No. Fac.: 11.17.001.008.029 October 14, 2020 ME TO HERI Subject: Complaint regarding the security of personal data held by the TEF-ATIK Association and the ATIK Company DECISION I reviewed (Law 125(I)/2018), of the Data I refer to the correspondence between us regarding the above matter and inform you of the following: Facts 1.1. Based on the task of examining complaints provided to the Personal Data Protection Commissioner by article 57(1)(f) of Regulation (EU) 2016/679 (hereinafter "the Regulation") and article 24(b) of the Law which provides for the Protection of Natural Persons Against the Processing of Personal Data and for the Free Movement of the complaint/complaint of XXXXXX, employed by the Company ATIK (Cyprus Telecommunications Authority - hereinafter "the Company"), regarding security issues of the employees' personal data of the ATIK Company, which arose during the examination of the complainant's request to exercise the right of access to her personal data held by the TEY-ATIK Association (Cyprus Telecommunications Authority Employees Welfare Fund - hereinafter "the Association"). Specifically, on October 26, 2019, the complainant requested via email from XXXXXX, the Union's Data Protection Officer, to exercise her right of access based on Article 15 of the Regulation and to obtain a copy of the personal data held by the Union for the individual as well as the source of origin of said data that were not collected by it. 1.2. On November 18, 2019, XXXXX, responded by email to the complainant, stating the following "The personal data that the Association maintains for the specific member are as follows Employee number, Gender, Full name, Date of birth, Date of employment, Date of registration in the TEY -ATIK, Mailing address, 1 Service phone, Mobile phone, E-mail address. The above is collected from the CYTA database through the "Personal Data Exchange and Protection Agreement" signed between TEY-ATIK and CYTA. 1.3. On November 28, 2019, the complainant sent a new request to the Union, asking how she "has a direct relationship with the Union, regarding the personal data held on [her] person". 1.4. As XXXXXX states in her complaint, on December 3, 2019, XXXXXX contacted her by phone and asked her to come by his Office to hand-deliver the Union's letter to her, regarding the request dated October 26, 2019, and to obtain a copy of all personal data held by the Association about her person. 1.5. With the said letter, the Association also attached a copy of her photograph. 1.6. On January 22, 2020, the complainant, after not having received any response from the Union regarding the request dated November 28, 2020, sent a new email to XXXXXX, requesting as she has a response to her letter. 1.7. On the 23rd of the complainant, informing her that January 2020, XXXXX responded to her request "Regarding the above matter and in continuation of your request for a direct relationship with TEY-ATIK for the personal data kept on your person, we inform you that your request cannot be granted. Attempts have been made in the past to separate the database maintained by TEY-ATIK for its members from the database

maintained by CYTA for its employees, but technical problems have been encountered which remain insurmountable. Therefore, the collection of data by TEY-ATIK for its members from the CYTA database is considered a necessary condition for the smooth operation of TEY-ATIK and your data cannot be managed separately." 1.8. Based on the above, on February 25, 2020, I sent a relevant letter to the Company's Data Protection Officer and the Union's Data Protection Officer. With my letter in question, having as decisive criteria for the control of the legality of the processing of personal data, the principles of legality, limitation of purpose and above all minimization (Article 5(1)(a), (b) and (c) of the Regulation), I asked the Defendants of the complaint to state, by March 31, 2020 at the latest: (a) the reasons why the database of the Association could not be separated from the database of the Company, since the person in charge processing and the purpose of keeping each record is different, 2 (b) whether the staff of the Association had access to the personal data of all employees of the Company or only of its members and how such access was achieved, (c) the technical and organizational security measures observed by the Association in relation to the personal data it was processing and (d) on which legal basis of articles 6 and 9 of the Regulation the Association is authorized to process personal data, the are collected directly by the Company. 1.9. XXXXX, the Company's Data Protection Officer, by letter No. Fac.: LGLK10-426 and dated 27.03.2020, he told me, among other things, the following (a) The Association maintains an electronic file with the Register of Fund Members, which is updated by extracting information from the database of the Company's Personnel Services automatically electronically. The Union's file and the Company's Personnel Services database are two different files. (b) The automatic extraction of updated information from the database of the Company's Personnel Services is necessary in order to ensure the correct provision of benefits to the members of the Association, based on this updated information. (c) The Register of Members of the Union includes the following data of the Company's employees and pensioners, which it automatically draws from the Company's electronic database: Employee number Gender Full name Photograph Date of birth Date of employment Date of death (where applicable) Date retirement Mailing address Business telephone (where available) Landline (where available) Mobile telephone (where available) Email address Associated employee number Status widow, dependent child In addition, the Company sends Association, Excel files, with the following information of members of the Association, for the purposes of checking and netting subscriptions and other amounts payable to the Association Employee number Employee name Status Active employ Retired/widower/widow Amount of monthly subscription 3 Amount of VAT on the monthly subscription Other payable, to Union, amount deducted from a Union member's salary/pension/benefit. (d) The staff of the Union (a total of nine people), has

automatic electronic access to the Registry of Union Members and to the excel files sent by the ATHIK Company. (e) Additionally, the staff of the Union has access to the following personal data of the Company's employees who are not members of the Union□ □ Employee number □ Employee name □ Business phone (where available) □ Mobile phone (where available) □ Electronic address (where available) □ Rank and specialty in the service □ Work address (f) Access to the above d is ensured by automatic connection of the official computers of the Union's staff with the official Intranet Portal of the Company. (g) The suspension of access by the Union to the Company's database, to personal data of Company employees, who are not members of the Union, is expected to be completed on March 31, 2020. (h) Since the adoption of the Regulation, the Union has proceeded , among other things, in the following technical and organizational measures□ - Creation of a safe storage area for the paper file and introduction of security measures for the storage of the electronic file, with limited access, only by the necessary staff of the Association. - Destruction of a file that included personal data from earlier years and updating of the electronic and paper file. - Staff training. - Appointment of XXXXX, as Data Protection Officer. - Signing of Data Exchange and Protection Agreement, dated October 15, 2018, between the Company and the Union. - Posting of the Privacy Policy of Personal Data, on its website. (i) The legal basis on which the processing of personal data by the Association was based is articles 6(1)(a) and (b) of the Regulation. 1.9.1 In said letter dated 27.3.2020 the relevant agreement dated between the Company and the Union was also attached. 15.10.2018 for "Exchange and 4 Protection of Personal Data". In par. 3.1 of the Agreement of this, the data which the Company undertakes to deliver to the Fund, after having previously received the written consent of the Company's employees and pensioners, were mentioned. It was agreed that a File with the Register of Members of the Fund and information such as Employee Number, Identity Card Number, Gender, Full Name, Date of Birth, etc., would be delivered. In the data that would be delivered, there was no agreed photo of the employee. 1.10. On April 9, 2020, I sent a letter to the Chief Executive Officer of the Company and the Chairman of the Board of Directors of the Association stating, inter alia, that: (a) The Association and the Company are two separate controllers who maintain two separate records for different purposes . (b) The Association and the Company have an obligation to observe the basic processing principles, as defined in article 5 of the Regulation. Therefore, the Company should have known that granting Union staff access to its database, in relation to employees who are not members of the Union, violates the principle of purpose limitation, the principle of minimization and the principle of integrity and confidentiality (Article 5(1) of the Regulation). (c) Additionally, the illegal granting of access by the Company to the Union and by extension, the illegal access to the Company's file by the Union, constitutes a

violation of the security of the processing (article 32 of the Regulation). (d) From the letter and the purpose of article 32 of the Regulation concerning the security of the processing, it is clear that the obligation of the controller to ensure the security of the processing is both preventive and repressive in nature. Preventive, so that the applicable measures prevent incidents of personal data breach, repressive, so that any incident can be detected and investigated. It is pointed out that the Company had not implemented the technical possibility to allow access by the Association only to the personal data that it is authorized to process and that only concern its members. (e) Based on the above, it appears that the Company did not adopt the most appropriate measures for the security of the processing, in violation of Article 32 of the Regulation. In the same letter, I requested the positions/comments of the Complainants regarding the above as well as how they would answer the following questions (a) The legal basis by which the Union had access to the Company's database and received personal data not members of the Association (and by extension the legal basis on which the Company provided such access), (b) whether said access had already been terminated, 5 (c) the actions taken by the Association to destroy the data kept on file and related to non-members and (d) the reasons why the Association needed to keep the photograph of its members. 1.11. XXXXX, in an email dated April 27, 2020, informed me that: (a) The access granted to the Association by the Company allowed the Association to view ("view only") and retrieve only the necessary basic service information of the employees the company's. The extraction of the basic service data was achieved using a relevant application designed by the Company's IT department. The application allowed the authorized persons of the Union to enter the number of the employee whose status they wished to update and only receive a confirmation that the employee with the number they entered is a member of the Union, by viewing information such as the employee's first and last name, his department, the building he works in, his rank and specialty, information which was already registered in the Company's Intranet Employee Information File. (b) No copies or files were created by the Association with these data. (c) The Association, after having carried out the relevant inspection, then updated the relevant status of its member. These situations were updated at regular intervals. (d) The Company, for security purposes, limited the members of the Association who were able to view the above-mentioned information and installed a system to track their access. (e) The legal basis on which the access was based is Articles 6(1)(a) and 6(1)(b) of the Regulation. (f) The ability to view the information of non-members of the Association was suspended from March 31, 2020, with a relevant upgrade of the application. (g) The Association did not keep copies or records of data of non-members. (h) The Association did not keep the photo of its members in any file. Only the Company maintained a photo of its employees on the intranet. 1.12. By letter

from the Office with No. Fac. 11.17.001.008.029 and dated April 29, 2020, I requested from the Company as stated: (a) Exactly one by one the types/categories of personal data that the Association had the right to view ("view only") for its members. (b) The types/categories of personal data that the Association drew from the Company's database and to explain the meaning of the term "draws" in this case. 6 (c) The types/categories of personal data that the Association had the right to view and/or retrieve and/or process in any form for its non-members. (d) The number of people of the Association who had the possibility to view the personal data of their members and non-members before March 31, 2020, the date on which, as the Defendants reported the complaint in their letter dated April 27, 2020, a relevant upgrade had been made and the ability to view the information of non-members of the Association was stopped. (e) The number of members of the Association who, after March 31, 2020, were able to view the personal data of the members of the Association. (f) The reasons why the aforementioned possibility of viewing was not initially limited to the absolutely necessary persons. (g) The reasons why the Company had not installed a system to track their access in the first place. (h) The reasons why the Association could not maintain its own database, as a separate and independent controller. 1.13. On May 12, 2020, via email, Ms. Christou informed me, among other things, that: (a) The types/categories of personal data that the Association has the right to view ("view only") for its members from the intranet are the following: For active members: photo, employee number, full name, work phone number, work cell phone number, work email, department, specialty, grade and the building in which they work. For retired members: photo, employee number, full name, mobile phone number (for those who have signed a form saying they want their mobile phone to be displayed on the intranet) and specialty. (b) The Association can view the intranet data, but does not extract any data from the database. (c) The types/categories of personal data that the Union had the right to view ("view only") for its non-members were as follows: For active employees who were not members: photo, employee number, full name, work phone , work mobile phone number, work e-mail address, department, specialty, grade and the building in which he works. For retired employees who were not members: photo, employee number, full name, mobile phone number and specialty. 7 (d) The individuals/staff of the Association who were able to view the personal data until March 31, 2020, the date on which, as the Complainants have stated in their letter dated April 27, 2020, a relevant upgrade had been made of the application and the ability to view the Association's non-member information was interrupted, there were nine (9). (e) It was decided that as of May 15, 2020, only one (1) person, the General Manager, can now view it, for the purposes of better compliance with the provisions of the Regulation. 2.6. Regarding my question about the reasons why the possibility of viewing was not initially limited to the

absolutely necessary persons, the Plaintiffs replied that: "The viewing was judged to be limited to the absolutely necessary persons.". 2.7. With reference to my question about the reasons why the Company had not installed a tracking system for the access of the Union's staff in the first place, the Plaintiffs replied that: "The Tracking System was installed during the upgrade that took place on 31.3.2020 to assist the restriction carried out.". 2.8. The reasons why the Association cannot maintain its own database are economic. The implementation cost of creating its own database was estimated at approximately €450,000. 1.14. On June 3, 2020, I sent a letter to the Company and to the Union in which I concluded that there were possible violations of the provisions of articles 5(1)(a), 5(1)(b), 5(1)(c) , 5(1)(f), 5(2), 13, 14, 25 and 32 of Regulation, as well as article 33(1)(m) of Law 125(I)/2018. To this end, I asked to be informed within a specified period, for which reasons any administrative sanction should not be imposed, but also for their turnover. 1.15. On June 22, 2020 in a joint letter, both the Company and the Union cited as reasons for not imposing an administrative sanction, briefly the following: (a) Lack of due investigation: This reason was based on the decisions contained in June, 2020 , which are repeated in this decision. In particular, it was the position of the Company that the facts on which Decision 44/2019 of the Greek Authority was based, were different from the present one. In that case, it concerned the illegal copying of the personal data and all official e-mail of the employees and senior executives of the subsidiary company that was stored on the server in question (of the subsidiary), by a third person who claimed to be acting for the parent company. The case that my Office is investigating, concerns exclusively an individual complaint of an employee who is a member of the Union and who requested the Union, exceptionally, to confirm his information by himself. The ability to view the non-members that existed was practically not exercised by the authorized members, as the employees of the Union only viewed the information of their employee-members and only when it was required to serve them, a clarification given in the daily letters . 27.4.2020 and my letter dated 3 8 12.5.2020. There was no technical possibility to create copies or any other files, nor possibility to link databases and leak or lose information. The viewing was necessary because it was aimed at confirming by the Association itself the details of its members on the basis of updated information. Only 2% of the Company's employees are not members of the Union at the same time. (b) Mitigating factors: The following mitigating factors were mentioned: (1) The complainant had not made a direct complaint to the Company. (2) No damage has been caused to the complainant, who is a member of the Union. (3) The information to which the 9 members of the Association had access, was general official information of the employees that is already posted and updated on the Company's intranet and is intended to identify them and communicate with them when and if necessary. (4) It was not possible to view more information

than the absolutely necessary up-to-date service information. Viewing the photo was deemed necessary for identification purposes. (5) There was no fraud or negligence on the part of the Company or Association. (6) There has been no unlawful loss or copying or disclosure of data to unauthorized persons. The 9 members of the Association who had access were authorized by a relevant agreement. (7) There was no unauthorized access to personal data. (8) No database connection was made, nor any processing using any software. (9) No complaint has been filed in the past. 98% of the Company's employees are also members of the Union. Both the Company and the Union are dedicated to serving the Company's employees and retirees. (10) Following technical support, it was arranged to end the viewing option for the 2% of employees who were not members of the Union. Those authorized to view were reduced to 1 of the original 9. (c) Finally, it was said that the turnover of the Company, according to the published and audited financial statements of 2018, amounted to €343,559,000 (three hundred and forty-three million and five hundred and fifty-nine thousand euros). Legal Framework 2.1. Article 4 - Definitions: ("subject identifiable natural person ""personal data": any information relating to an identified or of the data"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person." . ""processing": any operation or series of operations carried out with or without the use of automated means, on personal data or 9 sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or the alteration, retrieval, retrieval of information, use, communication by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction." "'filing system': any structured set of personal data that is accessible according to specific criteria, whether that set is centralized or decentralized or distributed on a functional or geographical basis.". ""controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and manner of processing personal data; when the purposes and manner of processing thereof are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State." 2.2. Article 5 – Principles governing the processing of personal data The Regulation requires that the personal data processed be in accordance with the principles of Article 5 of the Regulation. Specifically: 2.2.1. Paragraph 1(a) of Article 5 of the Regulation provides that personal data "are processed lawfully and legitimately in a transparent manner in relation to the subject of the data (legality, objectivity and transparency)". 2.2.2. Paragraph 1(b) of Article 5 of the Regulation provides that

personal data "are collected for specified, explicit and lawful purposes and are not further processed in a manner incompatible with these purposes; further processing for archiving purposes in the public interest or scientific or historical research purposes or statistical purposes is not considered incompatible with the original purposes according to Article 89(1) ("purpose limitation"). 2.2.3. Paragraph 1(c) of Article 5 of the Regulation provides that personal data "are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"). 2.2.4. Paragraph 1(f) of Article 5 of the Regulation provides that personal data 10 the authority has highlighted "are processed in a way that guarantees the appropriate security of personal data, including their protection from unauthorized or illegal processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality")'. 2.2.5. In addition, paragraph 2 of the same article provides that: "The controller is responsible and able to demonstrate compliance with paragraph 1 ("accountability")". 2.2.6. The Regulation of "integrity and confidentiality" as a basic principle of personal data processing1 so that by applying "appropriate technical and organizational measures", unauthorized access or use of the data and the equipment used for processing is prevented (Rationale 39 of the Regulation and European Agency for Network and Information Security-ENISA2). 2.2.7. Therefore, when the processing that is to be carried out takes place in a way that does not guarantee appropriate security, it is unnecessary to examine the fulfillment of the principles provided for in Article 5(1) of the Regulation, since the processing will not be secure and therefore will is illegal. 2.2.8. According to the Decision of the Greek Personal Data Protection Authority with no. 44/2019 "The existence of appropriate policy documents, approved by the management of a (responsible or processing entity) that are applied and implemented in practice (a contrario APDPX 98/2013 par. 5), is a key criterion for proving compliance with the principle of integrity and confidentiality, to the extent that there is no other type of evidence such as the observance of an approved certification mechanism." 2.2.9. The processing of personal data in a transparent manner is an element of the principle of fair processing and is linked to the principle of accountability, giving subjects the right to exercise control over their dataholding the controllers accountable, in accordance with the Guidelines on transparency under Regulation 2016/679, dated 11.4.2018. 2.2.10. As an exception and pursuant to article 14(5)(b) of the Regulation regarding the information provided if the personal data has not been collected by the data subject, paragraphs 1-4 do not apply 1 XXXXXX, p. 219 , which states that "Security is a sine qua non for the effective protection of personal data. However, as a preliminary point, it should be pointed out that this is a necessary but not sufficient condition for the protection of data, as their protection from unauthorized access, disclosure and general use does not automatically mean

that they are the subject of legal processing". Also see The General Data Protection Regulation, new law - new obligations - new rights, Sakkoulas 2017, p. 108. 2 "Handbook on Security of Personal Data Processing", December 2017, p. 8 and "Guidelines for SMEs on the security of personal data processing", December 2016 p. 12. code of ethics or approved 11 of allowed the collection of personal data of the same article and the relevant information is not provided by the data controller since it is likely to greatly harm the achievement of the purposes of the said processing. A condition for the application of this provision in accordance with the Guidelines on transparency under Regulation 2016/679 dated 11.4.2018, (paragraph 65), recommends that the processing of said personal data complies with all the principles provided in article 5 of the Regulation, while the most important thing is that, in all circumstances, the processing of personal data is legitimate and has a legal basis. Therefore, the data controller must take the necessary measures on his own to comply with the provisions of the Regulation and at the same time has an obligation to prove his compliance to the Personal Data Protection Commissioner at any time.

2.2.11. Recital 50 of the Regulation states that "The processing of personal data for purposes other than those for which the personal data were originally collected should only be permitted if the processing is compatible with the purposes for which the personal data were originally collected . In this case, no legal basis is required separate from that of the nature of .... For to ascertain whether the purpose of the further processing is compatible with the purpose of the initial collection of the personal data, the controller, if it meets all the requirements for the lawfulness of the initial processing, should take into account, among others: any links between their purposes and the purposes of the intended further processing; the context in which they have collected the personal data, in particular the reasonable expectations of the data subject based on his relationship with the controller regarding their further use; the nature of the personal data · the consequences of the intended further processing for the data subjects; and the existence of appropriate guarantees for both a initial as well as the intended acts of further processing. Where the data subject has provided his consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to ensure, in particular, important purposes in the general public interest, the controller should be allowed processing to proceed with the further processing of personal data, regardless of the compatibility of the purposes. In any case, it should be ensured that the principles laid down in this Regulation are applied and, in particular, that the data subject is informed about these other purposes and about his rights, including the right to raise objections."

2.2.12. The Regulation adopted the principle of accountability as a compliance measure, based on which, the data controller

has an obligation to plan, implement and take the necessary measures and policies so that the processing of data is in accordance with the provisions of the Regulation. 12 In addition, the controller is burdened with the further duty to prove by himself and at all times his compliance with the principles of article 5(1) of the Regulation. The Regulation therefore shifts the "burden of proof" as to the legality of the processing (including compliance with the principles) to the controller. 2.2.13. Opinion no. is also a useful tool. 3/2010 of the Article 29 Working Group, regarding the principle of accountability, dated 13.7.2010, for the international standards approved in Madrid by the competent authorities for the protection of personal data. According to the said Opinion, the Working Group recommended that appropriate accountability measures for compliance with the principles of Article 5(1) of the Regulation may include establishment of internal procedures before the creation of new processing operations, establishment of written and binding data protection policies available in data subjects, process mapping, maintaining a list of all data processing operations, appointing a data protection officer and other persons with responsibility for data protection, providing appropriate education and training to data protection employees, establishing procedures for managing access, rectification and erasure requests, which must be transparent to data subjects, establishing an internal complaint handling mechanism, establishing internal procedures for the effective management and reporting of security breaches, privacy impact assessment in specific cases, implementation and monitoring of verification procedures to ensure that all measures are not only on paper, but implemented and working in practice (internal or external audits, etc.). 2.3. Article 6 – Legality of processing 2.3.1. According to the provisions of article 6 of the Regulation, regarding the legality of the processing: "1. The processing is lawful only if and as long as at least one of the following conditions applies: a) the data subject has consented to the processing of his personal data for one or more specific purposes, b) the processing is necessary for the performance of a contract whose the data subject is a contracting party or to take measures at the request of the data subject prior to the conclusion of a contract, c) the processing is necessary to comply with a legal obligation of the controller, d) the processing is necessary to preserve vital interest of the data subject or other natural person, 13 e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of public authority delegated to the controller, f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that require the protection of personal data, in particular if the data subject is a child. Item f) of the first paragraph does not apply to the processing carried out by public authorities in the exercise of their duties. 2. Member States may maintain or adopt more

specific provisions to adapt the application of the rules of this Regulation regarding processing to comply with paragraph 1 points c) and e), specifying more precisely specific requirements for processing and other measures to ensure legal and legitimate processing, including for other special cases of processing as provided for in chapter IX. 3. The basis for the processing referred to in paragraph 1 items c) and e) is defined in accordance with: a) Union law , or b) the law of the Member State to which the controller is subject. The purpose of the processing is determined on that legal basis or, with regard to the processing referred to in paragraph 1 point e), is the necessity of the processing for the performance of a task performed in the public interest or in the exercise of a public authority vested in the person in charge processing. This legal basis may include specific provisions to adapt the application of the rules of this regulation, among others: the general conditions governing the lawful processing by the data controller; the types of data processed; the relevant subjects of of data; the entities to which the personal data may be communicated and the purposes of such communication; the limitation of the purpose; the storage periods; and the processing operations and processing procedures, including measures to ensure lawful and legitimate processing, such as those for other special cases of processing as provided for in chapter IX. Union law or Member State law responds to a public interest purpose and is proportionate to the intended legal purpose. 4. When the processing for a purpose other than that for which the personal data have been collected is not based on the consent of the data subject or on Union law or the law of a Member State which is a necessary and proportionate measure in a democratic society for the ensuring the purposes referred to in article 23 paragraph 1, the controller, in order to verify whether the processing for 14 of the purposes the existence of appropriate guarantees, which may include another purpose is compatible with the purpose for which the personal data is initially collected nature, takes into account, among others: a) any relationship between the purposes for which the personal data have been collected and the intended further processing, b) the context in which the personal data were collected, in particular with regard to the relationship between data subjects and the controller, c) the nature of the data of a personal nature, in particular for the special categories of personal data processed, in accordance with Article 9, or whether personal data related to criminal convictions and offenses are processed, in accordance with Article 10, d) the possible consequences of the intended further processing for the data subjects, e) encryption or pseudonymization.". 2.3.2. Recital 44 of the Regulation states the following in relation to Article 6(1)(b) of the Regulation: "The processing should also be lawful if it is necessary in the context of a contract or intention to conclude.". 2.3.3. With reference to Article 6(4) of the Regulation, recital 50 of the Regulation adds that: "The processing of personal data for purposes other than those for which the personal data

were originally collected should only be allowed if the processing is compatible with the purposes for which the personal data was originally collected. In this case, a legal basis separate from that which allowed the collection of the personal data is not required.

.... The legal basis provided by Union or Member State law for the processing of personal data may also constitute the legal basis for further processing. In order to ascertain whether the purpose of the further processing is compatible with the purpose of the initial collection of the personal data, the controller, if it meets all the requirements for the lawfulness of the initial processing, should take into account, among others: any links between of these purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of the data subject based on his relationship with the controller regarding their further use; the nature of the personal data character; the consequences of the intended further processing for the data subjects; and the existence of appropriate safeguards for both the initial and intended further processing operations. Where the data subject has provided his consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure 15 in a democratic society to ensure, in particular, important purposes in the general public interest, it should be allowed to responsible processor to proceed with the further processing of personal data, regardless of the compatibility of the purposes. In any case, it should be ensured that the principles laid down in this Regulation are applied and, in particular, that the data subject is informed about these other purposes and about his rights, including the right to raise objections." 2.4. Articles 13 and 14 – Information provided if the personal data is collected from the data subject and Information provided if the personal data is not collected from the data subject (informing the data subjects) 2.4.1. According to recital 39 of the Regulation: "Every processing of personal data should be lawful and fair. It should be clear to natural persons that personal data concerning them is collected, used, taken into account or otherwise processed, as well as to what extent the personal data is or will be processed. This principle requires that all information and notices regarding the processing of such personal data be easily accessible and understandable and use clear and plain language. This principle concerns in particular the information of data subjects about the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in relation to the natural persons in question and their right to receive confirmation and to achieve communication of the personal data related to them that are subject to processing. Natural persons should be informed of the existence of risks, rules, guarantees and rights in relation to the processing of personal data

and how to exercise their rights in relation to this processing. In particular, the specific purposes of the processing of personal data should be clear, lawful and determined at the time of collection of the personal data. Personal data should be sufficient and relevant and limited to what is necessary for the purposes of their processing. This requires in particular to ensure that the period of storage of personal data is limited to the minimum possible.... Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including for to prevent any unauthorized access to such personal data and the equipment used to process it or the use of such personal data and said equipment.". 2.4.2. Recital 60 of the Regulation states the following: "The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure 16 fair and transparent processing taking into account the specific circumstances and the context in which the processing of personal data takes place". 2.4.3. Regarding the information of the data subjects, recital 61 of the Regulation adds that "Information in relation to the processing of personal data relating to the data subject should be provided to him at the time of collection by the data subject or , if the personal data is obtained from another source, within a reasonable time, depending on the circumstances of each case. If the personal data is allowed to be disclosed to another recipient, the data subject should be informed when the personal data is first disclosed to the recipient.....'. 2.5. Article 24 – Responsibility of the controller "1. Taking into account the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity to the rights and freedoms of natural persons, the controller implements appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with this regulation. These measures are reviewed and updated when deemed necessary. 2. When justified in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate policies for the protection of data by the controller." 2.6. Article 32 – Processing security 2.6.1. The obligations of the controller regarding the security of the processing are explicitly defined in article 32 of the Regulation, which provides that "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, where appropriate:" "b) the ability to ensure the privacy, integrity, availability and reliability of systems and services processing on a

continuous basis, c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical incident, 17 the regular testing, personal data assessment and evaluation of the d) process for technical and organizational effectiveness measures for d ensuring the security of processing.". 2.6.2. In paragraph 2 of the same article, it is stated that: "When assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access transmitted, stored or otherwise processed'. 2.6.3. According to the last paragraph of recital 39 of the Regulation: "Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to this data personal data and the equipment used to process them or the use of such personal data and said equipment." 2.6.4. Recital 74 of the Regulation states that: "Responsibility and obligation to indemnify the data controller should be established for any processing of personal data carried out by the data controller or on behalf of the data controller. In particular, the controller should be required to implement appropriate and effective measures and be able to demonstrate the compliance of the processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, context, scope and purposes of the processing and the risk to the rights and freedoms of natural persons." 2.6.5. According to Rationale 78 of the Regulation “The protection of the rights and freedoms of natural persons against the processing of personal data requires the adoption of appropriate technical and organizational measures to ensure that the requirements of this regulation are met. In order to be able to demonstrate compliance with this regulation, the data controller should establish internal policies and implement measures which respond in particular to the principles of data protection by design and by default.' 2.6.6. With reference to Article 32 of the Regulation, recital 83 of the Regulation adds that: "To maintain security and avoid processing in violation of this Regulation, the controller or processor should assess the risks involved the processing and implement measures to mitigate such risks, such as through encryption. These measures should ensure an appropriate level of security, which includes confidentiality... When assessing the risk to data security, attention should be paid to the 18 risks arising from the processing of personal data... ». 2.6.7. Additionally, Rationale 87 of the Regulation provides that "It should be ascertained whether all appropriate technological protection measures and organizational measures have been put in place for the immediate detection of any breach of personal data and the immediate notification of the supervisory authority and the subject of the data", as detailed in the Article 29 Working Group Guidelines of 02-06-2018, dated 02.06.2018, regarding the notification of a data breach. 2.6.8. According to Decision number 186/2014 of

the Hellenic Personal Data Protection Authority in part "D. Security measures – Technical measures of separation of applications", an essential element of the legal operation of information systems and other infrastructures when processing personal data is the taking of appropriate security measures, in particular measures of physical and logical separation of hardware, software and data. Here is a relevant excerpt: "Logical separation exists when software, at all levels, used to access personal data held to satisfy a particular purpose is distinct and logically isolated from software used to access data held for others aims. This without requiring the physical infrastructure used for the processing of personal data for a specific purpose to be physically separated from the rest of the data...". 2.7. Decisions 2.7.1. By Decision dated 17.7.2009 (appeal no. 20511/2003, paras. 37 - 46), the European Court of Human Rights in the case of I. v. Finland, examined whether the data controller ensured the security of personal data and found a violation of article 8 of the European Convention on Human Rights, from the non-application of security measures that led to unauthorized access to them. 2.7.2. A useful reference can also be made to the following excerpts from the Greek Personal Data Protection Authority: Decision No. 98/2013 "First of all, security is specialized in three main objectives, i.e. confidentiality, integrity, while complementary objectives, especially from the point of view of personal data protection, are in particular the non-disclaimer of responsibility (or accountability) as well as the separation of data accordingly with the purpose of processing. According to the internationally accepted information system security standards (e.g. see ISO/IEC 27000 series) the appropriate measures according to article 10 par. 3 of Law 2472/1997 are part of an Information Systems Security System (ISMS). The availability of data, of and 19 due System presupposes the preparation of a risk study based on the risks and the nature of the data, and among other things includes the preparation of security policy and plans, where specific technical and organizational measures are identified. These measures, in addition to having to be applied, are also monitored and evaluated with the aim of their continuous adaptation to the operational needs of the data controller and to technological developments, which the data controller must take into account (see article 17 par. 1 Directive 95/46/EC).' Decision No. 44/2019 "In view of the above, the Authority considers that the audited company AMRNI as a data controller: On the one hand, it did not apply all the principles of article 5 para. 1 GDPR (General Data Protection Regulation) and 6 para. 1 GDPR regarding the legality of the processing of personal data …… which took place in the used computing infrastructure …… but also in the context of any subsequent or further processing of the same personal data, nor did it prove by no. 5 para. 2 GDPR the observance thereof. On the other hand, he violated the provisions of articles 5 par. 1 sec. a' and f' and par. 2 in conjunction with articles 24 par. 1 and 2 and 32 par. 1 and 2 GDPR regarding the principle of secure

processing (in particular "confidentiality") of personal data that took place in used computing infrastructure …… from not taking appropriate technical and organizational measures, but also in the context of any subsequent or further processing of the same personal data, so that the examination of compliance with the processing principles of subsections b', c', d' is omitted and e' of par. 1 of article 5 as well asof article 6 par. 1 GDPR...". 3. Rationale 3.1. Definitions 3.1.1. The data held by the Complaining Defendants and relating to a living person constitute "personal data". 3.1.2. Access (such as the viewing/viewing of data), use, search, and association/combination of personal data held in a database constitute data processing that is personal data, within the meaning of Article 4(2) of the Regulation. confirmation/check 3.1.3. The automated system that operates and is used by the Company "filing system" based on the definition in article 4(6) of the Regulation. and concerns its employees, recommends 3.1.4. Controllers are the Company and the Association (Article 4(7) of the Regulation) and they are two separate controllers. 3.1.5. Data subjects are the Company's employees who are not members of the Union and the Company's employees who are members of the Union (article 4(1) of the Regulation). 3.2. Processing principles 20 3.2.1. In order for personal data to be lawfully processed, the conditions for compliance with the principles governing the processing of personal data (Article 5 of the Regulation) must be cumulatively met, as also emerges from the decision of the Court of the European Union dated 16.01.2019 in case C-496/2017 XXXXXX3. According to the aforementioned Decision, the existence of a legal basis (Article 6(1) of the Regulation) does not exempt the data controller from the obligation to comply with the principles (Article 5 of the Regulation). 3.2.2. As XXXXX, Lawyer, Member of the Personal Data Protection Authority and Member of the Expert Group of the E.U. for Regulation 2016/679 and Directive 2016/680: "Cumulative fulfillment of conditions for application and observance of principles no. 5 par. 1 and 6 GDPR (General Data Protection Regulation) The existence of a legal basis (no. 6 par. 1 GDPR does not exempts the Deputy Director (processor) from the obligation to comply with the principles of Article 5 paragraph 1 of the GDPR. Illegal collection and processing in violation of the principles of Article 5 of the GDPR is not cured by the existence of a legitimate purpose. If it is violated one of the principles of article 5 par.1 GDPR (e.g. legitimate and legal processing, security) does not consider the other principles or article 6 par.1 GDPR."4 3.2.3. In addition, the data controller is burdened with the further duty to prove at all times its compliance with the principles governing the processing of personal data, as set out in Article 5 of the Regulation. Specifically, accountability is included in the principles governing the processing of personal data and in essence shifts to the controller processor gas "burden of proof" of the legality of the processing. 3.2.4. In addition, the Court of Justice of the European Union in Decision C-201/14 (XXXXXX), dated 01.10.2015,

considered as a condition for the legitimate and legal processing of personal data the information of the subject of the data before the processing thereof. 3"57. However, any processing of personal data must comply, on the one hand, with the principles to be observed in terms of data quality, which are set out in Article 6 of Directive 95/46 or Article 5 of Regulation 2016/679 and, on the other hand , to the basic principles of lawful data processing listed in Article 7 of this Directive or Article 6 of this Regulation (Related decisions ... C-465/00, C-138/01, C-139/01, C- 131/12". 4 See Decision 517/2018 of the Council of the Territory of the Hellenic Republic, paragraph 12 "...in order for personal data to be lawfully processed, it is required in any case that the conditions of article 4 par. 1 of n . 2472/1997 (legal collection and expl data processing for clear and legitimate purposes), it is further examined whether the conditions of the provision of article 5 par. 2 of Law 2472/1997 [legal bases] are also met. 21 Here are relevant excerpts: "The data controller or his representative is subject to an obligation to inform, the content of which is defined in articles 10 and 11 of Directive 95/46 and differs depending on whether the data is collected by the person to whom the data or not, subject to the exceptions provided for in Article 13 of the Directive in question." "Consequently, the requirement for lawful data processing provided for in Article 6 of Directive 95/46 obliges the administrative authority to inform the data subjects of the transmission of said data to another administrative authority for the purpose of processing them from the latter as the recipient of said data". 3.3. Articles 13 and 14 – Information provided if the personal data is collected from the data subject and Information provided if the personal data is not collected from the data subject (information of the data subjects) Complainants should to inform the members of the Association that the Association would have access to more personal data concerning them (photo) than was necessary to confirm their information. In addition, they had to inform the Company's employees that the Union would have access to personal data concerning them. 3.4. Responsibility of the controller (Article 24 of the Regulation), data protection by design and by definition (Article 25 of the Regulation) and security of processing (Article 32 of the Regulation) 3.4.1. The Plaintiffs, in the framework of the implementation of the Regulation, had to comply with their obligations regarding security and their general responsibility for the determination of appropriate technical and organizational measures, taking appropriate measures, which can be documented in individual procedures or in more general security policies5. 3.4.2. Such appropriate technical and organizational measures for the security of personal data processing within the framework of the Regulation are also proposed by the European Agency for Network and Information Security (ENISA). 3.4.3. Additionally, before determining the security measures that were to be adopted, the Defendants should have assessed the risks and their possible consequences for the data subjects6. 5 See

website of the Hellenic Personal Data Protection Authority www.dpa.gr, Section Security and in particular "Security Policy, Security Plan and Disaster Recovery Plan"). 6 See XXXXX, specialist scientist of the Hellenic Personal Data Protection Authority, "Processing security and breach notification" in Report of the National Center for Public Administration and Self-Government "GDPR: the new landscape and the obligations of the public administration", Athens, January 2018, p. 20 (www.ekdd.gr/images/seminaria/GDPR.pdf). 22 3.4.4. From the letter and the purpose of the provisions of recital 83 of the Regulation, it is clear that the obligation to observe the security of the processing by the processor is both preventive and repressive in nature. Preventive, so that applicable measures can prevent incidents of security breaches and repressive, so that any incident can be detected and investigated. 3.4.5. Also, the implemented measures should be reviewed and updated, as provided for in Article 24(1) of the Regulation. 4. Conclusions In the case under consideration, from the data in the case file, I am of the opinion that: 4.1. The Company did not take the necessary technical and organizational measures, especially those that mandate physical and logical separation, as a result of which the Association: □ □ Until March 31, 2020, had access to view/view personal data of data subjects that were not linked to the Association (non-members) and had access to more personal data of its members (photograph) than is necessary to carry out the required processing (confirmation of personal data of members), but also than was agreed with the Agreement dated October 15th between them, 2018. Therefore□ □ persor data of members of the Association were further processed against processing, violating the principle of purpose limitation (Article 5(1)(b) of the Regulation), in a way incompatible with the original purpose □ personal data of non-members of the Association continued until 31.3.2020, to be further processed in a manner incompatible with the original purpose of of processing, violating it principle of purpose limitation (article 5(1)(b) of the Regulation), (in the form of viewing/projection) the Association has access to more personal data concerning its members (photo), which, however, is not necessary for the confirmation of their details, in violation of the principle of minimization (article 5(1)(c) of the Regulation), □ □ The Union had access to personal data of employees of the Company who were not its members, in violation of the principle of minimization (article 5 (1)(c) of the Regulation), □ personal data of the Company's employees who are not members of the Union, were processed in a way that does not guarantee their appropriate security, including their protection from unauthorized or illegal access and thus the threatened 23 risk to their confidentiality occurred, violating the principle of integrity and confidentiality (Article 5(1)(f) of the Regulation). □ The same applies to the personal data of members of the Association, to which the Association still has access (photo). On June 22, 2019, it was reported that they consider the photo necessary for the purpose

of identification and communication with the data subjects. This position is not consistent with the position they put forward on April 27, 2020, that is, the application allowed the authorized persons of the Union access for purposes of confirmation, that the employee with the number they registered is a member of the Union. In addition to the fact that this data is deemed disproportionate, it is also data whose granting of access was not agreed upon in the Agreement between the Company and the Union, dated October 15, 2018. In any case, the purposes for which access was granted to the Union, would be satisfied even if there was no access to the employee's photograph. 4.2. Therefore, the processing carried out by the Complaining Defendants was unlawful since the principles of purpose limitation, minimization and data integrity and confidentiality were not respected. 4.3. In view of the above, given that, in the case under consideration, the processing of personal data is already judged to be illegal and in violation of the provisions of article 5(1) of the Regulation in combination with articles 24(1) – (2), 25(1)) – (2) and 32 (1) – (2), the examination of the legal purpose and legal basis of the processing is omitted. 4.4. The Plaintiffs, before determining the security measures that were to be adopted, did not assess the risks and their possible consequences on the rights and freedoms of the data subjects, as provided by articles 25 and 32 of the Regulation. 4.5. The Defendants of the complaint did not prepare any plan for the purpose of implementing and monitoring such measures to observe the security of the processing in order to identify any weaknesses/gaps. As a result, the Union had access to more data than was needed to confirm the details of its members (photo) and at the same time had access to data of non-members. 4.6. The Plaintiffs did not implement the appropriate technical and organizational security measures to ensure that, by definition, only the personal data that was necessary for the purpose of the processing is processed. As expressly stated in Article 25(2) of the Regulation, this obligation of the Complainant applies to the scope of the data collected, the degree of their processing, the storage period and their accessibility. In this case, the implemented measures did not ensure that, by definition, personal data could only be processed by authorized persons, respecting the principles set out in Article 5 of the Regulation. 4.7. Therefore, from the above, I find that the Company 24 4.7.1. From the outset, it did not adopt/implement in the correct and appropriate manner the appropriate organizational and technical security measures to ensure that, by definition, only the data necessary for the purpose of the processing it performs are processed (Article 25 of the Regulation), 4.7 .2. during the execution of the processing, did not implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks (Article 32 of the Regulation) and 4.7.3. did not proceed with the review/update of the existing security measures to identify any weaknesses/gaps (Article 24 of the Regulation), only after the

investigation process of this complaint began, where it was decided to end the possibility of viewing the data of 2% of non-members of the Association, from 31.3.2020 onwards, with subsequent: The provision of access to the Association to personal data of non-members until 31.3.2020, as well as to more personal data (photograph) related to its members which were not necessary for the realization of the required purpose of the processing (i.e. the confirmation of the details of its members), violating the principles of purpose limitation, minimization and integrity and confidentiality of data (Article 5 of the Regulation). Additionally, the Company 4.7.4. It did not design, prepare and implement, in compliance with the provisions of Article 5(1) of the Regulation, any measure of accountability, as provided for in Article 5(2) of the Regulation, including personal data security policies, nor did it take measures to physically separate the data (i.e. different database) or logical separation of data (i.e. the types/categories of personal data to which access is granted). 4.7.5. Also, the Company did not provide my Office with any evidence that: (a) it informed the members of the Association that the Association would have access to more of their personal data than was necessary to confirm their information, as provided in Articles 13 and 14 of Regulation, (b) informed its employees that the Union, as a separate controller, would have access to their personal data, as provided for in articles 13 and 14 of the Regulation. 4.8. In addition, from the above, I find that the Association: 4.8.1. From the outset, it did not adopt/apply in the correct and appropriate manner the appropriate organizational and technical security measures to ensure that, by definition, only the data necessary for the purpose of the processing it performs are processed (Article 25 of the Regulation), 25 4.8.2. during the execution of the processing, did not apply appropriate technical and organizational measures in order to ensure the appropriate level of security against risks (Article 32 of the Regulation) and 4.8.3. did not proceed with the review/update of the existing security measures to identify any weaknesses/gaps (Article 24 of the Regulation), only after the investigation process of this complaint began, where it was decided to end the possibility of viewing the data of 2% of non-members of the Association, from 31.3.2020 onwards, with subsequent access from the Company's database to personal data of non-members until 31.3.2020, as well as to more personal data concerning its members (photo), which was not necessary for the realization of the required purpose of the processing (i.e. the confirmation of the data of its members), violating the principles of purpose limitation, minimization and integrity and confidentiality of data (Article 5 of the Regulation). In addition, the Association: 4.8.4. Did not design, prepare and implement, in compliance with the provisions of article 5(1) of the Regulation, any measure of accountability, as provided for in article 5(2) of the Regulation, including personal data security policies specifically related to the existence/maintenance of a separate database from the

Company's database. 4.8.5. It did not provide my Office with any evidence that (a) informed its members that it will have access to more of their personal data than is necessary to confirm their details, as provided for in Articles 13 and 14 of the Regulation, (b) informed the employees of the Company that he would have access to personal data concerning them, as provided for in articles 13 and 14 of the Regulation. 4.9. While the Company granted access to its database to the Association, in violation of the current legislative framework, as I detail in paragraphs 4.7.- 4.8.5. above, I was never informed by the Defendants of the complaint about carrying out/carrying out such processing nor did they voluntarily stop it, except when I sent them a relevant letter on February 25, 2020, after I received a written complaint from an employee of the Company and a member of the Union . 4.10. The Company's claim that, the reason the Association cannot maintain its own database, as a separate controller (paragraph 2.8. of the Company's response, which was sent to my Office by email on 12.05.2020), is not correct, nor does it have any legal force, taking into account the provisions of articles 25(1) and 32(1) of the Regulation which define the following 26 Article 25(1) "Taking into account the latest developments, the costs of implementation and the nature scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons from processing, the controller effectively implements, both at the time of determining the means of processing and at the time of processing, appropriate technical and organizational measures, such as pseudonymization, designed to implement data protection principles , such as the minimization of data, and the incorporation of the necessary guarantees in the processing in such a way as to meet the requirements of the relevant regulation and to protect the rights of the data subjects.". Article 32(1) "Taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity to the rights and freedoms of natural persons , the controller and the processor implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks,...." 4.11. From the above, taking and implementing the appropriate organizational and technical security measures, both at the time of determining the means of processing and at the time of the processing, does NOT negate the cost of implementing the processing. On the contrary, based on articles 25 and 32 of the Regulation, the data controller has an obligation to take the appropriate organizational and technical measures already from planning at the time of determining the means of processing as well as at the time of processing. The fulfillment of these obligations constitutes a useful tool for its legal compliance as the design of procedures and systems from the outset with the philosophy of personal data protection will lead to the effective diagnosis and treatment

of problems at an initial level and therefore, reduce the possibility of risks from the processing. 4.12. The legal basis on which the Association relied to process personal data of non-members and to process more personal data concerning its members, are the provisions of article 6(1)(a) and (b) of the Regulation, as in this regard, the Defendants mention the complaint in their letters dated March 27, 2020, April 27, 2020 and May 12, 2020. 4.12.1. I should note that, in principle, the Defendants of the complaint did not provide any evidence/testimony demonstrating that the members of the Association had consented/agreed to the processing of more personal data concerning them than is necessary to confirm their information by the Association, nor did they provide any proof/testimony that they had consented/submitted to the processing of their personal data by the Association. 4.12.2. The "Request for Membership Registration" Form attached to the Defendants' response to the complaint to my Office, dated May 12, shows that, non-members of 27 2020, it is NOT consent of members to process their personal data, how much rather for the processing of more personal data than is needed (photograph) by the Union, as the Plaintiffs falsely claim in their letter. This form is entitled "Application for Membership Registration", according to which the contractual employee signs "application for registration as a member of the Union" and gives consent to have the monthly subscription determined by the Board of Directors deducted from his salary of the Association. Next, there is a space for filling in "requester details", which in any case are not compatible with the details for which an agreement was concluded between the Company and the Union for exchange. In any case, however, the specific document cannot be considered to constitute consent for data processing in the sense that the Defendants support the Complaint, since the provisions required by the Regulation, in relation to the provision of said information, are not met from the data subject (information and free express consent for specific processing). 4.12.3. Additionally, the provisions of article 6(1)(b) of the Regulation do not apply since the non-members of the Union did not have any contract with the Union. As for the members of the Association, they had a contract with two separate processors who served two different processing purposes. 4.12.4. In any case, I emphasize that, even in the event of the existence of a legal basis for the processing in question, given that, from the outset, the processing carried out by the Defendants in the complaint violated the principles of processing, as set out in articles 5(1)(a)), (b), (c) and (f) of the Regulation, the processing becomes illegal and the examination of the legal basis of the processing is omitted. 4.13. The conclusion of the Agreement dated October 15, 2018, between the Company and the Association for the exchange of personal data, does not have any legal force, since the processing carried out is illegal from the beginning. 4.14. The Company admitted the illegal processing in question since 4.14.1. XXXXX, with her letter No. Fac.: LGLK10-426 and dated March 27, 2020, told

me, among other things, the following (a) The Association maintains an electronic file with the Register of Fund Members, which is updated by pulling information from the Company's Personnel Services database automatically electronically. (b) The Register of Members of the Association includes the following data of employees and pensioners of the Company, which it automatically draws from the electronic database of the Company Employee number Gender Full name Photograph birth 28 Date of employment Date of death (where applicable) Date of retirement Mailing address Business telephon (where available) Landline (where available) Mobile telephone (where available) Email address Associated employee number Status widow/widower, dependent child (c) Additionally, the staff of the Union has access to the following personal data of the Company's employees who are not members of the Union Employee number Employee name Business pho (where available) Mobile phone (where available) Email address (where available available) Rank and specialty in the service Address of work let (d) Access to the above data is ensured by automatic connection of the official computers of the Union's staff with the official Intranet Portal of the Company. 4.14.2. XXXX, in an email dated 27.04.2020, stated that "The possibility to view the information of non-members of TEY-ATIK has been suspended from 31.03.2020, with a relevant upgrade of the application.". 4.15. While a simple upgrade of the application stopped the Association's access to viewing/viewing the personal data of non-members of the Association, something that should have been done in the first place, however the common database remains, violating the provisions of the Regulation, as I describe in detail in paragraphs 4.1. – 4.9. above. 4.16 With reference to the reason presented in the letter of the Defendants, the complaint dated June 22, 2020 for lack of due investigation, to state that this reason cannot be based on any reference to a passage in a previous relevant decision, but whether an Authority has carried out due investigation in relation to the incidents of the case under investigation , like the present one. Therefore, my reference to a passage of Decision 44/19 of the Greek Authority cannot justify a lack of due investigation. The reference was made mainly to demonstrate that a data controller must take appropriate technical and organizational measures to protect the personal data it holds (Article 32), but also to apply the general principles governing the processing of personal data (Article 5) and legality (Article 6 of the GDPR). In relation to the fact that there was no technical possibility to create copies of the data, I should mention that this does not justify any possibility of viewing the data, since they did not serve the specific purpose for which access was granted. If someone wishes to abuse the viewing facility, there are other 29 ways to do so besides electronically copying the data, such ase.g. photograph or simple handwritten copy. It is also not an excuse how

only 2% of the Company's employees are not members of the Union. One and only

individual's rights to be affected, is enough to conclude that it exists

violation of the Regulation, let alone 2%, in an organization of its size

of the specific Company.

5. Penalties

5.1.1. As defined in the provisions of article 83(5) of the Regulation, violation

of the provisions of articles 5, 13 and 14, entails, "according to paragraph 2,

administrative fines up to EUR 20 000 000 or, in the case of businesses, up to 4%

of the total global annual turnover of the previous financial year

year, whichever is higher."

5.1.2. As defined in the provisions of article 83(4) of the Regulation, violation

of the provisions of articles 25 and 32, draws, "according to paragraph 2,

administrative fines up to EUR 10 000 000 or, in the case of businesses, up to 2%

of the total global annual turnover of the previous financial year

year, whichever is higher."

5.1.3. Paragraph 2 of article 83 of the Regulation is quoted in its entirety:

"2. Administrative fines, depending on the circumstances of each individual

case, are imposed in addition to or instead of the measures referred to in

article 58 paragraph 2 items a) to h) and in article 58 paragraph 2

item j). When deciding on the imposition of an administrative fine,

as well as regarding the amount of the administrative fine for each individual

case, due consideration shall be given to the following:

a) the nature, gravity and duration of the infringement, taking into account the nature,

the extent or purpose of the relevant processing, as well as the number of

of data subjects affected by the breach and the degree of damage that

suffered,

b) the fraud or negligence that caused the breach,

c) any actions taken by the data controller or the

performing the processing to mitigate the damage suffered by the subjects

of the data,

d) the degree of responsibility of the controller or the person performing the

processing, taking into account the technical and organizational measures they apply

by virtue of Articles 25 and 32,

e) any relevant previous violations of the controller or

processor,

f) the degree of cooperation with the control authority to remedy the violation

and the limitation of its possible adverse effects,

g) the categories of personal data affected by the breach,

h) the way in which the supervisory authority was informed of the violation,

in particular if and to what extent the data controller or the person performing it

processing reported the violation,

i) in case it was previously ordered to take the measures that

referred to in Article 58 paragraph 2 against the person responsible

of processing or of the processor regarding the same object, h

compliance with said measures,

j) the observance of approved codes of conduct in accordance with article 40 or

of approved certification mechanisms in accordance with Article 42 and

k) any other aggravating or mitigating factor resulting from

circumstances of the particular case, such as the financial benefits which

were obtained or damages avoided, directly or indirectly, by

violation.".

6. Measurement of penalty

6.1. Taking into account the provisions of article 83 of the Regulation, which concerns in the General Conditions for the imposition of administrative fines, when measuring it administrative fine I took into account the following mitigating factors (1-3) and aggravating (4-7) factors:

(1) The position of the Defendants in the complaint, that there was no fraud or negligence on the part of the Association or the Company.

(2) The cooperation that existed with my Office, in relation to the redress of the violation and the limitation of its possible adverse effects, since during the examination of the specific complaint, the Company has proceeded in a technological upgrade according to which: (a) from 31.3.2020 no there is now access to the data of non-members of the Association, (b) has restrict access to the Association, from nine people who were previously, to an individual, and (c) set up a tracking system.

(3) In relation to the degree of responsibility of the data controller, I consider that responsibility lies more with the Company, which provided access to Union, in data which did not belong to its members.

(4) The extent of the violation, which is not limited to complainant, but also concerns 2% of the Company's employees, who do not were members of the Association.

(5) The fact that, according to the position they continue to the Defendants support the complaint, namely that the photo is theirs necessary for identification and communication purposes, indicates intent not to compliance, so far, with my suggestions, that it is disproportionate access this item.

(6) The fact that the violation came to my knowledge, from the subject of

data and not by the data controller.

(7) I do not accept the position of the Defendants as the complaint does not seem to have

cause any harm to the complainant. The offense, no

it is limited only to her, but it also concerns 2% of the rest of those affected

31

employees of the Company, to whose data the Union had access. THE

Company had not carried out a risk assessment taking sufficient technical

and organizational measures in place to segregate access to member data

and non-members of the Association.

6.2. Bearing in mind all the above, with the main factor being the fact that

TEY-ATIK does not have access from 31.3.2020 to data of non-members,

I decide not to impose an administrative fine at this stage.

6.3. However, an order is given, in accordance with the powers granted to me by the Article

58(2)(d) of GDPR 2016/679, to ATIK, as it adopts such measures

security and practices, so that TEY-ATIK no longer has access to

data disproportionate to what serves the purpose, excluding access

towards it in the photo of its members.

6.4 The ATHIK is also mandated, as within two months from today, with

inform about the actions taken to comply with the

this Decision.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

32