

# REGULATION ON THE PROTECTION OF PERSONAL DATA

YHANK INSTITUTE

Omniversity Edutech Ltd

DRAGONARA BUSINESS CENTRE 5TH FLOOR, TRIQ ID-DRAGUNARA, SAN GILJAN,  
STJ 3141, MALTA

## Summary

<b>Art. 1 - AREA OF APPLICATION</b> .....	3
<b>Art. 2 DEFINITIONS</b> .....	3
<b>Art. 3 - TYPES OF DATA PROCESSED BY THE YHANK INSTITUTE</b> .....	5
<b>ART. 4 - GENERAL PRINCIPLES OF TREATMENT</b> .....	7
<b>Art. 5 - AWARENESS RAISING AND TRAINING</b> .....	8
<b>Art. 6 - LEGAL BASIS OF THE TREATMENT</b> .....	8
<b>Art. 7 - CIRCULATION OF DATA WITHIN THE INSTITUTE</b> .....	8
<b>ART. 8 - INTERNAL ORGANIZATIONAL MODEL - RIGHTS OF THE INTERESTED PARTY - DATA SECURITY - INTERNAL ORGANIZATIONAL MODEL AND REFERENCE PERSONNEL</b> .....	9
<b>Art. 9 - OWNER OF THE TREATMENT</b> .....	9
<b>Art. 10 - DESIGNATED AND REFERENT FOR THE PROCESSING OF PERSONAL DATA</b> .....	10
<b>Art. 11 - RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA (DPO)</b> .....	10
<b>Art. 12 - PEOPLE AUTHORIZED TO PROCESS</b> .....	11
<b>Art. 13 - SYSTEM ADMINISTRATORS</b> .....	11
<b>Art. 14 - RESPONSIBLE FOR TREATMENT</b> .....	12
<b>Art. 15 - PRIVACY BY DESIGN IN THE DESIGN OF YHANK INSTITUTE PROCESSING FACILITIES</b> ....	13
<b>Art. 16 - RIGHTS OF THE INTERESTED PARTY</b> .....	13
<b>Art. 17 - REGISTER OF PROCESSING ACTIVITIES</b> .....	14
<b>Art. 18 - EVALUATION OF THE IMPACT ON DATA PROTECTION</b> .....	15
<b>ART. 19 - ADVANCE CONSULTATION</b> .....	16
<b>Art. 20 - INFORMATION FOR THE INTERESTED PARTY</b> .....	16
<b>ART. 21 - PRIVACY AND IT SECURITY</b> .....	17
<b>Art. 22 - BREACH OF PERSONAL DATA (DATA BREACH)</b> .....	18
<b>Art. 23 - TREATMENT OF PARTICULAR CATEGORIES OF PERSONAL DATA</b> .....	19
<b>Art. 24 - PROCESSING OF PERSONAL DATA IN THE HEALTHCARE FIELD</b> .....	21
<b>Art. 25 - PROCESSING OF DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENSES</b> .....	21
<b>Art. 26 - PROCESSING OF PERSONAL DATA FOR THE MANAGEMENT OF THE EMPLOYMENT RELATIONSHIP</b> .....	22
<b>Art. 27 - PROCESSING OF PERSONAL DATA IN THE MEETINGS OF THE COLLEGIATE BODIES</b> .....	22
<b>ART. 28 - TREATMENT FOR ARCHIVE, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES AND STATISTICAL PURPOSES</b> .....	22
<b>ART. 29 - TREATMENT FOR PUBLIC INTEREST OR HISTORICAL RESEARCH PURPOSES</b> .....	23
<b>ART. 30 TREATMENT FOR STATISTICAL OR SCIENTIFIC RESEARCH PURPOSES</b> .....	23
<b>Art. 32 - COMMUNICATION AND DISSEMINATION OF PERSONAL DATA</b> .....	24
<b>ART. 33 - COMMUNICATION AND DISSEMINATION OF DATA RELATING TO RESEARCH ACTIVITIES</b> .....	25
<b>Art. 34 VIDEO SURVEILLANCE</b> .....	25
<b>Art. 35 - RIGHT OF ACCESS AND CONFIDENTIALITY</b> .....	26
<b>Art. 36 - SCOPE OF LIABILITY</b> .....	27
<b>Art. 37 - REFERENT STRUCTURE FOR THE EXECUTION OF THE REGULATION</b> .....	27



# REGULATION ON THE PROTECTION OF PERSONAL DATA

## Art. 1 - AREA OF APPLICATION

1. This Regulation, adopted in implementation of EU Regulation 27 April 2016 n. 679 (hereinafter «EU Regulation») and of the DATA PROTECTION [ CHAP. 440.1 CHAPTER 440 DATA PROTECTION ACT, regulates the protection of physical people concerning the processing of personal data within Yhank Institute managed by Omniversity Edutech ltd based in Malta.
2. YHANK INSTITUTE handles the processing of personal data for the performance of its institutional purposes, within the limits established by its Statute and by its license issued by MFHEA under no. 005-2023, by the laws and regulations and in any case in compliance with the rights and fundamental freedoms and the dignity of the interested party, with particular reference to confidentiality, personal identity and the right to the protection of personal data.

## Art. 2 DEFINITIONS

1. For this Regulation, the following definitions apply:

1. personal data: any information relating to an identified or identifiable physical person. an identifiable physical person can be identified, directly or indirectly, for example using a name, identification number, location data, an online identifier or one or more characteristic elements of his physical, physiological, genetic identity, psychic, economic, cultural or social.

2. "special categories of data": personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership. genetic data. biometric data. data relating to health, sex life and sexual orientation.

3. "genetic data": personal data relating to the hereditary or acquired genetic characteristics of a physical person which provide unambiguous information on the physiology or health of that physical person, and which results from the analysis of a biological sample of the physical person in question.

4. biometric data: personal data obtained from a specific treatment, relating to the physical, physiological or behavioral characteristics of a physical person, which allow or confirm its unique identification, such as the facial image or dactyloscopy data.

5. "data relating to health": personal data relating to the physical or mental health of a person, including the provision of health care services, which reveal information relating to his state of health.

6. data subject: the physical person to whom the personal data refers.

7. "processing": any operation or set of operations, performed with or without the aid of automated processes and applied to personal data or sets of personal data, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation, cancellation or destruction.

8. "profiling": any form of automated processing of personal data consisting of the use of data to evaluate certain personal aspects relating to a physical person to analyze or predict aspects relating to professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that physical person.
9. automated decision-making process: a decision based solely on automated processing, including profiling, which produces effects in the legal sphere of the interested party, or which significantly similarly affects him.
10. "pseudonymization" means the processing of personal data in such a way that they can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organizational measures aimed at ensuring that personal data are not attributed to an identified or identifiable person.
11. "anonymous information": according to recital 26 of the GDPR, information that does not refer to an identified or identifiable physical person or personal data made anonymous enough to prevent or no longer allow the identification of the data subject.
12. archive: any structured set of personal data accessible according to specific criteria, regardless of whether this set is centralized, decentralized or distributed functionally or geographically.
13. "Data controller": the physical or legal person, public authority, service or other body which, individually or together with others, determines the purposes and means of processing personal data.
14. "Personal data protection officer" or "DPO" (Data Protection Officer): figure specialized in supporting the Data Controller, who performs liaison functions with the Guarantor and protection of data subjects.
15. "Data Processor": the physical or legal person, public authority, service or other body which processes personal data on behalf of the Data Controller.
16. Designated: senior figure of the YHANK INSTITUTE structure who has the task of supervising, monitoring and guaranteeing compliance with current regulations on the protection of personal data, identified according to the Attachment to these Regulations.
17. Referent»: subject specifically identified among the Authorized data processors operating in the structure of the Designated and assigned by the latter to manage privacy issues.
18. "Authorized to process": physical people formally authorized and instructed to process personal data under the direct authority of the Data Controller.
19. "recipient": the physical or legal person, public authority, service or other body that receives communication of personal data.
20. "third party": the physical or legal person, public authority, service or other body other than the interested party, the Data Controller, the Data Processor and the people authorized to process.
21. Consent of the interested party: any expression of the free, specific, informed and unequivocal will of the interested party, with which the same accepts, by unequivocal declaration or affirmative action, the processing of personal data concerning him.

22. "communication": giving knowledge of personal data to one or more specific subjects, in any form, including by making them available, consulting or interconnecting with them.
23. Dissemination: giving knowledge of personal data to unspecified subjects, in any form, including by making them available or consulting them.
24. "register of processing activities": the list of data processing in paper or electronic form carried out by the Data Controller and the Data Processor according to the respective areas of the processing.
25. «data protection impact assessment»: procedure aimed at describing the processing, assessing its necessity and proportionality and ensuring the management of the risks for the rights and freedoms of the data subjects.
26. breach of personal data: the breach which involves accidental or unlawful destruction, loss, modification, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.
27. Supervisory authority: the independent public authority, established by a Member State according to article 51 of the EU Regulation, in charge of supervising the application of the Regulation itself, to protect the fundamental rights and freedoms of physical people concerning processing and to facilitate the free flow of personal data within the Union. For Malta, the Supervisory Authority is identified in The Office of the Information and Data Protection Commissioner - IDCP.
28. "system administrators": the professional figure dedicated to the management and maintenance of the processing systems with which personal data processing is carried out, including database management systems, local networks and security equipment, in the extent to which they allow action on personal data.
29. research institute or body: a public or private body for which the purpose of statistics or scientific research results from the purposes of the institution and whose scientific activity can be documented.
30. scientific society, an association that brings together scholars of a disciplinary field, including the relative professional associations.
31. "scientific research" means a research project set up following the relevant sectoral ethical and methodological standards, following good practice.

### **Art. 3 - TYPES OF DATA PROCESSED BY THE YHANK INSTITUTE**

1. YHANK INSTITUTE is a private research and training institution, which pursues the aims of critical elaboration and dissemination of knowledge, the interaction between cultures, skills development, personal education and training, cultural enrichment of the company authorized by MFHEA Malta with license n. \_\_\_\_\_ as Higher Education Institute.
2. For the pursuit of its institutional purposes, YHANK INSTITUTE mainly processes the types of personal data indicated below.
- a) Data, also of a particular nature, relating to subordinate, para-subordinate or self-employment personnel, including subjects whose employment relationship has ceased, or other people operating in various capacities in the Institute such as, for

example, scholarship holders, trainees, visitors etc. This data are processed in the context of the following activities:

- tests for selections.
- management of the employment relationship.
- professional training and updating.
- research project management.
- research monitoring and evaluation.
- technology transfer activities.
- Welfare policies and the use of concessions.
- health and safety of people in the workplace.
- smart working and teleworking.
- provision of landline and mobile telephony services.

b) Data, also of a particular nature, relates to students, including those who have already completed their studies and similar categories. This data is processed in the context of the following activities:

- orientation activities.
- provision of entry tests and verification of access requirements.
- provision of training and career management, upon enrollment for graduation.
- provision of teaching activities and exams remotely.
- traineeship and internship activities.
- job placement activities.
- to promote further educational initiatives, publications, events and initiatives designed to spread knowledge and experience.
- activities related to the conduct of student elections and the representation of students in the governing bodies of the YHANK INSTITUTE.
- alumni association-related activities.
- fundraising, communication and institutional information and community development activities.
- statistical surveys and evaluation of teaching.
- dissemination of the final report or related elements.
- reply to requests forwarded by the Judicial Authorities, by the Forces of Order or by Public Administrations.
- tutoring services, assistance, and social inclusion.
- assistance services for the disabled and DSA.
- services and activities for the right to study.
- disciplinary proceedings against students.

3. Data relating to teaching and research.

4. Data relating to the internal management activities of the institution and to the activities carried out on behalf of third parties and data connected to transversal activities carried out also electronically. This data are processed in the context of the following activities:

- space management.
- workstation management.
- corporate bodies and positions.
- injury management.
- library services.
- document protocol and storage services.

- purchase of goods and services, the stipulation of contracts, debt collection, dispute management.
- email services and collaboration tools.
- distance learning services.
- proctoring and online exam delivery services.
- tracking of non-primary information and management of cyber security.
- holding competitions and meetings.

In any case, all data processing carried out by the Institute, even if not included in the above list, which falls within the performance of YHANK INSTITUTE's institutional tasks or which are prescribed to it by law, are governed by these Regulations.

#### **ART. 4 - GENERAL PRINCIPLES OF TREATMENT**

1. The processing of personal data is carried out by YHANK INSTITUTE in the application of the principles established by art. 5 of the EU Regulation.
2. personal data being processed are:
  - a) processed in a lawful, correct and transparent manner in relation to the data subject.
  - b) collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes. Further processing of personal data for archiving purposes in the public interest, for scientific or historical research or statistical purposes is not considered incompatible with the initial purposes.
  - c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
  - d) accurate and, if necessary, updated: to this end, all reasonable measures are taken to promptly cancel or correct inaccurate data concerning the purposes for which they are processed.
  - e) stored in a form that allows identification of the interested party for a period of time not exceeding the achievement of the purposes for which they are processed. may be stored for longer periods provided that they are processed exclusively for archiving purposes in the public interest, scientific or historical research or statistical purposes, provided that appropriate technical and organizational measures are implemented to protect the rights and freedoms of the interested.
  - f) processed in such a way as to ensure adequate security of personal data, including protection, through appropriate technical and organizational measures, against unauthorized or unlawful processing and loss, destruction or accidental damage.
3. Taking into account the state of the art, the implementation costs, the nature, object, context and purpose of the processing, YHANK INSTITUTE adopts adequate technical and organizational measures capable of demonstrating compliance with the principles set out above.
4. The systems provided and the services provided by all the central IT structures are configured in such a way as to minimize the use of personal and identification data, to avoid processing when the purposes pursued in individual cases can be achieved using anonymous data or methods of identification of the interested party only in case of need.

## **Art. 5 - AWARENESS RAISING AND TRAINING**

1. For the correct and punctual application of the regulations on the protection of personal data and IT security, YHANK INSTITUTE supports and promotes, with the involvement of the Institute's competent bodies, tools for raising awareness (also through classroom training activities, webinars or guidelines) aimed at consolidating awareness of the value of personal data protection, as well as training activities aimed at YHANK INSTITUTE staff and information activities aimed at those who maintain relations with the Institute.

## **Art. 6 - LEGAL BASIS OF THE TREATMENT**

1. The legal basis of the processing consists, alternatively:
  - in the execution of tasks in the public interest and connection to the exercise of the powers attributed to the Institute by law or regulation.
  - in the fulfilment of contractual obligations of which the interested party is a part or in the execution of pre-contractual measures adopted at the request of the same.
  - in the fulfilment of legal obligations to which the Institute is subject.
  - outside of its duties, in the pursuit of the legitimate interest of the Institute or of third parties, provided that the interests or fundamental rights and freedoms of the data subject who require the protection of personal data do not prevail if the data subject is a minor.
  - in safeguarding the vital interests of the data subject or another physical person.
  - in the consent of the interested party, where foreseen.
2. If the treatment is based on consent, YHANK INSTITUTE informs the interested party in advance and acquires the consent with methods capable of demonstrating that the interested party has given his consent, free, aware, and unequivocal, to the processing of his data. The interested party has the right to withdraw his consent at any time. The withdrawal of consent does not affect the lawfulness of the processing based on the consent before the withdrawal.

## **Art. 7 - CIRCULATION OF DATA WITHIN THE INSTITUTE**

1. Access to personal data by the Institute's administrative, service, teaching and scientific structures and employees, in any case, limited to cases in which it is aimed at pursuing institutional purposes, is inspired by the principle of the free circulation of information within the YHANK INSTITUTE, according to which the institute arranges for the organization of the information and data at its disposal through tools, including IT ones, designed to facilitate access and use.
2. Each request for access to personal data by the Institute's structures and employees, duly motivated and connected with the performance of the activity inherent to their specific function, is satisfied directly and without further formalities to the extent necessary for the pursuit of the interest of the Institute, without prejudice to the responsibility of the applicant deriving from any improper use of the data.

3. Where the request is aimed at a further and/or different use of personal data, the applicant is required to indicate this explicitly and formally in the request, to be assessed by the Designated and the authorization will be granted or denied depending on whether the purpose of the request falls within the institution's activity or not.
4. To access the data, bodies such as the Didactic Board, the auditor, the Evaluation Unit, the Ethics Committee as well as all the other institutional bodies are treated as equivalent to the Institute's structures, limited to the data necessary for the performance of their functions.

## **ART. 8 - INTERNAL ORGANIZATIONAL MODEL - RIGHTS OF THE INTERESTED PARTY - DATA SECURITY - INTERNAL ORGANIZATIONAL MODEL AND REFERENCE PERSONNEL**

1. Considering the internal organizational model, the reference figures for the protection of personal data are the following:
  - a) The Owner
  - b) The Designates,
  - c) Privacy Representatives.
  - d) The Personal Data Protection Officer.
  - e) People are authorized to process personal data.
  - f) System administrators.

## **Art. 9 - OWNER OF THE TREATMENT**

1. YHANK INSTITUTE, in the person of the Director \_\_\_\_\_ as the legal representative, is the Data Controller of the personal data processed by it.
2. All the people in charge of the treatment and the Authorized of the Institute are required to comply with the prescriptions of YHANK INSTITUTE. Failure to comply with the provisions could lead to both the Data Processors and the Authorized Authorities acting as independent Data Controllers, thus assuming the consequent obligations and responsibilities.
3. When the Institute determines the purposes and means of the processing jointly with another Data Controller, it assumes, together with the latter, the role of Joint Data Controller.
4. The Joint Controllers define transparently, through an internal agreement, their respective roles and responsibilities regarding the observance of the obligations deriving from the EU Regulation, about the exercise of the rights of the interested party, and the respective functions of communication of the Information referred to in the following art. 20. The essential content of the joint ownership agreement is made available to the interested party upon request.
5. The data subject can exercise his/her rights vis-à-vis each joint data controller.

## **Art. 10 - DESIGNATED AND REFERENT FOR THE PROCESSING OF PERSONAL DATA**

1. The Data Controller identifies the Appointees in the top managers of the structure referred to in Annex A, who has the task of supervising, monitoring and guaranteeing, within the structure to which they are responsible, compliance with the regulations in force and the instructions of the Data Controller on the matter of personal data protection.
2. The Designated can identify, within their structure, a contact person who will have the task of interfacing with YHANK INSTITUTE's data protection manager for any communication linked to the application of the legislation on the protection of personal data and support the designated in management of activities relating to the processing of personal data. The Designated is assigned the responsibilities of direction, supervision and control over the work of the Referent. The identification of the Referent subject does not release the Designated about his duties referred to in paragraph 1.
3. The Representatives are identified by the Designated among the technical-administrative staff of the structure, in possession of the necessary professional skills. For the Departments, based on the complexity and heterogeneity of the data processed, the Designated Person can identify the Contact Person also among the teaching or research staff. The names of the Contact People identified must be communicated electronically to the Data Controller and the Personal Data Protection Officer.
4. If the data are processed on IT systems centrally administered by the ICT Department, the Manager of the same Department, in addition to being the Designated Person, also acts as Contact Person.

## **Art. 11 - RESPONSIBLE FOR THE PROTECTION OF PERSONAL DATA (DPO)**

1. The Data Controller designates a Data Protection Officer (DPO), a figure identified based on professional qualities, in particular the specialist knowledge of data protection legislation and practices, and the ability to perform the tasks referred to in the following paragraph 3, which performs liaison functions with the Guarantor and protection of the interested parties.
2. The DPO can be an internal subject of the Institute or an external subject, in which case he performs his duties based on a service contract.
3. The DPO, considering the risks inherent in the processing, considering nature, the scope of application, the context and the purposes of the same, performs the following tasks:
  - informs and advises the Data Controller, the Data Processor and the Authorized subjects regarding the obligations deriving from the EU Regulation and other legislative provisions on the protection of personal data.

- supervises compliance with the regulations and Institutes policies on the protection of personal data - including the attribution of responsibilities, the awareness and training of personnel who participate in the processing and related control activities.
- provides, if requested, an opinion on the impact assessment on data protection and supervises its performance.
- cooperates with the Information and Data Protection Commissioner, acting as a point of contact for the same on matters related to the processing, including prior consultation, and consultations, where appropriate, concerning any other matter.
- collaborates in the drafting and updating of the treatment registers.
- maintains contact with the interested parties, in relation to the exercise of their rights.

The Data Controller may assign additional tasks and functions to the DPO, provided they do not give rise to conflicts of interest and do not hinder the fulfilment of the related responsibilities.

4. The DPO has wide access to information and is consulted for every issue concerning data protection and for every activity that involves data processing, right from its planning.
5. YHANK INSTITUTE guarantees that the DPO carries out its functions with autonomy and independence.
6. YHANK INSTITUTE informs the Information and Data Protection Commissioner of the name and contact details of the DPO, inserts them in the Information to data subjects and all documents containing the processing of personal data and publishes them on the institutional website.

## **Art. 12 - PEOPLE AUTHORIZED TO PROCESS**

1. Authorized subjects are all those who carry out the operations relating to the treatment under the direct authority of the Data Controller and, as such, are authorized to process personal data in full compliance with the instructions of the Data Controller.
2. The staff of the Institute is authorized to process data within the scope defined by the tasks assigned with an employment contract or deed of appointment, by the responsibilities of the assignment or affiliation structure and by the activities assigned by the Head of the structure.
3. All YHANK INSTITUTE employees are required to follow the instructions and provisions of the Institute regarding the protection of personal data and IT security and to act in compliance with current legislation even when they carry out remote work activities (work from home, agile work or telecommuting).

## **Art. 13 - SYSTEM ADMINISTRATORS**

1. System administrators are professionals who manage and maintain a processing plant or its components. For this regulation, database administrators, network administrators, security apparatus administrators, and administrators of complex software systems are also to be considered as such.
2. The System Administrator develops and manages the processing plant or its hardware and software components through which the processing of personal data is carried out by applying the directives of the Owner for the profiles relating to security.
3. The Controller identifies the system administrators with an individual designation deed which analytically defines the tasks and areas of operation permitted based on the assigned authorization profile.

#### **Art. 14 - RESPONSIBLE FOR TREATMENT**

1. The person in charge of the treatment is the subject external to the organization of the Institute which carries out treatments on behalf of YHANK INSTITUTE. For the processing of personal data, the Institute only uses Managers who present suitable guarantees, concerning the technical and organizational measures suitable to allow compliance with the provisions of the EU Regulation, including the protection of the rights of the interested parties.
2. The institute designates the Data Processor utilizing a contract or other legal act which determines the nature, duration and purpose of the treatment or treatments assigned, the type of data processed, the categories of interested parties, the obligations and rights of the Data Controller and the Manager, the responsibilities and the technical and organizational measures adequate to allow compliance with the instructions given by the Data Controller and with the regulatory provisions.
3. Specific obligations of the Manager are:
  - keeping the Register of treatments carried out on behalf of the Data Controller.
  - the adoption of suitable technical and organizational measures to guarantee the security of the treatments.
  - the designation of a Data Protection Manager, if required by law or if deemed necessary.
  - the designation of a representative in Malta (in the case of a manager not established in the EU).
  - compliance with the instructions provided by the Data Controller.
4. For specific processing activities, in compliance with the contractual obligations that bind him to the Institute, the Data Processor may appoint sub-processors only with the prior written, specific or general authorization of YHANK INSTITUTE and with the assignment to the sub-processor of the same obligations on the matter protection of personal data deriving from the contract - or other legal act - between YHANK INSTITUTE and the Manager. If a sub-manager fails to fulfil his obligations regarding data protection, the Manager retains full responsibility towards the Institute for the fulfilment of the

obligations of the sub-manager, and also for compensation for any damages caused by the treatment.

5. The Institute can be appointed Responsible for one or more treatments on behalf of another Owner.

#### **Art. 15 - PRIVACY BY DESIGN IN THE DESIGN OF YHANK INSTITUTE PROCESSING FACILITIES**

1. Anyone who designs or develops processing plants or their hardware and software components must ensure that the solution complies with the legislation on the processing of personal data right from the plant design and development phase, including the safety profiles.

#### **Art. 16 - RIGHTS OF THE INTERESTED PARTY**

1. The Institute guarantees the rights of the interested parties according to articles 15 to 22 of the EU Regulation. In particular, the interested party can:
  - a) obtain confirmation of the existence or not of personal data concerning him and their communication in an intelligible form.
  - b) obtain without unjustified delay the rectification of inaccurate data and the integration of incomplete data.
  - c) obtain the deletion of data without unjustified delay, in the cases and within the limits established by the EU Regulation.
  - d) obtain the limitation of the treatment in the cases and with the effects foreseen by the EU Regulation.
  - e) receive the data in a structured format, commonly used and readable by an automatic device, and transmit them to another Data Controller, if the treatment is based on consent and is carried out by automated means.
  - f) obtain the direct transmission of data from the Institute to another Data Controller, in the cases provided for in the previous letter and if technically feasible.
  - g) oppose the treatment.
  - h) complain with a Supervisory Authority.
  - i) appeal with the Judicial Authority.
2. The interested party, upon identification, can exercise the rights with a request to the Data Controller also through the Data Protection Officer of the Institute according to the following methods:
  - in person at the competent structures to receive the request as they process the data (e.g. Student Secretariats, Human Resources Department)
  - or by e-mail, writing to: [dpo@yhank.com](mailto:dpo@yhank.com)
  - or with a specific communication sent by post to YHANK INSTITUTE

\_\_\_\_\_.

3. The application can be presented by a delegate of the interested party, who exhibits or attaches a copy of the power of attorney or the signed proxy, together with an unauthenticated photocopy of his identification document and that of the interested party.
4. The rights referring to the personal data of deceased people can be exercised by those who have a personal interest or act to protect the data subject, as his agent, or for family reasons worthy of protection. This is without prejudice to the case in which the interested party has unequivocally expressed the specific, free and informed will to prohibit the exercise of the rights or some of them.
5. The request of the interested party is satisfied without unjustified delay and in any case within the maximum term of 1 month from receipt of the request, which can be extended for a further 2 months if necessary, considering the complexity and number of requests. The interested party is informed of the extension and the reasons for the delay within 1 month of receiving the request. Upon an explicit request from the interested party, the Institute informs any other Data Controller who processes the deleted personal data of the cancellation request.
6. The exercise of rights is free, except in cases of manifestly unfounded or excessive requests, also due to their repetitive nature, for which a reasonable fee may be charged based on the administrative costs incurred by the Institute. Alternatively, in these cases the Data Controller is entitled to refuse to satisfy the request, demonstrating its manifestly unfounded or excessive nature.

## **Art. 17 - REGISTER OF PROCESSING ACTIVITIES**

1. YHANK INSTITUTE, as Data Controller, establishes a Register of processing activities carried out under its responsibility.

The Registry contains the following information:

1. the structure responsible for the treatment.
2. where existing, the names and contact details of the Joint Controller(s) and the Data Processor(s).
3. the purposes of the processing.
4. a description of the categories of data subjects and the categories of personal data.
5. the categories of recipients to whom the personal data have been or will be disclosed.
6. the possible transfer of personal data to a third country or an international organization, with the indication of the third country or international organization and the documentation of adequate guarantees.
7. where possible, the deadlines foresaw the cancellation of the different categories of data.
8. where possible, a general description of the technical and organizational security measures adopted. To allow the Data Controller to keep the Register, in the event of the start or termination of treatment, the Head of the interested structure, also through any Contact person identified, promptly informs the Data Controller and the DPO providing all the information useful for entering the treatment in the Register.

2. The Institute also keeps a Register of all the categories of treatments carried out as Manager on behalf of other Data Controllers, containing:
  - a) the structure responsible for the treatment.
  - b) the name and contact details of the Data Controller on whose behalf the Institute acts and of the Data Protection Officer.
  - c) the categories of treatments carried out on behalf of each Data Controller.
  - d) the possible transfer of personal data to a third country or an international organization, with the indication of the third country or international organization and the documentation of adequate guarantees.
  - e) where possible, a general description of the technical and organizational security measures adopted.
3. The Registers, kept in written form, also in electronic format, are made available to the Guarantor or the assignors upon justified request.

#### **Art. 18 - EVALUATION OF THE IMPACT ON DATA PROTECTION**

1. When a type of processing, when it involves, in particular, the use of new technologies, given the nature, object, context and purposes of the processing, is likely to present a high risk to the rights and freedoms of physical people, before proceeding with the processing, the Institute carries out, in consultation with the DPO, an assessment of the impact on the protection of personal data. A single impact assessment can be conducted for a set of similar treatments posing similar high risks.
2. Without prejudice to the types of treatment identified by the IDPC, the impact assessment is carried out by the Institute in the following cases:
  - a) a systematic and comprehensive evaluation of personal aspects relating to individuals, based on automated processing, including profiling, and on which decisions are based that have legal effects or similarly significantly affect those individuals.
  - b) large-scale processing of categories of personal data referred to in the following art. 23 or data relating to criminal convictions and offences.
  - c) systematic large-scale surveillance of an area accessible to the public.
3. The impact assessment contains the following elements:
  - a) a systematic description of the processing and its purposes.
  - b) an assessment of the necessity and proportionality of the processing about the purposes.
  - c) an assessment of the risks to the rights and freedoms of data subjects.
  - d) the measures envisaged to address the risks, including the safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the EU Regulation, considering the rights and legitimate interests of data subjects and other people involved.

4. If necessary, the Institute reviews to evaluate whether the processing of personal data is carried out following the impact assessment, when changes in the risk posed by the processing activities arise.
5. The Designated, also through the Representatives, inform the Data Controller of all the new treatments they intend to carry out, to allow the same to carry out the impact assessment, where necessary.

#### **ART. 19 - ADVANCE CONSULTATION**

1. The Institute, through the DPO, shall, prior to processing, consult the Malta Privacy Authority if the impact assessment indicates that the processing would present a high risk in the absence of measures taken to mitigate the risk.
2. If it considers that the intended processing would violate the EU Regulation, in particular if the Institute has not sufficiently identified or mitigated the risk, the Authority shall provide a written opinion to the Institute.
3. During the consultation, the Institute shall inform the Authority of:
  - the respective responsibilities of the Institute as Data Controller, as well as of any Joint Data Controllers and Data Processors.
  - the purposes and means of the processing
  - measures and guarantees envisaged to protect the rights and freedoms of data subjects.
  - the contact details of the DPO the data protection impact assessment.
  - any other information requested by the Guarantor.

#### **Art. 20 - INFORMATION FOR THE INTERESTED PARTY**

1. Whenever the Institute provides for the collection of personal data from the interested party, it provides the latter, where it does not already have it and without prejudice to the other cases provided for by art. 14, paragraph 5, of the EU Regulation, the following information:
  - a) the identity and contact details of the Data Controller.
  - b) the contact details of the DPO.
  - c) the purposes and legal basis of the processing.
  - d) any recipients or any categories of recipients of personal data.
  - e) any intention of the Data Controller to transfer personal data to a third country or an international organization, with an indication of the legal basis of the transfer (existence of an adequacy decision by the European Commission or appropriate or suitable guarantees) and an indication of the means to obtain a copy of the data or of the place where they were made available.
  - f) the retention period of personal data or, if it is not possible to indicate the period, the criteria used to determine it.
  - g) the rights of the interested party.
  - h) the mandatory or optional nature of the provision of data and the possible consequences of failure to provide it.
  - i) the possible existence of an automated decision-making process, including profiling, with indications of the logic used as well as the importance and consequences of this treatment for the interested party.

2. If the collection of data does not take place from the interested party, the Institute provides the same, in addition to the indications referred to in paragraph 1, the following information:

- a) categories of data processed.
- b) source from which the data originates.

The Institute provides such information:

- within a reasonable time after obtaining the personal data and, in any case, within one month.
- if the data are intended for communication with the interested party, no later than the first communication with the same.
- if the communication of data to another recipient is envisaged, no later than the first communication to the same.

The Institute is not required to provide this information if:

- The interested party already has them.
  - Communication to the interested party is impossible.
  - communication to the interested party implies a disproportionate effort, in the case of processing for archiving purposes in the public interest, scientific research or statistical purposes, without prejudice to the adoption of adequate guarantees for the rights and freedoms of the interested party and of technical and organizational measures, such as pseudonymization, which ensure compliance with the data minimization principle.
  - communication to the interested party risks seriously jeopardizing the achievement of the purposes of the processing, without prejudice to the adoption of appropriate measures to protect the rights, freedoms and legitimate interests of the interested party, including by making the information public.
  - obtaining the data is expressly provided for by Community or national legislation which provides for appropriate measures to protect the legitimate interests of the data subject.
  - personal data must remain confidential due to an obligation of professional secrecy or a statutory obligation of secrecy.
3. The information is provided in a concise, transparent, intelligible and easily accessible form, with simple and clear language, in writing, also by electronic means, or orally, if requested by the interested party.
  4. If the Institute intends to process the data for a different purpose from that for which they were collected before such further processing it provides the interested party with information regarding this different purpose and any further pertinent information.

## **ART. 21 - PRIVACY AND IT SECURITY**

1. Taking into account the state of the art, the implementation costs, the nature, object, context and purposes of the processing, as well as the probability and seriousness of the risk for the rights and freedoms of physical people, the Data Controller implement

technical and organizational measures that guarantee a level of security appropriate to the risk, protect YHANK INSTITUTE's information assets and prevent the occurrence of security incidents. These measures are tested and verified regularly to guarantee the security of the treatment, with YHANK INSTITUTE having the right to prescribe corrective measures and temporarily or definitively block treatment and the system that contributes to carrying it out until acceptable security parameters are returned.

2. The security measures are described, together with the directives and procedures to be followed, on the YHANK INSTITUTE website.
3. The Designees, the Referrals and each Authorized person are required to comply with the measures and indications referred to in paragraph 2, which are also the subject of the training envisaged by art. 5.

### **Art. 22 - BREACH OF PERSONAL DATA (DATA BREACH)**

of physical people, the Institute communicates the violation to the interested party without unjustified delay.

1. In the event of a personal data breach, the Institute, with communication from the DPO, notifies IDCP of the breach without unjustified delay and, where possible, within 72 hours of becoming aware of it, unless it is unlikely that the violation of personal data presents a risk to the rights and freedoms of physical people. If the notification to the Guarantor is not made within 72 hours, it is accompanied by the reasons for the delay.
2. The notification must contain the following elements:
  - a) nature of the personal data breach, including, where possible, the categories and approximate number of data subjects as well as the categories and approximate number of personal data records involved.
  - b) name and contact details of the DPO or other contact point where more information can be obtained.
  - c) likely consequences of personal data breach.
  - d) measures taken or proposed to be taken to remedy the personal data breach and also, where appropriate, to mitigate its possible negative effects.
3. If and to the extent that it is not possible to provide the information at the same time, the information can be provided in successive stages without further undue delay.
4. When the violation of personal data is likely to present a high risk for the rights and freedoms of physical people, the Institute communicates the violation to the interested party without unjustified delay.
5. Communication with the data subject is not required if one of the following conditions occurs:
  - a) The Institute has implemented the appropriate technical and organizational protection measures (in particular those intended to make the personal data incomprehensible

to anyone who is not authorized to access it, such as encryption) and these measures have been applied to the personal data of the violation.

- b) The Institute subsequently adopted measures aimed at preventing the occurrence of high risk for the rights and freedoms of the data subjects.
  - c) Communication would require disproportionate efforts, in which case a public communication or similar measure is instead carried out, by which the data subjects are informed with similar effectiveness.
6. If the Institute has not notified the data subject of the personal data breach, the Guarantor, after assessing the likelihood that the breach presents a high risk, may request that it be done or may decide that one of the conditions in paragraph 5 is satisfied.
  7. The Institute documents any violation of personal data, the related circumstances, the consequences and the measures taken to remedy them.
  8. The Cybersecurity Sector supports the Data Controller by coordinating with the DPO in the management of data breaches.
  9. YHANK INSTITUTE staff is required to comply with the additional rules and instructions that have been adopted by the Institute, especially as regards the communication of relevant information and cooperation with the competent offices in the management of data breaches.
  10. The Designated, also making use of any Contact person identified, ensures, without unjustified delay, the sending to [data.breach@yhank.com](mailto:data.breach@yhank.com) of all the information useful for the management of the data breach.

## **TYPES OF TREATMENT AND METHODS OF DISSEMINATION OF PERSONAL DATA**

### **Art. 23 - TREATMENT OF PARTICULAR CATEGORIES OF PERSONAL DATA**

1. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data intended to uniquely identify a physical person, data relating to health or a person's sex life or sexual orientation is permitted only if one of the following conditions is met:
  1. the interested party has given explicit consent for one or more specific purposes.
  2. the processing is necessary to fulfil the obligations and exercise the rights of the Institute or the interested party in the field of labor law and social security and social protection.
  3. the processing is necessary to protect a vital interest of the data subject or of another physical person if the data subject is physically or legally unable to give consent.
  4. the processing concerns personal data made public by the data subject.
  5. the processing is necessary to ascertain, exercise or defend a right in court.

6. the processing is necessary for preventive medicine or occupational medicine, assessment of the employee's ability to work, diagnosis, assistance or health or social therapy or management of health or social systems and services and the data are processed by or under the responsibility of a professional subject to professional secrecy.
  7. the processing is necessary for archiving purposes in public interest, scientific or historical research or statistical purposes, the following art. 89 paragraph 1 of the EU Regulation.
  8. the processing is necessary for reasons of significant public interest if provided for by European Union law or by a provision of law or regulation which specify the types of data that can be processed, the operations that can be performed and the reason for the significant public interest, as well as the appropriate and specific measures to protect the fundamental rights and interests of the data subject.
2. Processing carried out on the following subjects is of significant public interest:
- access to administrative documents and civic access.
  - granting, liquidation, modification and revocation of economic benefits, subsidies, donations, other emoluments and qualifications.
  - relations between public entities and third-sector entities.
  - conscientious objection.
  - sanctioning and protection activities in administrative or judicial proceedings.
  - institutional relationships with religious bodies, religious confessions and religious communities.
  - tasks of the national health service and subjects operating in the health sector, as well as tasks of hygiene and safety in the workplace and safety and health of the population, civil protection, protection of life and physical safety.
  - planning, management, control and evaluation of health care, including the establishment, management, planning and control of relations between the administration and subjects accredited or affiliated with the national health service.
  - social protection of maternity and voluntary interruption of pregnancy, addictions, assistance, social integration and rights of the disabled.
  - education and training in school, vocational, higher or university fields.
  - establishment, management and termination of employment relationships of any kind, including unpaid or honorary ones, and other forms of employment, trade union material, compulsory employment and placement, social security and assistance, protection of minorities and equal opportunities in the context of relationships of work, fulfilment of salary, tax and accounting obligations, protection of YHANK INSTITUTE's information assets, occupational hygiene and safety or the safety or health of the population, assessment of civil, disciplinary and accounting liability, inspections.
3. Genetic, biometric and health-related data can be processed only in the presence of one of the conditions referred to in paragraph 1 and in compliance with the guaranteed measures set out by the IDCP.
  4. Genetic, biometric and health-related data cannot be disclosed.

5. In compliance with the obligations concerning the security measures for the protection of personal data, the use of biometric data is permitted concerning the physical and logical access procedures to the data by Authorized subjects, in compliance with the guaranteed measures provided for by law.

#### **Art. 24 - PROCESSING OF PERSONAL DATA IN THE HEALTHCARE FIELD**

1. The Institute's facilities and services operating in the health or occupational prevention and safety sector, except for those referred to in paragraph 5 below, process personal data suitable for revealing the state of health if necessary for preventive medicine or of work, assessment of the employee's ability to work, diagnosis, assistance or medical or social therapy, management of medical or social systems and services or for reasons of public interest in the field of public health, based on a provision of law or regulation or of European Union law. The treatment is carried out by a professional subject to professional secrecy, or under his responsibility, in compliance with the guaranteed measures established by the Guarantor and with the specific sector provisions.
2. The structures and services referred to in paragraph 1 may adopt simplified methods for releasing Information on the processing of personal data, including the release of Information for a plurality of data processing and the affixing of appropriate and suitable signs and notices easily visible to the public.
3. Information regarding the processing of personal data can be made, without delay, after the service in the event of:
  - a) physical impossibility, incapacity to act or incapacity of understanding or will of the interested party, when it is not possible to return the Information to those who legally exercise representation, or to a close relative, family member, cohabitant, civil partner, trustee or Head of the structure at where the person concerned lives.
  - b) serious, imminent and irreparable risk to the health or physical integrity of the data subject.
  - c) medical performance which may be jeopardized by the prior release of the Information, in terms of timeliness or efficacy.

After reaching the age of majority, information on the processing of personal data is provided to the interested party, if not previously released.

#### **Art. 25 - PROCESSING OF DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENSES**

1. The processing of personal data relating to criminal convictions and offenses for educational institutions is permitted under the GDPR and therefore does not prevent the Institute from asking candidates to produce the full certificate containing any convictions handed down by a court.
2. YHANK INSTITUTE will only be able to request the certificate on criminal convictions and offenses in teacher recruitment procedures and in the selection of governing bodies.

3. The certificate will only be physically presented by the candidate during the job interview and the Institute will not keep a copy. An internal note may be kept for record purposes, simply stating that the candidate is or is not of good conduct. No record of any convictions will be retained.

#### **Art. 26 - PROCESSING OF PERSONAL DATA FOR THE MANAGEMENT OF THE EMPLOYMENT RELATIONSHIP**

1. The Institute carries out the processing of employees' data for recruitment and execution of the employment contract - including the fulfilment of the obligations established by law and collective agreements, management, planning and organization of work, equality and diversity in the workplace, occupational health and safety, protection of YHANK INSTITUTE's property and information assets, termination of the employment relationship.
2. The processing does not require the consent of the interested party, as it is necessary to fulfil the obligations and exercise the rights of the Data Controller and of the interested party in the field of labor law, social security and protection.
3. The processing of personal data in the context of the employment relationship is carried out by adopting appropriate guarantees to ensure the protection of the fundamental rights and freedoms of individuals, including the individual and trade union prerogatives envisaged by the Workers' Statute and by the ethical rules promoted by the Guarantor.

#### **Art. 27 - PROCESSING OF PERSONAL DATA IN THE MEETINGS OF THE COLLEGIATE BODIES.**

1. In the meetings of the collegial bodies of the Institute, the processing of personal data takes place in compliance with these Regulations and for the sole purpose of carrying out, by the members of the Bodies, the preliminary activities necessary for the deliberative purposes of their competence.

#### **ART. 28 - TREATMENT FOR ARCHIVE, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES AND STATISTICAL PURPOSES**

1. In the processing of personal data for archiving purposes in the public interest, for scientific or historical research and statistical purposes, the Institute prepares technical and organizational measures that guarantee compliance with the principle of data minimization, including pseudonymization and anonymization if the purposes of the processing can be achieved by such measures.
2. The treatment for the purposes referred to in paragraph 1 is also carried out beyond the period necessary to achieve the purposes for which the data were previously collected or processed. For these purposes, the Institute may retain or transfer to another Data Controller the personal data of which, for any reason, the treatment has ceased, in compliance with the measures referred to in paragraph 1.

3. As part of its institutional purposes, to promote and support research and collaboration in the scientific and technological fields, the Institute can communicate and disseminate data relating to study and research activities, also to private individuals and electronically, to graduates, PhDs, technicians and technologists, researchers, teachers, experts and scholars, with the exclusion of special categories of personal data and data relating to criminal convictions and offences.

## **ART. 29 - TREATMENT FOR PUBLIC INTEREST OR HISTORICAL RESEARCH PURPOSES**

1. Without prejudice to the provisions of the previous art. 28, personal data collected for archiving purposes in the public interest or for historical research are not used to adopt deeds or administrative measures unfavorable to the interested party, unless they are also used for other purposes according to the principles established by art. 5 of the EU Regulation.
2. Documents containing personal data processed for archiving purposes in the public interest or for historical research are used, considering their nature, only if pertinent and indispensable for the achievement of such purposes. The personal data disclosed are used only for the pursuit of the same purposes.
3. Personal data may, in any case, be disclosed when they relate to circumstances or facts made known directly by the interested party or by his or her behavior in public.
4. The treatment is carried out in compliance with the ethical rules on the subject approved by the IDCP privacy guarantee authority.

## **ART. 30 TREATMENT FOR STATISTICAL OR SCIENTIFIC RESEARCH PURPOSES**

1. Without prejudice to the provisions of art. 28, personal data processed for statistical or scientific research purposes are not used to make decisions or measures relating to the data subject or for processing for other purposes.
2. The information given to the interested party must highlight the statistical and scientific research purposes and can also be given to the family member or cohabitant of the interested party, who answers in his name and on his behalf when the circumstances allow it. The Information is not due when it requires a disproportionate effort compared to the protected right, if the appropriate forms of advertising identified by the ethical rules on the matter, promoted by the Guarantor, are adopted.
3. Apart from the cases of investigations for statistical or scientific research purposes provided for by law, the consent of the interested party to the processing of particular categories of personal data, when requested, can be presented in simplified ways, identified by the deontological rules or by the measures guarantee issued by the Maltese National Privacy Authority.

## Art. 32 - COMMUNICATION AND DISSEMINATION OF PERSONAL DATA

1. The Institute may communicate and disseminate personal data, other than particular data and relating to criminal convictions and offences, in the following cases:
  - communication between Data Controllers who carry out the processing for the execution of a task of public interest or connected to the exercise of public powers, if required by law, regulation or by European Union law. In the absence of these rules, communication is permitted if necessary for the performance of tasks of public interest and the performance of institutional functions and can be initiated after the term of forty-five days from the communication to the National Privacy Authority, without itself having adopted a different determination of the measures to guarantee the interested parties.
  - Communication and dissemination necessary for purposes of defense or security of the State or for the prevention, detection or repression of crimes, with the observance of the rules governing the matter.
  - communication and dissemination, also at the request of private individuals and by electronic means, of data relating to the intermediate and final training results of students, graduates, specialists, scholarship holders, doctoral students, research fellows and other training profiles, as well as of subjects who have passed the state exam, and other pertinent common personal data concerning the purpose of facilitating the orientation, training and professional insertion, even abroad, of YHANK INSTITUTE students and graduates, also through invitations to meetings, events, meetings and congresses.
  - communication to funders of doctoral scholarships and research fellowships of personal data relating to doctoral students and research fellows who have made use of the funding.
  - communication to other public administrations and dissemination, also on YHANK INSTITUTE's websites, of the names of the Institute's personnel and collaborators, of the role, held, of the telephone numbers and the institutional telematic addresses, to favor institutional communication.
  - communication to public and private entities of data necessary for the management of the employment relationship relating to personnel transferred, seconded, seconded or in any case assigned for service to an entity other than the one to which they belong.
  - communication to public and private subjects who organize and manage training courses of common data of the personnel who participate in these courses.
2. Requests addressed to the Institute to obtain the communication or dissemination of personal data must be addressed in writing to the Head of the structure and must contain:
  - the name, denomination or company name of the applicant.
  - the data to which the request refers, the purposes and methods of use of the requested data.
  - the possible scope of communication of the requested data.
  - the declaration that the applicant undertakes to use the data received exclusively for the purposes and in the context of the methods for which they were requested.

3. The communication and dissemination of categories of personal data of students, graduates and other educational profiles are excluded.
4. The Institute issues certificates containing personal data relating to YHANK INSTITUTE students or graduates to third parties, upon presentation of a proxy signed by the interested party, accompanied by a photocopy of an identity document of the delegating party and the delegate.
5. The Institute may communicate and disseminate anonymous or aggregated data for scientific research or statistical purposes.

### **ART. 33 - COMMUNICATION AND DISSEMINATION OF DATA RELATING TO RESEARCH ACTIVITIES**

1. Within the scope of its purposes, to promote and support research and collaboration in the scientific and technological fields, the Institute may communicate and disseminate data relating to study and research activities, including to private individuals and electronically, to graduates, PhDs, technicians and technologists, researchers, teachers, experts and scholars, with the exclusion of data belonging to particular categories and data relating to criminal convictions and offences.
2. The Institute may communicate information relating to scientific productivity, recognitions and funds acquired by individuals, groups or specific scientific-disciplinary sectors, also in the context of evaluation procedures for funding requests or research projects, to:
  - promote planning models for research activities and resource allocation according to mechanisms that make it possible to guarantee transparency in the definition of priorities, to adequately exploit the capabilities of individuals and groups and to respect the principles of transparency and fair treatment.
  - encourage cooperation between individuals and groups through precise knowledge of the results achieved, to improve the ability to attract external funding or to establish forms of structured collaboration with third parties.
  - provide guidance and support for the development of organizational models to support research, also through the implementation of comparative analyses and the sharing of good practices.
3. The Institute can communicate personal data to public entities that have disbursed funding for research, for reporting purposes and to allow statistical processing.

### **Art. 34 VIDEO SURVEILLANCE**

1. The processing of personal data through video surveillance systems by the Institute takes place exclusively in the context of carrying out institutional functions, for:
  - a) safety and security of the Institute's staff, students and visitors to various capacities of the Institute's spaces.
  - b) protection of YHANK INSTITUTE's real estate assets.
  - c) protection of the movable property of the Institute and users.

- d) prevention of vandalism. access to gates or properties pertaining directly to the YHANK INSTITUTE.
2. The processing is carried out, following the provisions of the YHANK INSTITUTE Regulation on video surveillance, in compliance with the rights, fundamental freedoms and dignity of the data subjects and in compliance with the principles of necessity and proportionality.
  3. Where from the impact assessment, due to the nature of the data processed, the methods of treatment or the effects that the treatment can determine, specific risks emerge for the fundamental rights and freedoms of the interested parties, the Institute requests the Guarantor Authority a prior consultation. The need to carry out an impact assessment remains unaffected whenever large-scale video surveillance systems are installed in rooms or areas accessible to the public.
  4. In the structures where video surveillance systems are in operation, specific information must be posted, visibly by the interested party and before entering the operating range of the video cameras, informing the public of the presence of the systems, of the name of the Data Controller and the aims pursued.
  5. The Institute guarantees the protection and security of personal data collected through video surveillance systems by:
    - the limitation of access to the images to specifically Authorized subjects.
    - specific training on data protection of the personnel involved in the operations of recording, displaying and storing the images and of the personnel in charge of plant maintenance.
    - the conservation of the images only for the time necessary to achieve the aims pursued and in any case for a maximum time of 3 days from the collection, except in cases of specific investigative requests from the judicial authority or the judicial police, as well as the cases of closure scheduled by the YHANK INSTITUTE or special needs related to certain systems that may require shorter or longer storage times,
    - the application of security measures appropriate to the level of risk aimed at reducing the risk of destruction, loss, and even accidental, unauthorized access, and processing that is not permitted or does not comply with the purposes of the collection.

#### **Art. 35 - RIGHT OF ACCESS AND CONFIDENTIALITY**

1. The conditions, methods and limits for exercising the right of access to administrative documents containing personal data and relative protection are governed by the provisions of the law on the subject, as well as by the relative implementing regulations, also as regards the categories of data and data relating to criminal convictions and offences.
2. The exercise of the right of access, if it involves the communication of personal data of third parties, must be limited to the data necessary to satisfy the right itself. The principle remains that conflicts between the right of access and the privacy of third parties must be resolved in the sense that access, aimed at the care or defense of one's legitimate

interests, prevails over the need for confidentiality, to the extent that it is necessary for the defense of a legally relevant interest.

3. When the treatment concerns genetic data, relating to the health, sex life or sexual orientation of the person, the treatment is allowed if the legally relevant situation that it is intended to protect with the request for access to administrative documents is at least equal in rank to the rights of the data subject or consists of a personal right or another fundamental right or freedom.

## **FINAL RULES**

### **Art. 36 - SCOPE OF LIABILITY**

1. The Institute, as Data Controller, is responsible for the material or immaterial damage caused by the treatment itself in violation of the provisions of the EU Regulation and of the Code, unless it demonstrates that the harmful event is not attributable to it in any way.
2. The Institute, as Data Processor, is responsible for the damage caused by the processing only if it has not fulfilled the obligations of the EU Regulation and the Code specifically aimed at Data Processors or if it has acted in a different or contrary way to the legitimate instructions of the Data Controller unless it demonstrates that the harmful event is not attributable to it in any way.
3. If the Institute were to be sanctioned for actions or omissions related to the violation of data protection rules and instructions, the responsibility of which is exclusively attributable to one of its employees, it will assess whether the conditions exist for contesting the damage and acting in the competent offices both for regarding the patrimonial aspect and the disciplinary aspect.
4. The criminal liability specifically provided for by the Code rests with the single person to whom the illegitimate use is attributable.

---

27

### **Art. 37 - REFERENT STRUCTURE FOR THE EXECUTION OF THE REGULATION**

The structure of the YHANK INSTITUTE referent for the implementation of this Regulation, indications, forms and information useful for the implementation can be found on the page <https://www.yhank.com/.....>

### **Art. 38 - ENTRY INTO FORCE AND REVISION OF THE REGULATION**

1. These Regulations and any subsequent amendments are approved by the Board of Directors and enter into force on the fifteenth day of publication on the YHANK INSTITUTE website. This procedure does not apply to the amendment referred to in Annex A to this regulation.
2. For anything not expressly provided for by this Regulation, please refer to the provisions of the EU Regulation and the relevant national legislation, in addition to the provisions of

the Deontological Rules approved by the Malta Privacy Authority and the YHANK INSTITUTE legislation on the protection of personal data.