ (where applicable) **TRANSFERS OF DATA TO NON-EU COUNTRIES and/or INTERNATIONAL ORGANISATIONS** and, for transfers referred to in Article 49.2, the documentation of adequate guarantees.	
▪ (where possible) **DEADLINES FOR ERASURE** of the various categories of data.	
▪ (where possible) general description of the technical and organisational **SAFETY MEASURES** referred to in Article 32.	

Once filled in, the Record must be registered through the University's "Titulus" system, entering the "Data Protection Officer - DPO" as the recipient, and the classification "I/6 - Personal Data Protection".
A special guide will be made available to assist in correctly compiling the Record of Processing Activities.

10. HOW TO DRAFT A PRIVACY NOTICE

Before data is processed, the data subject must be provided with a comprehensive privacy notice, drawn up in compliance with the provisions of Article 13 of EU Regulation 2016/679.

The University's repository 'Privacy and GDPR: legislation and background information"' contains the "Privacy Notice" folder where one may find several standard forms[10], both of a general nature (see the Standard Privacy Notice, in the Italian or English version), and of a more specific nature (e.g. Privacy Notice for access to laboratories, Privacy Notice for photos/audio and video recordings, Privacy Notice for Open Days, Privacy Notice for Newsletters and Events, Privacy Notice for Visiting PhDs, Privacy Notice for questionnaires and surveys), to be adapted to the specifics of the intended data processing in question.

General notes for compiling a Privacy Notice The Data Controller and the latter's contact particulars should always be referenced at the beginning of the form. If the Controller is Politecnico di Milano, the following formula should be entered: ***"The Data Controller*** of Politecnico di Milano is the Director General on authority from the current University Chancellor - contact: ***dirgen@polimi.it***".

Then the internal Data Processor should always be referenced, with the latter's contact particulars.

The following parties must be identified as internal Data Processors in line with Privacy Organisational Model of Politecnico di Milano: the respective Area Managers or the respective Heads of Management or the respective Responsible Operating Unit Managers or the respective Scientific Coordinator in the context of research projects in which personal data are processed and which are controlled by the University.

Once the internal Data Processors have been identified, the Data Protection Officer (or DPO) should be referenced, along with his or her contact details.

The purposes of the data processing should then be summarily described i.e. a brief explanation of the reason for the data collection and processing. The legal basis for each purpose indicated should always be given, by reference to one of the criteria indicated in Article 6 of EU Regulation 2016/679, which legitimises the intended data processing, namely:

- Consent of the data subject;
- Implementation of a contract;
- Legal obligation;
- Essential/vital interest for the data subject (note: special case);
- Public interest/institutional obligation;
- Legitimate interest **(note: this does not apply to data processing by public authorities carried out in the performance of their duties, where the public interest prevails)**

[10] The cited document is available on the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

After the purposes and related details have been indicated, a list should be provided of the categories of personal data to be processed, thus distinguishing between identification data, contact data, health data, data on political opinions and any other types of data referred to in Article 9 of EU Regulation 2016/679.

The data retention period should always be indicated at this point, by including a specific and feasible time limit. Generic time references or those that fail to identify a specific interval of time should be avoided, unless this cannot in fact be identified. Illustrations of identified time intervals are provided in the table below, for guidance only[11]:

Purposes/Type of processing	**Data retention period identified**
Scientific research	At least 5 years.
Newsletter/Communication of events and initiatives	3 years.
Photos and audio/video recordings during events and initiatives	10 years.
Video surveillance	72 hours after the footage is taken. Where detriment or a criminal offence is suspected or reported, the data retention may be extended for up to 15 days, to facilitate compliance with legal obligations.
Management of tracked mail received at the Politecnico, delivered by public or private carriers, with association of data of the external sender and of the internal recipient.	2 years.
Provision of library services.	10 years.

[11] The definition of a time interval is closely linked to the specific characteristics of the individual data processing operation intended. However, the table is illustrative only and gives a number of examples of time intervals that have been defined and deployed in recent privacy notices.

Health surveillance activities and other workplace health and safety protection obligations.	20 years from the date of termination of employment for workers exposed to ionising radiation; 10 years from the date of termination of employment for all other workers.

The nature of the data processing should then always be indicated i.e. whether the provision of the requested data is optional (if the purpose of the data processing is legitimised by the data subject's consent or, even if consent is not forthcoming, where data-processing for other purposes is not compromised) or mandatory (e.g. if the data must be provided in order to comply with a legal or contractual obligation), in order to avail of the proposed service.

If the data processing involves special categories of personal data, as defined in Article 9 of EU Regulation 2016/679, a more detailed explanatory paragraph of the type of data processed is included.

Next, important information must be provided on the methods by which the data processing will be carried out, highlighting any profiling activities as appropriate.

This paragraph should also indicate the presence (if any) of "authorised" persons i.e. those granted authority to process data as defined by the Privacy Organisational Model of Politecnico di Milano on page 13 (e.g. technical-administrative personnel, Teachers, Researchers, Research Fellows, Scholarship or Grant holders, Students and others).

Next, it is necessary to indicate a list of third party recipients (if any) to whom the data subject's personal data needs to be transmitted in order to ensure they can perform their activities and to fully realise the purposes anticipated. These may be public or private entities or bodies also simultaneously classified as external Data Processors.

It must always be indicated whether a data transfer to non-EU countries is envisaged, and guarantees of the adequacy of data security levels provided for by EU Regulation 2016/679 should always be referenced. If data transfer is not anticipated, a paragraph entitled "Transfer to non-EU countries" should be included in any case, in which it is stated that personal data will not be transferred to any non-EU country.

The list of the data subject's rights and entitlements should always be indicated at the end of the Privacy Notice (rights pursuant to Articles 16, 17, 18, 19, 20, 21 of EU Regulation 2016/679) and contact details should be provided in order to properly claim those rights (for Politecnico di Milano: privacy@polimi.it).

If the data processing involves the taking of photographs and/or audio and video recordings, for publication on social networks, the Privacy Notice should reference (preferably before the section on the nature of the data processed) the specific rules on copyright and use of images/video recordings.

In other words, the text of the Privacy Notice should be supplemented with the following (illustrative) text:

"We hereby inform you that for the anticipated Purposes of the data processing, with particular reference to Purpose no. ..., the data subject may be involved in audio-video filming and recording. Data processed, including images, audio/video footage and recordings (hereinafter, "Images") which are made during the event (even in partial and/or modified or adapted form) will be processed in full compliance with EU Regulation 2016/679. The data will be processed, also electronically, by persons who are specifically assigned in relation to the dissemination and communication activities of the Controller/Co-Controllers. Images collected will be stored, also in electronic form and on any technology media, for the purposes and subject to the limits defined above, and may be disseminated in compliance with Law 150/2000 on institutional websites and on social network channels (e.g. Facebook, Twitter, Youtube). There shall be no entitlement to remuneration for the use of the images. The Controller/Co-Controller may access or disclose the user's Images without the requirement for the latter's consent, in accordance with the provisions of Article 97 of Law 633/1941. This authorisation entails the grant of a non-exclusive worldwide licence transferable to third parties, and unlimited in duration, for the use of Materials and includes the rights referred to in Articles 12 to 19 of Law No. 633 of 22 April 1941, including (without limitation) the following rights: publication; reproduction in any manner or form; transcription, editing, adaptation, elaboration and reduction; communication and distribution to the public, including the rights of projection, transmission and broadcast, also in summary and/or abbreviated form, by any technical means; the right to keep a copy of Materials, also in electronic form and on any existing or future technology media, for the purposes and subject to the limits defined above. Any use of Images that could compromise the good name and reputation of the person portrayed, filmed or recorded is excluded pursuant to the aforementioned article and also to Article 10 of the Italian Civil Code".

N.B.

The particular case of **public or institutional events** arises in relation to images and audio/video recordings: here it is not necessary to obtain a special release or waiver from the participant, unless photos and video recordings featuring him/her are collected in a targeted and deliberate manner. It is good practice, however, to use special signs (e.g. at the entrance to the room or space, or the place where the event is held) to indicate that photographic sessions and video/audio recordings involving participants may be taking place at that time.

Once it has been drafted, the Privacy Notice can be presented to the data subject either in paper form or electronically by means of a web link in a forum/first access page (e.g. event registration page). The important thing is that it is fully accessible to the data subject.

11. THE DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Article 35 of EU Regulation 2016/679 provides for a so-called Data protection impact assessment i.e. the assessment of risk inherent in the data processing. This assessment must be carried out if the data processing operations involve:

- profiling or other automated data processing operations;
- processing of special data on a large scale (Article 9.1 of EU Regulation 2016/679) or of data on criminal convictions and offences (Article 10 of EU Regulation 2016/679);
- large-scale systematic surveillance of public areas.

The Data Controller and Data Processors carry out a data protection impact assessment prior to the data processing, in order to assess the probability and severity of the risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. The impact assessment should also, in particular, address the measures, safeguards and mechanisms in place to mitigate that risk.
There are data processing operations for which a DPIA is mandatory: these are identified in the EU Regulation 2016/679 and in the general measure of the Italian Data Protection Authority of 11 November 2018. The DPIA implementation methods are described in detail in the DPIA procedure, which may be accessed in the University repository "Privacy and GDPR: legislation and background material"[12].

12. EXERCISE OF RIGHTS

Rights may be exercised in relation to the University by sending a written request to this effect, without special formalities, to privacy@polimi.it.The University must reply to the data subject within 30 days of receiving the request, or 90 days in cases of particular complexity, duly documented. The reply may also be provided in verbal form; however, if specifically requested, the Administration is obliged to transfer the data onto paper or digital media or to transmit them to the data subject electronically, by the communications method by which the request was received.
If an individual function receives a request for the exercise of rights, it should be forwarded to privacy@polimi.it, which will assess and process the request.

[12] The cited document is available on the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

.

1. Right of access by the data subject

According to Article 15 of EU Regulation 2016/679, the data subject has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and to the following information:

a. the purposes of the processing;
b. the categories of personal data concerned;
c. (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e. the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f. the right to lodge a complaint with a supervisory authority;
g. where the personal data are not collected from the data subject, any available information as to their source;
h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data is transferred to a third country or an international organisation, the data subject has the right to be informed of the existence of appropriate safeguards pursuant to Article 46 of EU Regulation 2016/679 relating to the transfer.

2. Right of rectification

According to Article 16 of EU Regulation 2016/679, the data subject has the right to obtain from the Data Controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right of erasure (right to be forgotten)

As set out in Article 17 of EU Regulation 2016/679, the data subject has

the right 'to be forgotten', effectively, the right to have one's personal data erased in an enhanced form. Data Controllers are obliged (if they have "made public" the data subject's personal data e.g. by publishing them on a website) to notify this erasure request to other controllers that are processing the personal data subject to erasure, including "any link, copy or replication" (see Article 17.2 of EU Regulation 2016/679). It has a broader scope than the previous Personal Data Protection Code, as the data subject is entitled to request the erasure of his or her data, for example, even after consent to the data processing has been withdrawn (see Article 17.1 of EU Regulation 2016/679).

4. Right to restriction of data processing

This is a different and more extensive right in comparison with the provisions of the previous Personal Data Protection Code: specifically, it can be exercised not only in case of a breach of the conditions for lawful processing (as an alternative to the erasure of data), but also if the data subject requests the rectification of data (pending such rectification by the Controller) or objects to their processing pursuant to Article 21 of EU Regulation 2016/679 (pending assessment by the Controller). With the exclusion of data storage, any other processing of data in relation to which restriction is requested is forbidden, unless certain preconditions are present (consent of the data subject, establishment of rights in court, protection of rights of another natural or legal person, reasons of substantial public interest). The right to restriction requires that personal data be "marked" pending further decision or assessment; accordingly, the Data Controller should adopt suitable measures for this purpose in its own electronic or other IT systems.

5. Right to data portability

This is one of the new rights under EU Regulation 2016/679, although it is not entirely unknown to consumers (think of telephone number portability). It does not apply to non-automated data processing (so it does not apply to paper-based archives or records) or where the data processing is based on the public interest or the legitimate interest of the Data Controller. Therefore, specific conditions are laid down for its exercise; in particular, only data processed with the consent of the data subject or on the basis of a contract entered into with the data subject (), and only data which the data subject has "provided" to the Data Controller, are portable (see recital 68 of the EU Regulation). In addition, the Data Controller must be able to directly transfer the portable data to another data controller indicated by the data subject, if technically possible.

6. Right of objection

As set out in Article 21 of EU Regulation 2016/679, the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6.1, including profiling based on those provisions.

The Data Controller must no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

7. Management of applications from Data Subjects

When a request is received from data subjects for the exercise of one of the rights granted to them under the EU Regulation, and addressed to the Data Controller or the Data Protection Officer (DPO), the Privacy Management Office is responsible for taking charge of the request and involving delegated officials with competence in relation to the scope of the request. It shall also submit the request to a preliminary examination and attendant assessment, ensuring that response time frames are in conformity with those indicated by EU Regulation 2016/679.

In addition, the Privacy Management Office must register the application received in the Register of Data Subjects' Petitions (Annex 2).

8. Automated decision-making process (profiling)

As set out in Article 22 of EU Regulation 2016/679, the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

This principle does not apply if the decision:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent.

In order for data subjects to exercise their rights, a special procedures for **REQUESTING THE EXERCISE OF RIGHTS**, must be followed, to which reference is made.

13. DESIGNATION OF EXTERNAL DATA PROCESSOR

The Privacy Organisational Model of Politecnico di Milano defines External Data Processors as any persons extraneous to the administration who are required, based on an agreement, contract, procurement award record or appointment, to process personal data on behalf of the Controller. This relationship between Data Controller and External Data Processor must therefore be formalised by means of a special deed of appointment.

Three different models have been developed and are currently available at the University, each of which is linked to different risk circumstances entailed by a data processing operation. In fact, the original "medium" risk model (of May 2019) was supplemented by a "light risk" model for cases that present a limited level of risk; there is, finally, a model that contains a description of relevant data security measures, which is more recent and more complete than the others and is suitable for more complex and potentially high-risk data processing operations.

As a rule, the choice of model is assessed on a case-by-case basis, depending on the data processing operation being considered, and taking into account the underlying risk.

Managers, Heads of Management and Department Managers - within the scope of their respective competences in contractual matters and in their capacity as internal Data Processors - are assigned the task of drawing up and signing legal instruments for the management of data processing, with external parties who collaborate with Politecnico di Milano in the exercise of its institutional functions.

External Data Processors are appointed by internal Data Processors (Managers, Heads of Management and Department Directors). The choice of the external Data Processors is made only after the most suitable position has been identified, as the same persons could also be qualified to act instead as independent Controllers or Co-Controllers of the data processing (or indeed, as persons granted authority to carry out ordinary data processing operations). In addition to the qualification factors of external Data Processors, internal Data Processors are responsible for providing them with instructions related to the position conferred.

The deed of appointment as external Data Processor is deemed to be attached to the contract signed by the parties and, as such, should have the same index number as that contract.

If no contract exists to which the deed of appointment as external Data Processor can be attached, it should be indexed under the item "contracts".

N.B. N.B. If a Politecnico di Milano function or facility is appointed by another Controller to act as "External Data Processor", an Excel template of the Data Processing Register - Sheet "Acknowledgement of Data Processor Register" in the repository[13] should be compiled and communicated to the DPO at privacy@polimi.it.

[13] The cited document is available on the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-

In this case, the Appointment should be registered using the University's "Titulus" system, entering as the addressee (with reference copy) ("Data Protection Officer - DPO" and the classification "I/6 - Personal Data Protection".

14. DESIGNATION OF AUTHORISED PERSONS

Internal Data Processors identify "authorised" persons, i.e. individuals who are authorised to carry out data processing operations pursuant to Article 29 of EU Regulation 2016/679. In concrete terms, authorised persons are all those who handle data on a daily basis in paper or digital form, namely: technical-administrative personnel, lecturers, researchers, scholarship holders, 150-hour students and collaborators of various kinds[14].

They are formally appointed by filling in the relevant University form[15] or using the privacy management application.

Doctoral students must also receive authorisation to process personal data from the Scientific Coordinator/Tutor of their research project, for the entire duration of their course. If the doctoral student is an active participant in more than one research project different from and addition to the one initially envisaged, then the Scientific Coordinator of the new project considered must sign the appropriate authorisation for the processing of data, for each additional research project.

Authorised persons are obliged to process personal data, to which they have access, in accordance with the Data Controller's instructions, paying attention to the nature and purpose of the data processing carried out, the types of personal data being processed and the technical and organisational measures implemented for the proper protection of personal data. In addition, they receive adequate training and specific instructions from the internal Data Processor at the time of their appointment. Persons to be recruited after their appointment should also receive adequate training in the area of personal data processing and protection.

Specifically, authorised persons have the following obligations:

- to keep strictly confidential their activities and any information which they receive in the context of those activities;
- not, without proper authorisation, to communicate to third parties or to disseminate (using electronic means or otherwise) news, information or data acquired in connection with facts and circumstances that have come to their attention in their capacity as persons authorised to process personal data, as a result of the activities carried out;

GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=EGjUWJ .

[14]Students writing theses, 150 hour-students and collaborators are appointed by the Scientific Coordinator in relation to research activities or by the Head of Management in relation to administrative and management activities.

[15] The cited document is available on the repository at the following link: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?viewid=5aec781e%2Dc4c2%2D487c%2Db0af%2Dba781f7fb0bf&id=%2Fsites%2FPriv

acy%2DGDPR%2FDocumenti%2FAutorizzazione%20soggetti%20esterni .

.

- to attend information and training seminars on personal data protection, which are mandatory in view of the new provisions of the European data protection regulation, and to sit relevant learning verification tests;
- to promptly notify their internal Data Processor of any anomalies, incidents, thefts, accidental losses of data, so that the procedures for notifying data breaches to the Italian Data Protection Authority and to the data subjects concerned can be initiated, if a serious risk exists that the rights and freedoms of individuals have been seriously compromised (data breach).

15. CO-CONTROLLER AGREEMENT

Where a joint control relationship exists in relation to a data processing, the co-controllers are obliged to draw up a co-control agreement, using the standard template prepared for the various facilities or functions of Politecnico di Milano which is available in the repository[16].

More specifically, this is required where two or more data controllers together determine the purposes and methods of the data processing i.e. they decide together to process data for common purposes and using procedures that are mutually determined. Therefore co-control represents, in effect, a declaration of shared responsibility by each individual (Co-)Controller.

If a University facility or function receives a proposal for co-control of a personal data processing, the DPO should be contacted so that the required assessments can be carried out.

Managers, Heads of Management and Department Managers - within the scope of their respective competences in contractual matters and in their capacity as internal Data Processors - are assigned the task of drawing up and signing legal instruments for the management of data processing, with external parties who collaborate with Politecnico di Milano in the exercise of its institutional functions.

Once signed by the parties involved, the Agreement should be registered using the University's "Titulus" system, entering as the addressee ("Data Protection Officer - DPO" and the classification "I/6 - Personal Data Protection".

16. DATA BREACH PROCEDURE

EU Regulation 2016/679 provides that the Data Controller must “without undue delay” and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach, unless it is considered unlikely to compromise the rights and freedoms of natural persons.

[16] The cited document is available in the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .

. In any case, failure to report a data breach must be adequately justified. Therefore, it is not mandatory to notify a data breach, as the obligation depends on an assessment, by the Data Controller, of the risk entailed for data subjects .

The University has drawn up a procedure and special forms for reporting data breaches. If a data breach occurs, the person who initially becomes aware of the data breach is obliged to report it immediately to the Coordinator identified in the structure/facility or to the Manager, or (in the case of Departments) to the Department Coordinator or Department Manager. These persons must, in turn (within the following 24 hours) email the report to the DPO to databreach@polimi.it.

More specifically, in the event of a manifest personal data breach, the following five steps should be observed, two of which may/may not be applicable:

Step 1: Identification and preliminary investigation;

Step 2: Containment, recovery and risk assessment;

Step 3: Notification to the Italian Data Protection

Authority (as applicable); **Step 4:** Notification to data

subjects (as applicable); Step **5:** Documentation of

the breach.

Further details for each step are explained in the **DATA BREACH PROCEDURE.**

17. COMPUTER INCIDENT LOG

If a personal data breach occurs as a result of any kind of IT event, this should be reported and an incident log compiled.

The incident log should have the following contents:

- a description of the nature or type of personal data breach (misconduct, hardware or other issues), including, where possible, the categories and approximate number of data subjects involved and the categories and approximate number of personal data records;

- a report on any communication made to data subjects affected by the personal data breach, indicating the contact point for information and assistance;
- a description of the probable consequences of the data breach;
- a description of the measures taken or proposed to remedy the data breach and also, where feasible, to mitigate its potential negative effects.

The requirement to communicate to the data subject is dependent on the nature of the personal data breach. Communication to the data subject is not required if one of the following conditions is satisfied:

a) the Data Controller has already adopted suitable technical and organisational safeguards;
b) the Data Controller has subsequently adopted measures to prevent the emergence of a high risk to the rights and freedoms of the data subjects.

18. DATA TRANSFER OUTSIDE THE EU AREA

The European Regulation has specific rules for data transfers abroad. In general, the transfer of personal data outside the EEA Area is permitted if the recipient can guarantee a level of data protection that is adequate to European data protection levels in force. Procedures for managing a transfer of personal data to non-EU countries must be based on information provided in the procedure **TRANSFERRING DATA ABROAD** contained in the dedicated folder in the repository[17].

19. SPECIFIC CASES OF PERSONAL DATA PROCESSING

Recording of lessons by students

Students are entitled to record the lessons they attend exclusively for personal and individual study purposes, as also explained by the Italian Data Protection Authority in the document "School and data privacy. Frequently asked questions", published on its website on 12/12/2019. [18].

Any other use or dissemination, including on the Internet, of the recorded lesson requires the express consent of those involved in the recording (teachers, other students, etc.).

[17] The cited document is available in the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=7t9Wfz .
[18] Link to Italian Data Protection Authority website: https://www.garanteprivacy.it/home/faq/scuola-e-privacy .

Use of electronic mail

The University provides its users with an institutional e-mail box belonging to the "POLIMI.IT" domain or to an appropriate sub-domain. E-mail is an institutional tool for internal and external communication within the University. The use of this mailbox represents a processing of personal data.

The user must use his/her e-mail account only for teaching, research and administrative purposes and for other activities that are instrumental or related to the University's institutional purposes, in compliance with the provisions of applicable rules and without causing detriment to Politecnico di Milano or to third parties.

The use of the email account for personal purposes is permitted within the “reasonable use” principle and exclusively for purposes that are not contrary to law, public order or public morality; nor shall the email account be used in such a way as to cause detriment to the University, or compromise the proper functioning of information systems or undermine the employee's professional responsibilities.

It is forbidden to utilise the institutional email address in online registration forms used for personal purposes, which may result in spam or malware being sent to the mailbox.

The user may not use electronic mail to transmit (including by means of links or attachments in any format) messages containing or referencing:

a. Non-institutional advertising (overt or covert);
b. Private commercial communications;
c. Communications of political propaganda outside the University;
d. Pornographic material or similar;
e. Material that is discriminatory or harmful in relation to race, gender, religion, etc;
f. Material that violates data privacy legislation;
g. Content or material that infringes the property rights of third parties;
h. Defamatory or manifestly offensive content;
i. Other illegal content.

The list is not exhaustive and may be applied by analogy.

Users should not act in a way that compromises the University's IT security when consulting their emails. In particular:

- ✓ beware of messages or attachments from unknown or untrustworthy senders and, if you cannot identify the sender, do not open them;

- ✓ do not open attachments of e-mail messages with an executable extension (e.g. .exe, .bat, .com);
- ✓ scan e-mail attachments with antivirus software before opening them;

Users should consult their mailboxes regularly.

The user assumes all criminal and civil liability, including any costs, expenses and burdens associated with the improper or illegitimate use of electronic mail. The user shall not use the service in such a way as to undermine or jeopardise its use by other users.

Without prejudice to possible criminal liability, the improper or legitimate use of electronic mail will trigger disciplinary liability pursuant to the Disciplinary Code, contained in the National Collective Labour Agreement (CCNL) for the relevant sector.

Limitations on the space available to each user are also defined: in order to guarantee that the e-mail system functions properly, each user is requested to keep their assigned mailbox organised by deleting unnecessary and/or bulky files and attachments.

Messages with very large attachments or with a large number of recipients should only be sent when strictly necessary, in order not to encumber the University's e-mail service.

It is possible for email to be intercepted by outsiders; therefore, it should not be used to send strictly confidential work documents or those that contain sensitive data. The sender should deploy protection tools such as encryption where such data communications are required for work purposes.

If the user receives a message with suspicious content or from an untrusted sender, he or she should notify ASICT (the ICT Service Area of Politecnico di Milano) and refrain from acting on the message in any way (opening a link, previewing it) or on any attachments (storing, opening or executing a file).

N.B.

Example of secure transmission of documents in digital format

To ensure **confidentiality, integrity and availability of the transmitted data,** asymmetric encryption can be used, with reading keys. The recipient will be required to provide his public key, which will be used to encrypt the document in digital format (using the GPG4Win software available for managed workstations). Then we will send the documents via FileSender and, once received, the recipient will decrypt the data using one’s own private key.

Protecting one's own account

Each employee is assigned a personal account to access the information system and all related services. The account represents the computer identity of the user and must be carefully and diligently managed: each event generated by a specific account is attributed to its legitimate assignee.

The password must remain secret, and should not be disclosed to any person, written on sheets of paper or stored on unprotected media.

To minimise the risk of theft, passwords should be entered out of eyeshot of third parties, and should be changed on a regular basis.

It is therefore forbidden to:

- share one's personal account with others, including colleagues;
- use an account different from one that the University has assigned in order to interface with the University's IT systems that require authentication (e.g. accessing University IT systems using access credentials you are not authorised to use).

Workstation protection

Each workstation is configured by ASICT personnel to ensure full functionality. For security reasons the user is not authorised:

- to modify system or application settings;
- to modify network parameters;
- to change network sockets, i.e. using network sockets other than those assigned;
- to install unauthorised programmes;
- to remove or alter identification labels.

If a fault occurs, the user is responsible for notifying ASICT personnel of this by opening a ticket on a dedicated report management system .

It is good practice, in general, for an employee/collaborator to regularly clean up his or her files, deleting obsolete, useless or duplicate files.

The workstation is also, potentially, a target for information theft. One should therefore:

- keep one's desk as clear as possible, filing away any documents containing sensitive information;

- use the screen lock function when leaving one’s workstation in order to conceal on-screen data in use;
- lock drawers and cabinets containing sensitive information (including judicial information) outside working hours or if absent for over one hour;
- report any unusual workstation configurations or suspicious activities to ASICT personnel.

Below are some examples of suspicious behaviour:

- a user insists on accessing another’s data or knowing another user's password;
- a user or outsider requests to use a workstation without authorisation;
- an outsider requests information or unusual operations at the workstation;
- an unusual e-mail requests information or suggests clicking on a suspicious link.

To protect one's computer from viruses and other active attack agents, data or programmes should not be used if their origin is uncertain: a malicious programme could also originate from a trusted but innocent user, or be falsified.

If a smart working/teleworking employee uses a workstation that is centrally managed by ASICT, he/she should ensure that the same safeguards are adopted as those in place to protect the aforementioned workstation, also in the remote working context. In particular, ASICT reserves the right to disconnect and prevent access to any device initially authorised for smart working/teleworking purposes, where the device in question is not correctly used, particularly where attempts are made to compromise the University infrastructure.

More generally, devices connected by VPN (centrally managed or otherwise) are considered to be an extension of the University network’s security perimeter and therefore the same measures, principles and considerations apply to them, in terms of infrastructure protection.

University Hosting and Housing Services

ASICT offers hosting and housing services at the University's data centres to eligible users according to procedures described at https://hosting.polimi.it/

In particular, users of Hosting and Housing services are obliged to observant respect the thematic security policy available on the site.

ASICT reserves the right to disconnect, prevent access to or disable any hosted system that seeks to compromise the University's ICT infrastructure or that is compromised following a cyber attack.

Application cooperation (application integration)

Application cooperation services can be used only in Business2Business (B2B) scenarios within the University, e.g. between information systems managed by ASICT and departmental systems.

ASICT is responsible for evaluating and, as appropriate, authorising application cooperation requests, to be assessed on a case-by-case basis. ASICT is entitled to suspend, block or deactivate application cooperation services provided if this is justified for IT security reasons or if improper use has been detected.

If data transferred by means of application cooperation to the recipient system are to be displayed, they must not be manipulated in any way, de-contextualised or used in an outdated form by the latter.

Data network and internet connectivity

The computer and telecommunications network and ICT services of Politecnico di Milano constitute a shared asset of the University; as work tools and as means for promoting academic, research, teaching, third mission and infrastructure logistics activities, they are subject to restrictions on use if infringements are ascertained that could compromise their functioning or legal compliance. Personal use, where not specifically prohibited, must be based on good faith and moderation: uses that risk damaging the functionality of the tools or the image of the University will not be permitted in any circumstances.

ASICT reserves the right to disconnect, prevent access to or disable any network device that is unauthorised or that seeks to compromise the University's ICT infrastructure.

The Human Resources and Organisation Area (ARUO) can request to restrict or prevent access to the Internet for personal use on the University network, in relation to certain categories of websites that are not relevant for work purposes and/or to restrict access to the Internet at certain times.

The University also reserves the right to minimise risks to the ICT infrastructure arising from inappropriate use of the data network or of online browsing. ASICT is entitled to inspect users' encrypted web browsing in order to prevent unlawful conduct and/or potential criminal acts. In order to guarantee data security and the optimal functioning of the system, so as to safeguard the University's assets, it may deploy special automated hardware and software (antivirus, antispam, content filtering) and implement Black Lists as appropriate.

The use of the University's IT tools for remote working (e.g. teleworking or smart working) requires the same infrastructural safeguards as those in place for activities carried out in person, e.g. the connection of users linked by VPN to the University network gives the same level of control in terms of filtering as when users are connected in person from the head office.

Storage media

Mobile media and memory storage devices are a privileged vehicle when it comes to viruses and to offences that breach information confidentiality and systems security. The use of these media and devices in the University IT system should be limited to the exchange of working files only where it is not technically possible or economically viable to use alternative transfer methods (e-mail, shared network folder, direct file transfer).

Files contained in magnetic/optical media must not be downloaded for purposes other than work activities, and never outside the specifically permitted cases. If storage media are used for the processing of sensitive or judicial data, their use is strictly limited to the permitted circumstances and the authorised personnel; re-use is permitted only after ASICT personnel has securely erased the data, in conformity with the general provision of the Italian Data Protection Authority of 13 October 2008 (Waste of electrical and electronic equipment - *RAAE*) and with personal data security measures).

In general, the use of personal media and mobile memory storage devices for storing files and service information is not permitted.

Mixed use of mobile devices

The use of University mobile phones and smartphones for personal, non-work-related purposes is permitted in accordance with the principle of reasonable use and, in any case, for purposes that are not inconsistent with the law, public order or public morality, nor should they be used in ways that could cause detriment or harm to the University or compromise the proper functioning of the devices.

Abandonment and loss of devices

It is forbidden to leave these devices in public places or vehicles, or to leave them unattended even for short periods, including outside one’s immediate line of vision. The use of anti-theft devices (e.g. Kensington cable) is recommended, if available.

If University mobile property assigned to an employee is lost or stolen, it is the employee's responsibility to report this to the competent authorities within twenty-four hours. A copy of the report must be sent to ASICT, to enable action to be taken to ensure the confidentiality of the information.

ASICT-provided mobile phones and smartphones

Service mobile phones, SIM cards and ancillary equipment are University property. Mobile phones/smartphones are assigned for work reasons only, and their purpose is to facilitate contact with colleagues and ensure traceability (business trips, on-call periods). This also applies where a SIM card is allocated, or in the case of GSM/UMTS equipment for data transmission/reception purposes. The assignee must take the utmost care to keep the equipment safe and in good condition, promptly reporting any faults and malfunctions.

Upon termination of the employment/collaboration, mobile phones must be returned to ASICT in good condition together with the SIM card - unless ASICT has authorised number portability - and with all ancillary equipment by the final day of work at the latest.

If it is not returned, ASICT will immediately disable the SIM card for outgoing traffic; the mobile phone IMEI code will be reported to the operator, for blocking. ASICT also reserves the right to charge any higher costs (all or some) resulting from the failure to return a mobile phone by the appointed date.

Pseudonymisation, anonymisation and minimisation of personal data

- **Anonymised data** is data that has been stripped of all identifying elements. Anonymised data are not considered to be personal data and are therefore not subject to data protection rules. It is possible that the data may need to be stored for purposes of statistical, historical or scientific activities even after the projected data processing purposes have been fulfilled. In this case, suitable measures must be adopted to counter any possible misuse of the data.
- **Pseudonymised data** are personal data in which the identifying elements have been substituted by different elements, such as strings of characters or numbers (hashes), or by substituting a nickname for the name, provided that it makes it difficult to identify the data subject. Obviously, the person that holds the decryption key for decrypting the data (i.e. linking the pseudonym element to the personal data) must guarantee adequate measures against possible misuse.

  Pseudonymised data, unlike anonymised data, are still personal data (as they enable the person to be directly or indirectly identified by cross-referencing with other information), although benefiting from lower levels of protection than in the case of personal data properly so called.
- **Data minimisation,** on the other hand, means that only relevant data should be collected, i.e. the data processing should be limited to data that are in fact necessary and indispensable for their intended purpose. Data minimisation is a key principle (principle of data relevance) governing the processing of personal data, as a data processing must always be limited to strictly necessary data, in accordance with EU law.

Example

Pseudonymisation, therefore, means the replacement of true identification data with false identification data so that:

- third parties are unable to associate the personal data with a natural person (data subject);
- the Data Controller or Data Processor may implement the re-association as required.

These characteristics yield two essential corollaries:

1. the pseudonymisation process produces two objects, against a starting dataset: the first object is a dataset which, for each data subject, contains the pseudonym and the personal data concerning him or her (but which cannot identify him or her in any way), while the second object is a dataset which contains, again for each data subject, the pseudonym and the data that enable him or her to be identified;
2. the second dataset must be kept separate from the first dataset, it must be suitably protected, it must remain in the exclusive possession of the Data Controller or the Data Processor and must only be used when strictly necessary for the purposes intended.

For example, where a school register is kept on an electronic spreadsheet containing the following information:

1. pupil’s first and last name;
2. place and date of birth of the pupil;
3. pupil’s address;
4. father’s first and last name;
5. mother's first and last name;
6. number of siblings of the pupil;
7. Equivalent Economic Situation Indicator (ISEE) of the household;
8. the pupil's favourite sport;
9. grades for the last quarter.

Which records should be pseudonymised? The answer clearly depends on the context. Certainly the data in point 1 are directly identifiable, but the data in points 2, 3, 4 and 5 could also be considered indirectly identifiable if, for example, the Data Controller were a school in a town with 10,000 inhabitants: in such a small context, knowing the mother's first and last name could easily permit the pupil's identification. Accordingly, the pseudonymisation process must divide the initial dataset into two parts, which will be formed in this way:

dataset1

- ✓ pseudonym;
- ✓ number of siblings of the pupil;
- ✓ Equivalent Economic Situation Indicator (ISEE) of the household;
- ✓ the pupil's favourite sport;
- ✓ grades for the last quarter.

dataset2

- ✓ pseudonym;
- ✓ pupil's first and last name;
- ✓ place and date of birth of the pupil;
- ✓ pupil's address;
- ✓ father's first and last name;
- ✓ mother's first and last name.

Dataset 2, in line with the provisions of EU Regulation 2016/679, clearly constitutes additional information which enables dataset1 to be read correctly, and it must therefore be "stored separately and subject to technical and organisational measures to ensure that such personal data are not attributed to an identified or identifiable natural person". Obviously, the technical and organisational measures put in place to protect the additional information (i.e. dataset2) will no longer be based on pseudonymisation, but will need to be different in kind.

In fact, depending on the context and to make matters even more complex, the data referenced in points 7 and 8 of the records could indirectly identify a person if, statistically, they are broadly out of range (outliers). Again, to take the example of a school in a town of 10,000 inhabitants, the fact that a pupil has 12 siblings is an outlier that uniquely identifies him or her. Therefore the pseudonymisation process should be preceded by a thorough statistical analysis (quantitative as well as qualitative data) in order to ensure that data capable of identifying data subjects can be precisely identified.

What distinguishes pseudonymisation from anonymisation?

The possibility to re-associate personal data with a data subject: in case of pseudonymisation this is possible (if the Data Controller or Data Processor uses the additional information), but this is no longer possible in case of anonymisation. Anonymised data are no longer personal data and will never be again (irreversible process), provided that the anonymisation is done correctly.

Going back to our example, if the source register needs to be anonymised, it will be necessary to delete any personal data that could directly or indirectly identify the data subject (i.e. the data contained in points 1, 2, 3, 4, 5). Moreover, an effective anonymisation, in addition to erasing data that directly or indirectly identify the data subject, should restore (as far as possible) the other data to within generic ranges. To return to our example, the number of siblings should no longer be represented by an exact number but by a position within numeric ranges: 0 to 2, 3 to 5, over 5.

Documents published by the European Data Protection Authority and/or by other authorities on the use of these techniques in the anonymisation and pseudonymisation field, are available in the repository[19].

20. DATA-PROCESSING AND FREEDOM OF INFORMATION AND EXPRESSION

Data protection is not an absolute right. It must be balanced with other fundamental freedoms such as the right to freedom of expression and information in the academic, artistic or literary field. This provision is contained in Article 85 of EU Regulation No 2016/679 "*Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression*". In this context, for data processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States are authorised under Article 85 of EU Regulation 2016/679 to provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (data controller and data processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information. The scope of the exemptions from the provisions of the GDPR is broader, here, than the special regime for scientific research dealt with in the next paragraph.

[19] The cited document is available in the repository at the following link: https://polimi365.sharepoint.com/:f:/r/sites/Privacy-GDPR/Documenti/Documenti%20Istruzioni%20operative?csf=1&e=RfoMds .

. The processing of personal data for the purposes of 'academic expression' entails:

a. Data processing that is directly linked to the freedom of academics to disseminate information;

b. The freedom of academics to disseminate knowledge and truth without restriction, such as publication or the dissemination of research results;

The sharing of data and methodologies with colleagues and exchanging views and opinions[20]

Accordingly, the Personal Data Protection Code specifically regulates data processing operations for journalistic purposes and for other expressions of thought, by providing in letter c) of the first paragraph that this balancing act includes data processing 'aimed exclusively at the publication or dissemination, occasional or otherwise, of articles, essays and other expressions of thought, including academic, artistic and literary expressions'.

According to Article 137 of the Code, special and judicial data may be processed for the aforementioned purposes, without consent.

Article 137 also provides for exemptions where data are transferred for purposes of academic expression, as a number of provisions do not apply, the most significant being the transfer of data to third countries or to international organisations contained in Chapter V of the regulation.

21. INSTRUCTIONS FOR DATA PROCESSING IN THE RESEARCH FIELD

Research activities should be preceded by the drafting of documents which document data processing activities for effective statistical and/or scientific purposes in compliance with applicable ethical standards.

Therefore, the research team should implement the following procedures:

1. **To draw up a Personal data processing analysis form[21] if the subject of the research entails the use of personal data:**
   - **a.** which is drafted in conformity with methodological standards applicable in the relevant subject area;
   - **b.** which documents the implementation of the data processing for appropriate and effective statistical and scientific purposes, specified therein.

[20] Sorguç v. Turkey App no 17089/03 (ECHR, 23 June 2009), para. 35. The ECHR has understood "academic" freedom as the ability to freely express one's opinion about the institution or system in which they work and the freedom to disseminate knowledge and truth without restriction. The Court, in this context, cited Recommendation 1762 (2006) of the Parliamentary Assembly of the Council of Europe on the protection of academic freedom of expression, where it is stated that academic freedom in research and education should guarantee freedom of expression and action, freedom to disseminate information and freedom to conduct research and disseminate knowledge and truth without restriction.

[21] The cited document is available on the repository at the following link:https://polimi365.sharepoint.com/:x:/r/sites/Privacy-GDPR/Documenti/5.%20SCHEDA%20ANALISI%20ATTIVITA%27/NUOVA%20Scheda%20analisi%20attivit%C3%A0.xlsx?d=wd74fd67d72e443ac9259c4a966dcc652&csf=1&web=1&e=pqefDV .

2. To draft a Privacy Notice pursuant to Article 13 of Regulation (EU) 2016/679;

3. Filing of the Project and related documentation with the relevant Department:

a. The project manager files the analysis form with the relevant department, which ensures it is kept confidential (not public).

b. The project may be consulted only for the purposes of applying personal data protection rules.

c. The file should be kept only for five years from the projected research end date.

4. Communication of data to other universities and/or research bodies and dissemination.

In order to promote and support research and collaboration in the scientific field, personal data may be disclosed, without identification markers, to a university or research body or to a researcher based on a special written request, indicating the specific scientific or statistical research purpose for which the data are sought. In this case the applicant should:

a. Indicate the following elements in his/her disclosure request:

- the purpose of the processing;
- the nature and type of data required;
- a declaration that processing activities will not be carried out for purposes other than those indicated;
- an undertaking not to disclose data received to unauthorised third parties;
- the specific reason justifying the possible use of identification data, where it is not possible to obtain the research results in any other way . (This justifying reason should be examined by the original Data Controller);

b. Attach a copy of the research project in respect of which the data are requested.

The party receiving the request (the original Data Controller):

- assesses the request for data disclosure and the purposes indicated therein;
- determines the procedures for exclusion in compliance with the principle of relevance and strict necessity, and observing any relevant data security measures;
- files the disclosure request and the attached research project with the relevant department, which will store it confidentially for five years from the projected research end date.

It is permitted to disseminate the research results (including through publication) exclusively in aggregate form or according to procedures which prevent data subjects from being identified, including by indirect identification data, unless the dissemination involves public variables.

Requirements for personal data processing conducted for purposes of scientific research.

Annex 1 point 5 "Official Provision regulating the processing of special categories of data, pursuant to Article 21.1 of Legislative Decree No. 101 of 10 August 2018" determines the requirements to be observed for specific data processing operations, and is reproduced in full (Published in the Official Gazette General Series No. 176 of 29 July 2019).

5. Requirements for personal data processing conducted for purposes of scientific research.

5.1 Scope

These requirements concern data processing activities conducted by:

a) universities, other research bodies or institutes and scientific societies, and researchers working within these universities, research bodies or institutes and members of these scientific societies;

b) health professionals and health bodies;

c) natural or legal persons, entities, associations and private bodies, as well as persons specifically appointed to carry out data-processing responsibilities (researchers, committees of experts, contract research organisations, analysis laboratories etc.) (Article 2-quaterdecies of the Code; Article 28 of EU Regulation 2016/679).

5.2 Types of research

The following requirements concern the processing of personal data for purposes of medical, biomedical and epidemiological research, carried out when:

- the data processing is necessary in order to conduct studies carried out using data previously collected for health care purposes or for the implementation of previous research projects, or obtained from biological samples previously collected for health care purposes or for the implementation of previous research projects;

or

- the data processing is necessary in order to conduct studies using data related to persons who, due to the seriousness of their medical condition, are unable to understand the information provided in the Privacy Notice and to give valid consent.

In such cases, the research should be carried out based on a plan that has received a favourable reasoned opinion from the competent local Ethics Committee.

5.3 Consent

The data subject's consent is not required if the research is carried out on the basis of applicable legislative and regulatory provisions or of EU law.

In other cases, where it is not possible to obtain data subjects' consent, Data Controllers must document, in the research project, the special or exceptional grounds which make it impossible to inform the data subjects, or which make this unfeasible (without disproportionate efforts) or where doing so could render impossible or seriously undermine the purposes of the research including, in particular:

1. for ethical reasons arising from the fact that the data subject is unaware of his or her condition. This category includes research in relation to which, if a Privacy Notice were be provided to the data subjects, this would involve a disclosure of information about the conduct of the research, knowledge of which could cause material or psychological harm to the data subjects (this could include, for example, epidemiological studies on the distribution of a factor that predicts or could predict the development of a disease for which no treatment exists);

2. for reasons of organisational impossibility attributable to the fact that the research results would be significantly altered if account were not taken of data referable to the estimated number of data subjects who cannot be contacted in order to provide them with a Privacy Notice, compared with the total number of those it is intended to involve in the research; having regard, in particular, to the inclusion criteria of the research, the enrolment procedures, the statistical size of the sample, and having regard to the length of time that has elapsed since the data subjects' data were originally collected (e.g. in cases where the study involves data subjects with diseases associated with a high mortality rate or those with terminal illnesses or of advanced age and with serious health conditions).

In relation to these reasons of organisational impossibility, the following requirements also apply to the processing of data of persons who - after all reasonable efforts are made to contact them (also by verifying whether they are still alive, consulting the data in their clinical file, calling any telephone numbers provided, and by obtaining contact details from the register of patients or of the resident population) - turn out to be (at the time they are enlisted in the research):

- deceased or
- not contactable.

The obligation remains to provide the Privacy Notice to data subjects included in the research programme whenever this is possible during the research and, in particular, if they visit the treatment centre, including for medical checkups, also to enable them to exercise their rights under the Regulation if they should so wish;

3. for health reasons attributable to a serious clinical condition of the data subject which makes it impossible for him/her to understand the information provided in the Privacy Notice, and to give valid consent. In such cases, the study must be aimed at improving the data subject's clinical condition. Furthermore, it must be proven that the purposes of the study cannot be achieved through the processing of data of persons who are capable of understanding the information provided in the Privacy Notice and of giving valid consent, or by other research methods; having regard, in particular, to the inclusion criteria of the research, the enrolment procedures, the statistical size of the sample, and having regard to the reliability of the results achievable in relation to the specific purposes of the research. In relation to these reasons, the consent of the persons indicated in Article 82.2 a), of the Code (as amended by Legislative Decree no. 101/2018) must be obtained. All of this is subject to the requirement that the data subject be provided with a Privacy Notice as soon as his/her health condition so permits, also to enable him/her to exercise his/her rights under the Regulation if desired;

5.4 Data processing procedures

In cases where the purposes of the research cannot be achieved without the identification (even temporarily) of the data subjects, in the data processing that follows the retrospective collection of data, encryption or pseudonymisation techniques are applied or other solutions will be adopted which, having regard to the volume of data processed and the nature, subject-matter, context and purposes of the processing, ensure that they are not directly traceable to the data subjects, enabling the latter to be identified only when necessary. In such cases, the codes used are not inferable from the data subjects' personal identification data, unless this proves impossible on account of the special features of the processing or involves a manifestly disproportionate use of resources and is, furthermore, justified in the research project, in writing.

The combination of the data subject's identification data with the research material, provided it is temporary and essential for the research results, must also be justified in writing.

Applying the data minimisation principle, the processing of personal data for scientific research purposes in the medical, biomedical or epidemiological field can include data subjects' health data and also (in combination) - but only if indispensable to the purposes of the research - data on sexual life or sexual orientation, and on racial and ethnic origin (Article 5(1)(c), EU Regulation 2016/679).

5.5 Communication and dissemination

Those who act as Data Controllers for the purposes in question, including jointly with other data controllers, may disclose to one another personal data covered by this authorisation insofar as they are acting in the capacity of sponsor/organiser, coordination centre or participating centre and the disclosure is indispensable for the research.

In addition to the prohibition on disseminating health data of data subjects (Article 2-septies of the Code), nor is it permissible to disseminate or disclose data on sexual life, sexual orientation and racial and ethnic origin used for conducting the research.

5.6 Storage of data and of samples

Biological data and samples used to carry out the research are stored using encryption technology or identification codes or other solutions which, in view of the quantity of data and samples stored, ensure that they cannot be directly traced to the data subjects, for a period of time no longer than required for the purposes for which they were collected or subsequently processed.

To this end, the research project indicates the data retention period, post-research, after which these data and samples are anonymised.

5.7 Data storage and security

Subject to the obligation to adopt technical and organisational measures to ensure a level of data security that is adequate to the extant risks, the Data Controller(s) (based on their respective competences in the data processing, and attendant responsibilities) deploy(s) specific measures and technical safeguards to increase the security level of data processed for the purposes of the research.

This applies during the data storage or archiving phases (and, as relevant, the phase of collection and preservation of biological samples), in the later phase of processing of that information, and also in the subsequent phase of transmission of the data to the organiser/sponsor or to external parties who collaborate with the former to realise the research project. The following measures are adopted, in particular:

a. suitable safeguards to guarantee the quality of the data and their correct attribution to the data subjects;

b. suitable measures to ensure that research data is protected from risks of unauthorised data access, theft, or partial or complete loss of storage media or of portable or fixed processing systems (e.g. by the partial or complete application of encryption technology to file systems or databases, or through the adoption of other measures that render the data unintelligible to unauthorised persons) when recording and storing data;

c. secure transmission channels, taking into account the state of the art technology, in cases where the research data needs to be transmitted to a centralised database where the data are stored and archived or to an organiser/sponsor or to external parties sourced by the latter to conduct the research. Where such data transmission is effected by optical media (CD-ROM), a special recipient official is designated at the offices of the organiser/sponsor and a different transmission channel is used for sharing the data encryption key from the one used for the transmission of the content;

d. labelling techniques when storing and transmitting biological samples, using identification codes or other solutions which, in view of the number of samples used, ensure that they are not directly traceable to the data subjects, ensuring that they can be identified only when necessary;

e. with specific reference to the processing of research data stored in a centralised database, it is necessary to adopt:

- suitable authentication and authorisation systems for personnel specially assigned to data-processing activities based on their function and role and on their data access and data processing requirements, taking care to use credentials that are valid only for the duration of the research and to deactivate them at the end of the research;
- procedures to periodically ascertain the quality and consistency of authentication credentials and of authorisation profiles assigned to those designated to the data processing;
- audit log systems to control access to the database and detect any anomalies.

Special provisions for medical, biomedical and epidemiological research

Special care should be taken where the researcher/research team is involved in research involving medical, biomedical and epidemiological activities.

In this case, ethical rules apply to data-processing activities for statistical or scientific research purposes, published pursuant to Article 20.4 of Legislative Decree No. 101 of 10 August 2018 - 19 December 2018 (Published in the Official Gazette No. 11 of 14 January 2019).

Medical, biomedical and epidemiological research must be carried out in conformity with applicable international and EU standards, guidelines and provisions, such as the Convention on Human Rights and Biomedicine of 4 April 1997, ratified by Law No. 145 of 28 March 2001, the Recommendation of the Council of Europe R(97)5, adopted on 13 February 1997 on the protection of health data, and the Helsinki Declaration of the World Medical Association on ethical principles for medical research involving human subjects. In medical, biomedical and epidemiological research, the provision of information on the processing of personal data enables data subjects to make a distinction between research activities and health protection activities.

The Project Manager must:

- provide a Privacy Notice to the data subjects, ensuring that it is clear whether the activity involves research or health protection;
- obtain consent.

Consent to the processing of data that can disclose health data is, in general, required. The consent must be:

- **free and explicit, based on the elements provided for in the Privacy Notice;**
- **obtained in writing.**

If it is particularly difficult to acquire special categories of personal data in written form (in the case of telephone or computer-assisted interviews or similar), the data subject's consent may be documented in writing provided it is explicitly given. Documentary evidence of the Privacy Notice provided to the data subject and of the obtaining of consent is kept by the project manager for three years after the conclusion of the project, and is made available at the request of the Data Controller and/or the Data Protection Officer.

When consenting to a medical or epidemiological survey, the data subjects must state whether or not they wish to be informed about any unexpected findings that may emerge during the research that could be relevant to them. If so, then personal data revealing one's health condition may be disclosed to the data subject or, in the event of the physical impossibility, incapacity to act, incapacity to understand or unwillingness of the data subject, such data may be disclosed to the person who legally represents that person, namely:

- to a close relative, family member, cohabiting partner or civil partner;

- to a trustee within the meaning of Article 4 of Law No 219 of 22 December 2017 or, in their absence, to the head of the facility where the data subject is residing.

Only health care professionals and health bodies may disclose to the data subject personal data concerning his/her health condition, through a doctor designated by the data subject or by the Data Controller, except in the case of personal data previously provided by the data subject.
The consent of the data subject to the processing of health-related data for the purposes of medical, biomedical or epidemiological scientific research may be dispensed with if:

1. the research is carried out based on the provisions of applicable laws and regulations or of EU law , in conformity with Article 9.2(j) of the Regulation, including where the research is part of a biomedical or health research programme provided for pursuant to Article 12-bis of Legislative Decree No 502 of 30 December 1992, and an impact assessment is carried out and made public pursuant to Articles 35 and 36 of the Regulation;
2. it proves impossible, for specific reasons, to inform the data subjects or if this would involve disproportionate efforts or could render impossible or seriously undermine the achievement of the research objectives. In such cases, the Data Controller is obliged to take appropriate steps to protect the rights, freedoms and legitimate interests of the data subjects, and the research programme must receive a favourable reasoned opinion from the competent local Ethics Committee, and be submitted to the Italian Data Protection Authority for advance consultation pursuant to Article 36 of the Regulation.
3. The Italian Data Protection Authority may authorise the further processing of personal data, including data subject to special data processing operations indicated in Article 9 of the Regulation, for scientific research or statistical purposes, by third parties who are predominantly engaged in those activities, if it proves impossible, for specific reasons, to inform the data subjects or if this would involve disproportionate efforts or could render impossible or seriously undermine the achievement of the research objectives, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subjects, in accordance with Article 89 of the Regulation, including prior forms of data minimisation and economisation (Article 110-bis of the Personal Data Protection Code).

22. Data security measures to be taken - research area

Pursuant to Article 32.1 of EU Regulation 2016/676, for each data processing operation, the Data Controller shall implement suitable technical and organisational measures that guarantee data security levels proportionate to the risk involved.

The researcher must therefore, for each individual piece of research, identify suitable measures to guarantee data protection by reference to the state of the art, the costs of implementation, and the nature, purpose, context and purpose of the processing.
EU Regulation 2016/676 indicates a number of measures, by way of illustration:

- pseudonymisation,
- encryption of personal data,
- the ability to ensure confidentiality on a permanent basis,
- the integrity, availability and resilience of data processing systems and services, etc.

Similarly, AGID Circular No. 2/2017 of 18/04/2017 on "Minimum Data Security Measures" suggests a number of mandatory provisions that can be usefully adopted in the processing of personal data, depending on the level of risk identified for each individual data processing, such as encryption for portable devices, installation of local firewalls and antiviruses, etc.
A number of general guidelines are given below, which will assist in ensuring that personal data utilised for research activities are processed in accordance with the provisions of EU Regulation 2016/676.

Electronic processing of personal data

Data security levels

Identify the appropriate level of security to be applied to the data processing (pseudonymisation, encryption techniques, etc.), based upon an analysis of the category of personal data processed, i.e. whether the data are generic personal data or special personal data (health, genetic, biometric, judicial, etc.).

Saving of data

- Assess, with the technical support of the relevant Department/Centre, the type of support/device on which the personal data processed is to be saved, and that adequate data backup policies are in place where they are stored on the Department's storage systems or on the research team's systems.
- Ensure that the persons involved do not save the personal data on external storage devices (hard drives, pen drives, DVDs) unless they are protected by suitable encryption systems (to protect the data even if the storage devices are lost or stolen).

- Check, with the technical support of the relevant Department/Centre, that the data have been fully erased in the event of disposal/repair/reuse of the hardware containing the data.

Authentication and Authorisation

- Identify the persons who are authorised to process personal data, and define the correct access authorisations to devices and to areas where the data are processed and/or stored. If the reasons for accessing the data no longer exist (e.g. a researcher leaves the research team, the research project ends), ensure that the relevant authorisations are removed.
- Check which users have administrator rights and ascertain that they have the appropriate skills.

Adopt two-factor authentication mechanisms (pin numbers, passwords, etc.) granting access to the data and/or the systems that process the data, where possible activating physical media encryption mechanisms for all systems (especially mobile systems such as laptops and mobile phones).

Organisational provisions

Properly train and authorise research team members who process personal data on the correct procedures to follow and on the data security measures to be taken.

Workstations

Pay attention to the workstation from which the data processing operations take place. Private workstations (desktop PCs, tablets, laptops, mobile phones), for example, may not have all the requisite safeguards in place (antivirus, firewall) and, if connected to the Internet, may be more open to the risks of viruses, malware and ransomware.

Data exchange procedures

- If data is also communicated to non-EU countries (e.g. to research partners), evaluate the correct technical procedures.
- Avoid redirecting University email to private mailboxes.

Use of data processing systems

If data processing systems not owned by Politecnico di Milano are used (including for free), examine these systems in advance and, in particular, request a declaration from the supplier which certifies compliance with EU Regulation 2016/676 and the adoption of security measures appropriate to the anticipated data processing.

It is also recommended that

- Updated anti-virus software programmes should be installed on all systems used.
- The operating system and the applications installed on workstations used to access the data should be regularly updated.

Access credentials to University services:

- should not be transferred to third parties;
- should not contain significant parts of the account name or user name;
- should be regularly changed to new ones (rather than reusing ones already used);
- a note of one's user ID and password should not be left in plain sight;
- access permissions should be used exclusively for the purposes intended;
- when leaving the workstation, log out of any applications and/or the system, or lock the workstation or activate the screen-saver with a password.
- immediately report incidents, unauthorised accesses and security breaches (actual or suspected), erasure/alteration of data, loss/theft of devices containing personal data in compliance with data breach procedures. Note, here, that Politecnico di Milano is obliged to notify the Italian Data Protection Authority of the breach within at most 72 hours, consequently any incident should be reported immediately or without undue delay.

23. COOKIES

Cookies are used for different purposes (including digital authentication, session monitoring, storing information in specific configurations for users who access the server, storing preferences etc.), all of which require personal data that can identify the individuals concerned.

Especially when creating a new website, all relevant measures and expedients should be applied in order to implement the principles of Privacy by Design and Privacy by Default, thus ensuring that personal data processing operations are fully compliant[22].

Initial notes on creating a website

A) Distinguish between technical cookies and profiling cookies: the user's consent is not required when installing technical cookies, provided that a Privacy Notice has been provided, drawn up in compliance with Article 13 of the EU Regulation. Profiling cookies, on the other hand, may be installed on the user's terminal ONLY if the user has consented to this, after having received the relevant Privacy Notice.

[22] For more information and clarification on the subject of "Cookies" please consult: https://polimi365.sharepoint.com/sites/Privacy-GDPR/Documenti/Forms/AllItems.aspx?id=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2FCookies%2FUltimate%20Guidance%20on%20the%20use%20of%20cookies%2Epdf&parent=%2Fsites%2FPrivacy%2DGDPR%2FDocumenti%2FCookies .

B) Create a suitable **banner** that appears to the user when he/she accesses the website, containing information about cookies used. As indicated by the Italian Data Protection Authority, the banner should specify whether the site uses profiling cookies, possibly including 'third-party' cookies, which permit advertising messages to be sent in line with the user's preferences. The banner should also contain a link to the full Privacy Notice and state that by clicking on the link it is possible to withhold one's consent to the installation of any cookies and, finally, it should specify that if the user chooses to continue by "skipping" or "accepting" the banner, he/she thereby consents to the use of cookies.

When creating a new website it is advisable, in any case, to consult with the Data Protection Officer from the earliest stages of the setup process.

24. PAPER DOCUMENTATION

Data processing operations may still frequently take place in paper form. A number of rules should be observed when managing paper documentation.
Designated internal Data Processors should observe the following procedures:

- identify any persons with authority to access personal data kept on paper media outside normal working hours;
- verify, after consultation with the DPO, the proper implementation of procedures for the destruction of documents when no longer required or when the data subject so requests;
- do not leave documents containing Personal Data and/or "special categories of personal data", (" Sensitive Data" and/or Judicial Data) unattended, during and after working hours;
- do not leave documents containing Personal Data and/or "special categories of personal data", (" Sensitive Data" and/or Judicial Data) in places accessible to the public;
- store documents in data archives when no longer required for operational reasons;
- limit the making of copies of such documents and/or the external transmission of such documents to what is absolutely necessary.

The reproduction of documents containing special categories of personal data and/or judicial data on non-electronic media (e.g. photocopies) is prohibited unless absolutely essential in order to implement the contract and fulfil legal compliance obligations. Reproduced documents are subject to the same rules as the original documents.

Furthermore:

- paper documents should be stored in suitably protected data archives in order to prevent the unauthorised reading and/or removal thereof, thus guaranteeing the confidentiality and integrity of personal data;
- paper documents should be stored in suitable locked archives or in special cabinets or rooms at the end of the working day. Keys should be kept in a safe place and not left in locks;
- keys should be kept in a safe place and not left in locks;

Consultation of hard copy documents.

Authorised persons alone have authority to consult documents containing personal data, exclusively where this is operationally required and, where possible, in situ.

Authorised persons may consult such documents outside working hours only if they have received advance authorisation to do from the Data Processor, identified and registered by the supervisory authority.

Destruction of hard copy documents

In relation to the provisions of Articles 5(e) and 89 of Regulation (EU) 2016/679, which provide for personal data to be retained for a definite period of time, documents there are not legally required to be retained must be destroyed at the end of their use.

Documents must be destroyed, subject to permitted legal limits, whenever the data subject so requests and/or when so communicated by the Data Controller or by the Data Processor, in accordance with their respective remits, and the destruction of documents should be formalised and authorised by the Data Controller or by the Data Processor, according to their respective competences, based on the ownership of the data contained in the document under examination.

Documents should be destroyed under the supervision of the relevant unit Manager.

The lawful destruction of paper documents containing personal data should be performed using suitable means (document shredder) which ensure that the document cannot be reconstructed.

25. MONITORING

These operating instructions are adopted pending the full implementation of the regulatory framework on data protection and the activation of the data protection application, and will therefore be subject to adaptation based on the outcome of that activity.

Even when fully operational, Politecnico di Milano's operating instructions should be monitored by the Administration on an ongoing basis in order to facilitate rapid intervention (also on a proposal from the DPO) in the organisational

structure following regulatory changes or technological developments, or where the need arises to introduce new and more effective personal data management practices.

THE DIRECTOR GENERAL
Mr. Graziano Dragoni

Digitally signed pursuant to the Digital Administration Code.