No. Fax.: 11.17.001.009.174 No. tel. 22 818456 No. Fax.: 22304565 Decision in the form of Orders regarding the processing through the electronic form rei... START – Lime Survey by TEPAK On the occasion of phone calls and written questions that I have received from students as well as representatives of Trade Union Organizations of the Academic Staff of the Technological University Cyprus (TEPAK), regarding the above matter, I have investigated and confirmed the following: A. Facts - findings - communication: 2.1 TEPAK, for the purposes of checking the possession of vaccination and disease certificates, collects and processes personal data of Academic and Research staff and the Students. The collection of data concerns simple data but also special categories of data, i.e. health data (information about vaccination or illness from COVID - 19 and the relevant certificates). The collection and processing of data is carried out through a tool/electronic form which is available at the online address: https://web.cut.ac.cy/limesurvey/index.php/395957?lang=en 2.2 The said form belongs to the software /platform for creating electronic questionnaires of the company LimeSurvey GmbH based in Germany and operating via the Internet. The creation, management and hosting of data in the company's cloud infrastructures are among the services it offers. 2.3 My Office's investigation carried out on August 3, 2021 showed that the collection and processing related to the following data ADT, Position, Department, certificate (of illness and vaccination) and date. of their issuance, which fall within the interpretation of the term "personal data" in accordance with the provisions of Article 4(1) of General Regulation 1 ("subject identifiable natural person for Data Protection (Regulation (EU) 2016/679 ("hereinafter the Regulation")): "personal data": any information concerning identified or data"); 2.4 TEPAK for all purposes of the Regulation and in accordance with the definition attributed to the term "processor" of the above database and of the processing in general, constitutes the controller: "7) "controller": the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of processing of personal data;" 2.5. Based on the same investigation by my Office on August 3, 2021, it was noted and/or noted the content of the information based on the electronic form prior to the collection of the personal data of the data subjects which is quoted in full for the purposes of easy reference: " The data is submitted on an optional basis, in the context of the collective effort to operate the University and to offer the courses from September 2021 with a physical presence. The academic and research staff (faculty members, EEP, EE, Research Associates) who submit here proof of vaccination or illness (last 6 months), will not be subject to a safe pass check during their presence at the University. In this way, we significantly facilitate our movements in the spaces. The following are considered as evidence: a) Certificate of vaccination with at least one dose and after a period of 3 weeks has passed, or b) Evidence that the person has suffered from

the disease COVID-19 in the last 6 months. The certificate from the GESY vaccination portal or the EU Digital Covid Certificate (vaccination or disease) are accepted. The information entered is kept confidential under the responsibility of the University's Health and Safety Officer. The data will be deleted after one year. Academic staff who have not been vaccinated or ill DO NOT complete this form and do not submit any safe pass certificate here. The safe pass possession check for these people will be done in a way that will be determined and announced separately by the University. 2.6 In a telephone conversation I had on August 2 and 3, 2021, with the Rector and the Head of the Studies and Student Welfare Service of TEPAK, it was confirmed that the collection and processing of data through the electronic form concerned other than the Academic Staff and students (even though based on the relevant information in the form it is not clear that it also concerns the collection of student data), 2 of their positions were heard and the positions of my Office were explained regarding the following: "the legislative framework and specifically - - that the collection and processing of the above data cannot be based on the consent of the data subjects due to the heteronormative relationship between employer and employee, - that the collection of data via an electronic form and its preservation in electronic and/or paper form for a period of time exceeding one year the limits of what is lawful and legitimate in so far as it is set outside the mandate of the law (Decree) - that said processing negates and/or violates the basic principles of lawful data processing (see article 5(1)), such as the Principles of Lawfulness, Proportionality, and limitation of the period of data storage / retention, - that the collection of data via the Internet constitutes processing which by its nature carries and/or entails risks related to the security of processing and personal data. For the purpose of minimizing the risks deriving from the use of the Internet I introduced to TEPAK as an excellent alternative the use of an intranet instead of the Internet. 2.7 In subsequent communication with TEPAK on 3/8/2021, I was informed of its intention to take the following actions to comply with the legislative framework and its positions in general: (a) Delete and/or delete the field of the electronic form on which required the uploading of vaccination and disease certificates (b) Non-observance of the data for one year, (c) Deletion of the certificates of approximately 65 data subjects that had already been uploaded to the TEPAK database. (d) Assurance that the data is stored on TEPAK's local servers and that it is not hosted in the cloud infrastructure of the provider LimeSurvey GmbH and, (e) The special circumstances of the Foundation regarding the large number of controlled natural persons regarding the possession of safe pass (personal and students) and its housing in different buildings and facilities. 2.8 According to a more recent investigation and/or check of the electronic form carried out by my Office on 4/8/2021, the following has been established and/or confirmed: 2.8.1 The wording of the information at the beginning of the form has been formatted as follows:

3 for this they inform "rei... START - Responsible declaration for vaccination/disease (Academic and Research Staff) 1. The data is submitted voluntarily, in the context of the collective effort to operate the University and to offer the courses from September 2021 with physics presence. Alternatively, you can inform about it by sending an email to XXXXXX or by calling XXXXXX. The academic and research staff (members of the Faculty, EEP, EE, 2. Research Associates) who have had a vaccination or illness (last 6 months), will not be subject to a safe pass control during their presence at the University, with the exception of the first time they they are asked to show the certificate to an authorized person. In this way, we significantly facilitate our movements in the spaces. 3. The information registered (on the University's server) is kept confidential under the responsibility of the University's Health and Safety Officer. 4. Academic staff who have not been vaccinated or ill DO NOT fill out this form and do not submit any safe pass certificate here. The safe pass possession check for these people will be done in a way that will be determined and announced separately by the University." 2.8.2 In the light of the above actions of TEPAK based on the wording of the information as above, I consider that TEPAK has partially taken individual actions to comply and/or restore legality as follows: (a) Set alternatives to the completion of the electronic form solutions such as sharing the information by sending an e-mail or by phone call. (b) Deleted and/or deleted the field of the electronic form that required the uploading of vaccination and disease certificates. (c) He deleted that part of the information that referred to the retention of the data for one year, but without providing information about the retention period to the data subjects, a constituent element of the principle of transparency and the fulfillment of the obligation for a specific , specific, legitimate, objective, complete and transparent information (articles 5(1)(a), 12 and 13 of the Regulation). It is pointed out that the above actions of TEPAK do not imply full restoration of legitimacy and compliance with the provisions of the Regulation, but in any case they will be taken into account as mitigating factors in context and for the purposes of imposing the appropriate administrative sanction. 4 B. Legislative framework: 3.1. Undoubtedly, Decree No. 32 of the Ministry of Health dated 30/7/2021 in pars. 82, 83,84 and 48(c) as a Regulatory Administrative Act and secondary legislation constitutes the legal basis for the minimum permitted collection and processing, by the relevant Safety and Health officer, of the minimum data for the purposes of controlling the implementation of the restrictive measures in the facilities / infrastructures of TEPAK. The collection and processing derives legally from a combination of the provisions of the articles of Regulation 6(1)(c), as a legal obligation of the data controller pursuant to the Decree and 9(2)(i) by which the processing of sensitive data becomes permissible data, i.e. health data such as the information about the disease with covid 19 or vaccination where the processing of personal data is considered

necessary for reasons of public interest in the field of public health. 3.2 The following paragraphs of the Decree are relevant: "82. All workers, including the self-employed, must have either a negative laboratory test or rapid antigen detection test for COVID-19 disease with the sample taken within 72 hours, or a certificate of vaccination for COVID-19 disease with at least one dose and provided that a period of three weeks has passed after the date of vaccination, or a certificate of recovery from the disease of COVID-19 and provided that a period of six months has not passed since the sampling date of their initial positive diagnosis: Provided that, employers must to ensure the compliance of their employees with the provisions of this Regulation: 83. In all indoor and outdoor spaces as well as premises where, observing the distancing measures, there is the possibility of gathering more than 10 people, including employees, it is required for persons of age 12 years of age or older production of either a negative laboratory test or rapid antigen detection test for COVID-19 disease with the sample taken within 72 hours, or a certificate of vaccination for COVID-19 disease with at least one dose and assuming that a period of three weeks has passed after the date of vaccination, or a certificate of recovery from the disease of COVID-19, with a validity of six months from the sampling date of their initial positive diagnosis: It is understood that, for control purposes, it is acceptable to present a Digital COVID Certificate of the European Union (EU Digital Covid Certificate): 84. All persons who enter and/or travel in areas for which it is required to present either a negative laboratory test or rapid antigen detection test for the disease of COVID-19 with the sampling carried out within 72 hours, or vaccination certificate from the Republic for the disease of COVID -19 at least with one dose and provided that a period of three weeks has passed after the 5 date of vaccination, or a certificate of recovery from the disease of COVID-19 and provided that a period of six months has not passed from the sampling date of their initial positive diagnosis, must carry an identity card or passport with them, as additional proof, when requested by the competent authorities and/or by the owners and/or directors and/or administrators who have under their control the business and/or property and/or and the persons authorized by them, pursuant to Regulation 48. 48(c) for the purposes of control and supervision of the implementation of the measures of the Law on Disinfection (Chap. 260), as well as of this Decree, in cooperation with the Cyprus Police, are authorized by the respective Competent Authority, officials of the following Ministries and/or Services as well as the self-employed persons who have been selected by the Ministry of Energy, Trade and Industry, after procedure for announcing a tender for the purchase of services: (i) Ministry of Finance, (ii) Ministry of Education, Culture, Sports and Youth, (iii) Ministry of Labour, Welfare and Social Insurance, (iv) Ministry of the Interior, (v) Ministry of Transport, Communications and of Works, (vi) Deputy Ministry of Research, Innovation and Digital Policy, (vii) Deputy Ministry of

Shipping, (viii) Deputy Ministry of Tourism, (ix) Health Services of the Department of Medical Services and Public Health Services of the Ministry of Health, (x) Department of Agriculture, Department of Forestry , Department of Fisheries and Marine Research, Mines Service and Veterinary Services of the Ministry of Agriculture, Rural Development and Environment ) /Departments, Law Organizations, Independent Authorities, Local Government Authorities and Businesses, (xvi) hold a Law Security Services license 3.3 From the above provisions of the Decree and specifically from the wording used and marked in bold letters (presentation), it does not appear with clarity and accuracy legal requirement for the collection, processing and retention of personal data of the controlled natural persons, however for the purposes of practical application of the control measures in combination with expansive interpretation of the provisions and teleological interpretation of the intention and / or purpose of the legislator, will could be justified, especially in the context of the labor sector and with regard to large Privately Written a of the Provision of Security Services and Private Guards which is issued pursuant to the 2007 to 2014 Laws on Private Public Service Providers. Private Health Officers and 6 Organizations, as necessary the collection and observance of the absolutely necessary data / information in relation to the possession of the safe pass by the staff, in the sense of for example the creation of an xls file which could include e.g. name or employee / student registration number and that he holds a vaccination or illness certificate. Any other and/or further information which is not absolutely necessary for the purposes of identifying employees / students, e.g. in the case of a surname, is not deemed necessary under the circumstances. The duration of data retention should not exceed the period of the legal requirement, i.e. the validity of the Decree. 4. Relevant as the reference in par. 3.1 above are the following provisions of the Regulation: 4.1 Basic principles (article 5): 5. (1). Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), b) are collected for specified, explicit and lawful purposes and are not further processed against in a manner incompatible with those purposes; further processing for archiving purposes in the public interest or for scientific or historical research or statistical purposes shall not be deemed incompatible with the original purposes pursuant to Article 89(1) ("purpose limitation"), c) for which data are processed"), are accurate and, where necessary, updated; d) all reasonable steps must be taken to immediately delete or correct personal data that is inaccurate, in relation to the purposes of the processing ("accuracy"), e) are kept in a form that allows the identification of data subjects only c for the period required for the purposes of processing the personal data; the personal data may be stored for longer periods, as long as the personal data will be processed only for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical

purposes, in accordance with Article 89 paragraph 1 and provided that the appropriate technical and organizational measures required by this regulation are applied to safeguard the rights and freedoms of the data subject ("restriction of the storage period"), f) are subjected to processing in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"). are appropriate, relevant and limited to what is necessary for the purposes ("minimizing the 7 of health care and 4.2 The legal basis for data processing is the provisions of articles 6(1)(c) and 9(2)(i): 6(1)(c) the processing is necessary to comply with a legal obligation of the controller, 9(2)(i) the processing is necessary for reasons of public interest in public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of medical devices, based on Union law or Member State law, which provides for appropriate and specific measures to protect rights and freedoms of the data subject, in particular professional confidentiality, or". 5. Also relevant are the provisions of the Regulation which grant me the following powers within the framework of the duties and responsibilities in light of which I act – 5.1 Article 57(1)(a) and (h): Subject to the others tasks set out in this regulation, each supervisory authority on its territory: of medicines or "a) monitors and enforces the implementation of this regulation, conducts investigations related to the implementation of this regulation, h) inter alia based on information received from another supervisory authority authority or other public authority,'. to notify the controller or processor 5.2 Article 58(1)(a) and (d) and Article 58(2)(a), (d) and (i): “58(1)(a) to instructs the controller and the processor and, where applicable, the representative of the controller or the processor to provide any information it requires for the performance of its duties, d) for an alleged violation of this regulation, 58 (2)(a) to issue warnings to the controller or processor that intended processing operations are likely to violate provisions of this regulation, d) to instruct the controller or processor to make the processing operations compliant with the provisions of this regulation, if necessary, in a specific way and within a certain period, 8 the identity and contact details of the data controller to impose administrative p ripe under article 83, in addition to or instead of i) the measures referred to in this paragraph, depending on the circumstances of each individual case. 5.3 Article 12(1): Information / Transparency "(1) The controller shall take appropriate measures to provide the data subject with any information referred to in articles 13 and 14 and any communication in the context of articles 15 to 22 and article 34 regarding the processing in a concise, transparent, understandable and easily accessible form, using clear and simple wording, especially when it comes to information addressed specifically to children. The information is provided in writing or by other means,

including, if appropriate, electronically. When requested by the data subject, the information may be given orally, provided that the identity of the data subject is proven by other means." Article 13: "1. When personal data concerning a data subject is collected from the data subject, the controller shall, upon receiving the personal data, provide the data subject with all of the following information: a) and, where applicable, the controller's representative , b) case, c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing, d) if the processing is based on Article 6 paragraph 1 point f), the legitimate interests pursued by the data controller or from a third party, e) character, if any, f) as the case may be, the intention of the data controller to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission or, when it comes to the transmissions referred to in article 46 or 47 or in article 49 paragraph 1 second subparagraph, reference to the evidence or suitable guarantees and the means to obtain a copy of them or where they were made available. 2. In addition to the information referred to in paragraph 1, the controller, when receiving the personal data, provides the data subject with the following additional information necessary to ensure fair and transparent processing: a) the time period for which the personal data will be stored or, when this is impossible, the criteria that determine the period in question, b) the existence of the right to submit a request to the data controller for access and correction or deletion of the data the contact details of the data protection officer, against recipients or categories of recipients of personal data 9 the receipt of automated personalization or restriction of processing concerning the subject of the data or the right to object to the processing, as well as the right to data portability, c) when the processing is based on Article 6 paragraph 1 item a) or in article 9 para paragraph 2 point a), the existence of the right to withdraw his consent at any time, without affecting the legality of the processing based on the consent before its withdrawal, d) the right to submit a complaint to a supervisory authority, e) whether the provision of personal data constitutes a legal or contractual obligation or requirement for the conclusion of a contract, as well as whether the data subject is obliged to provide the personal data and what possible consequences would be the failure to provide such data, f) decisions, existence including profiling, referred to in Article 22 paragraphs 1 and 4 and, at least in these cases, important information about the logic followed, as well as the importance and intended consequences of said processing for the data subject." C. Conclusion / Disposition: 6. In view of all the evidence before me including the investigation carried out by my Office, the communication / positions / actions of TEPAK, the reasoning and the Legislative framework in accordance with Parts A and B above - I judged , the collection/processing and preservation of personal data by TEPAK via the Internet, using the electronic form of the LimeSurvey

platform, as processing contrary to the Principles - (a) of legality (in excess of the legal requirement of the Decree), objectivity, transparency, (lack of and insufficient information since the information part at the beginning of the form does not provide the necessary and minimal information to ensure the necessary transparency on the basis of articles 12 and 13 of Regulation (EU) 2016/679, as set out in Part B above, (b) of necessity and proportionality, in the sense that the processing exceeded the measure of what is necessary and proportionate as referred to with the use of the electronic form of the mentioned platform, considering that on the one hand there were other less intrusive solutions (xls file via intranet), as well as with regard to the quantity and quality of the data that have been collected before the formation of the form, e.g. certificate disease, vaccination certificate, 10 (c) the data retention period (one year) which is not justified by the legal requirement, i.e. the Decree, which does not even provide for the retention of this data, as well as (d) data security , due to their exposure to the internet environment and third-party software, i.e. the provider of the specific platform instead of the processing being carried out in a digital environment of the internal network or intranet of TEPAK. 7. However, since I counted as mitigating factors the actions of TEPAK to restore legitimacy, as in par. 2.8.2 above I decided to impose on TEPAK the administrative sanction of the Order, in compliance with the provisions of article 58(2)(d), which I consider appropriate and proportionate under the circumstances. According to the provisions of article 58(2)(d) – Each Control Authority has the power - “d) to instruct the data controller or the processor to make the processing operations comply with the provisions of this regulation, if necessary, in a specific way and within a certain period," Exercising the aforementioned powers granted to me by the Regulation, I direct the following Commands to TEPAK - Command 1st: Immediately terminate the processing through the electronic form as the process described in Part A. Command 2nd: Delete or destroy, as the case may be, the vaccination certificates and disease from its database or records, which it has already collected. Order 3rd: Take all the necessary, legal actions to make the processing legal, legitimate and compliant with the above basic principles of the Regulation in accordance with my suggestions. Order 4th: Notify my Office within an exclusive period of 2 weeks from receipt of this all actions to implement Orders 1 - 3. Irini Loizidou Nikolaidou NICOSIA Data Protection Commissioner August 5, 2021Personal Character

TO