Athens, 03-06-2021 Prot. No.: G/EX/1364 DECISION 23/2021 (Department) The Personal Data Protection Authority (hereinafter "the Authority") met as a Department via teleconference on 02-17-2021 and at 10:00 a.m., upon the invitation of its President, in order to examine the case referred to in the present history. Georgios Batzalexis, Deputy President, in the absence of the President of the Authority Konstantinos Menoudakos, and the alternate members Grigorios Tsolias, as rapporteur and Evangelos Papakonstantinou, in place of the regular members Charalambos Anthopoulos and Konstantinos Lambrinoudakis respectively, who, although legally summoned in writing, were present attended due to disability. Regular member Spyridon Vlachopoulos, although legally summoned in writing, did not attend due to disability. The meeting was attended by order of the President, Efrosyne Siougle, special scientist - examiner as assistant rapporteur, who left after the discussion of the case and before the conference and decision-making, and Irini Papageorgopoulou, an employee of the administrative affairs department of Authority, as secretary. The Authority took into account the following: Complaint No. C/EIS/5650/13-08-2019 by A and Complaint No. C/EIS/5910/30-08 were submitted to the Authority -2019 complaint, as supplemented by the document No. C/EIS/5912/30-08-2019 from B, with which the complainants complain that their former employer company with the name PURPLE SEA MONOPROSOPI IKE (hereinafter "the company") 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr monitors and controls employees through the video surveillance system. In particular, the first of the complainants complains about the following, briefly mentioned: installation of cameras without any information to the employees, monitoring of the employees on a permanent basis, that he was given an inappropriate recommendation in a strict style by the Personnel Manager for the way they sat observing him unaware of the cameras, that one morning it was suddenly announced to the workers that they were being secretly watched by the cameras and found that they were fiddling with their mobile phones and were asked to hand over their personal mobile phones to the Manager ... C although these are personal property belonging to of workers without whom they would not be able to communicate with the outside world as well as that there was a spirit of intimidation and verbal warnings after implied threats-retaliation that everything is controlled and recorded by the video surveillance system so that workers better be careful what they say and what they do in working time . The second complainant also complains about the same issues as above, in addition to the recommendation made to the first complainant. The complainants requested that the above two complaints be considered together as they are directed against the same company for the same issue. The Authority, with its document No. C/EX/5650-1/24-09-2019, forwarded to the complained company copies of the above complaints, briefly informed it about the

conditions for legal processing of personal data through a system video surveillance and requested the provision of its written opinions on the accused. Since the Authority did not receive a response, it sent the complained company the reminder No. C/EX/461/20-01-2020. Since no response was received, the Authority sent a new reminder to the complained company with the 24-6-2020 e-mail message. The complained-about company replied, with document No. G/EIS/5388/31-07-2020, the following: 2 It is located on the 4th floor of the apartment building on Messolonghiou Street no. 40 A in Piraeus, where it maintains its offices. It is an apartment building where exclusively business premises are housed. Following a unanimous decision of the General Assembly of the tenants of the apartment building, it was decided to install a video doorbell at the main entrance of the apartment building for security reasons to control the central door of the building and communicate with visitors. It is a camera that oversees the absolutely necessary area of the central entrance of the apartment building, which only works when the call button is pressed and without absolutely any image or sound recording. Following a unanimous decision of the General Assembly of the tenants of the apartment building, it was decided to install a video surveillance system around the perimeter of the building for security reasons. According to the technical report of D, a technician of the company SECURITY G&T SYSTEMS – INSTALLATION OF SECURITY SYSTEMS, these are analog type cameras, with a detection angle of 90°, color recording without sound. These cameras do not receive an image from side streets and sidewalks and do not transmit a signal to private offices. Following a unanimous decision of the General Assembly of tenants of the apartment building, it was decided to install a video surveillance system in the common areas, specifically in the following areas: stairwell/stairs/storage areas/underground parking for security reasons. There is no employee working in any of these areas. The cameras have the same features as above and do not record sound. Data is kept for a maximum of 14 days and then deleted automatically as the system is configured to automatically delete files beyond these days. There are no video and audio recording cameras in any of the company's offices. Therefore, in the workplaces of the company, no recording is made, especially of employees during their work. The cameras shown in the photos 3 attached to the complaints were installed years ago, around the spring and summer of 2008 by the company's management at the time and at a time when the company had not yet recruited staff and its office space was still at that time not accessible to the public. During that period of time, only the members of the company were present and working on the premises and no one else, especially an employee as no staff had been hired yet. The cameras were installed during that period of time solely for security reasons because some of the company's members, for reasons of personal service, spent the night and slept in the office premises. Since then and before

the company started hiring, the cameras were turned off and remain turned off to this day. The cameras do not record sound, nor do they have the ability to capture the image in a photo, and they operate with the widest possible angle of view and the least possible focus on faces. There are informational signs posted in prominent places of the entrance-exit areas of the building and the offices of the company being complained about, which clearly and explicitly inform those entering the offices that the area is being videotaped. Workers were never recorded with these cameras and any data was never used to evaluate their efficiency, as is baselessly exposed in the complaints brought to the attention of the Authority. Subsequently, the Authority, with document No. C/EX/5910/01-09-2020, requested from the complained company the following additional information and clarifications: To provide the Authority with the statutes of the apartment building and the decisions of the General Assembly by which it was decided to install a video surveillance system in the common areas and around the perimeter of the building for security reasons. To inform the Authority: a) about the area or areas where the monitor or monitors of the video surveillance system and the 4 recorder are located, b) about the number of cameras and the areas where they are located inside the 4th floor, (attaching relevant photos showing the location of each camera and the space in which it is located), the way to deactivate these cameras and the reasons why the cameras were not removed from the installation points since they are not in operation since the 2008, c) if it is about separate video surveillance systems (perimeter of the building, in the internal common areas, inside the 4th floor) or a single system, d) about the way, time and content of informing the employees about the cameras, e) regarding the adaptation of information signs and texts to satisfy the right to information during processing data through a video surveillance system based on the relevant recommendations of the Authority, which are available through the no. prot. C/EX/3921/9.6.2020 press release pointing out that the model information sign attached to Directive 1/2011 has been replaced by the new information models and f) for the retention time of the image data taking into account that in article 15 par. 3 of Directive 1/2011 provides that the data is kept for a maximum of forty-eight (48) hours. Explain what it means that cameras cannot capture the image in a photograph. Because the Authority did not receive a response to the letter No. G/EX/5910/01-09-2020document, sent to the complained company the reminder No. C/EX/6545/28-09-2020. The complained-about company responded with document No. C/EIS/6886/09-10-2020, in summary, as follows: Regulation for the apartment building at 40 A Messolongiou Street in Piraeus, in which it maintains its offices exists. He presented the minutes of the general meeting dated 10/03/2015 by which it was unanimously decided to install cameras in the common areas and around the perimeter by the four co-owners 5 companies, namely 1) EMERALD SEA SOLE PERSON

SOLE PERSON SOLE PERSON IKE. IKE, 2) BLACK SEA IKE, 3) VORAS NAVIGATION SA and 4) PURPLE SEA There is no monitoring screen on site. Monitoring can only be done by the Controller, from his computer, which is protected by multiple passwords and no one else has access to it. The recorder is located in a lockable room within the building which is protected by an alarm system and only the Processing Manager has access to. There is no working camera inside the 4th floor and all work areas. The cameras installed in the company's offices on the 4th floor are a total of six (6) and are located in the following areas: conference room, office 1, office 2, secretariat, kitchenette and balcony. The cameras are positioned upside down from the jobs even if it were to be assumed that they could be activated. All cameras are isolated and locked through the recorder menu and only receive a "black" image. The cameras are deactivated by the intervention of the installation technician. The cameras were not removed from their mounting points in order to avoid, primarily, the disturbances that would arise in the area as well as for the possibility that in the event of a change in the use of the area, there is the possibility of re-operating them if and when it is deemed necessary at some point. The video surveillance system works as a single. An updated information sign was provided stating that the data subjects are referred to the complained company to exercise their rights and the data controller is E. Employees are informed about the video surveillance system through posted information signs. 6 The data is kept for a maximum of 48 hours taking into account article 15 par. 3 of Directive 1/2011. Cameras are not capable of taking photos. The photos were taken in real time by the Editor while monitoring the cameras from his computer with 'printscreen' (computer capability). These photographs capture the images taken by photography exclusively and solely for the purposes herein and in order to be submitted to the Authority. Following the aforementioned, the Authority with calls No. C/EIS/7955/19-11-2020, C/EIS/7954/19-11-2020 and C/EI/7952/19-11-2020 invited the complainants and the complained-about company, respectively, to attend the meeting of the Department of the Authority on Thursday 26/11/2020, in order to discuss the complaints in question. At this meeting Christos Oikonomakis (...) was present, as attorney of the complained company, who stated that he had nothing more to add than what is written in the documents that have already been submitted to the Authority. Complainants B and A also attended this meeting, ... The complained-about company received a deadline and filed the memorandum No. C/EIS/8398/07-12-2020 within the deadline, which briefly states the following: The company with the above memorandum denies that it violated the legislation on the protection of personal data, that the complainants did not provide any evidence in support of their complaint so as to make any rebuttal impossible and that this complaint receives interest from the existing civil dispute and the related trial. The Authority, from the hearing process and

from the evidence of the case file and after hearing the rapporteur and the assistant rapporteur, who left after the discussion of the case and before the conference and decision-making, after thorough discussion, taking into account in particular: 1. The provisions of the Constitution, and in particular those of articles 2 par. 1, 5 par. 1, 9, 9A and 25 2. The provisions of the European Convention on Human Rights of 7 04.11.1950 ratified by n .d. 53 of 19.9.1974, as it applies today and in particular those of article 8 3. The provisions of the Operation of the Treaty of the European Union and in particular those of article 16 4. The provisions of the Charter of Fundamental Rights of the European Union (2012/C 326/02) and in particular those of articles 7, 8 and 52 5. The provisions of the Council of Europe Convention for the Protection of Individuals with regard to the Automated Processing of Personal Data of 28.1.1981 ("Convention 108"), ratified by law. 2068/1992, as it applies today and in particular those of articles 5 and 6 6. The provisions of the General Data Protection Regulation (GDPR) 679/2016, the law 4624/2019 and in general the national legislation for the protection of personal data 7. The under no. 1/2011 Directive of the Personal Data Protection Authority for the use of video surveillance systems for the protection of persons and goods 8. The Guidelines of the European Data Protection Board [EDPB] no. 3/2019 "on processing of personal data through video devices" of 29-01-2019 (version 2) 9. Under no. 4/2004 Opinion of the Article 29 Working Group on the processing of personal data through video surveillance (WP89) 10. The no. 06/2014 Opinion of the Article 29 Working Group on the concept of legitimate interests of the controller (WP 217), insofar as it is interpretatively useful in the context of this 11. The Guidelines of the Article 29 Working Group "Guidelines on transparency under Regulation 2016/679", WP260 rev.01, insofar as they are interpretatively useful in the context of this CONSIDERED IN ACCORDANCE WITH THE LAW 8 1. From the provisions of articles 51 and 55 of the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR") and Article 9 of Law 4624/2019 (Government Gazette A' 137) it follows that the Authority has the authority to supervise the implementation of the provisions of GDPR, this law and other regulations concerning the protection of individuals from processing personal data. 2. The image of a person which is collected through the use of a video surveillance system constitutes personal data according to article 4 paragraph 1 GDPR, to the extent that the possibility of identifying the specific natural person1 is provided directly or indirectly, while the recording of the image which is stored and maintained in a streaming video recording mechanism, such as on the system hard drive recommends automated data processing2. 3. The installation and operation of video surveillance systems with the capture or recording of images and/or sound through the collection, preservation, storage, access and transmission of personal data constitute, as individual acts of processing, interference with the individual rights to respect for private life

according to art. 9 S., 7 XTHDEE3 and 8 ECHR as well as the protection of personal data according to art. 9A S., 8 ESDA and 8 XTHDEE4, as the Authority decided in detail with its Opinion No. 3/2020. 4. In order for personal data to be lawfully processed, i.e. processed in accordance with the requirements of the GDPR, the conditions for the application and observance of the principles of Article 5 para. 1 GDPR must be cumulatively met, as also emerges from the recent decision of the Court of the European Union (CJEU) of 16-01-2019 in case C-496/2017 Deutsche Post AG v Hauptzollamt Köln5. The existence of a 1 CJEU C-212/13 judgment Rynes para. 22, CJEU C-345/17 judgment Sergejs Buivids para. 31, CJEU C-708/18 judgment TK v. M5A para. 35. 2 CJEU Rynes para. 23, 25, Sergejs Buivids para. 34, TC para. 34. 3 CJEU Digital Rights Ireland para. 29. 4 CJEU Digital Rights Ireland para. 38. 5 "57. However, any processing of personal data must be in accordance, on the one hand, with the principles that must be observed in terms of data quality, which are set by Article 9 of the legal basis (Article 6 GDPR) does not exempt the data controller from the obligation to observe the principles (article 5 par. 1 GDPR) regarding the legitimate character, necessity and proportionality and the principle of minimization6. In the event that any of the principles provided for in article 5 para. 1 of the GDPR are violated, the processing in question is considered illegal (subject to the provisions of the GDPR) and the examination of the conditions for applying the legal bases of article 6 GDPR7 is omitted. Thus, the unlawful collection and processing of personal data in violation of the principles of Article 5 of the GDPR is not cured by the existence of a legitimate purpose and legal basis (see Decision no. 43/2019 of the Authority). In addition, the CJEU with its decision of 01-10-2015 in the contextof the case C-201/14 (Smaranda Bara) considered as a condition of the legitimate and legal processing of personal data the information of the subject of the data before such processing8. 5. Furthermore, the data controller, in the context of compliance with the principle of legitimate or fair processing of personal data, must inform the data subject that it is 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 enumerated in Article 7 of this Directive or Article 6 of this Regulation (cf. decisions ... C-465/00, C-138/01, C-139 /01, C-131/12".. 6 Relatedly, cf. L. Mitrou, the general regulation of personal data protection [new law-new obligations-new rights], ed. Sakkoula, 2017 pp. 58 and 69-70). 7 Compare StE 517/2018 para. 12: "[...] in order for personal data to be lawfully processed, it is required in any case that the conditions of article 4 para. 1 of Law 2472/1997 be met cumulatively, which among other things, it stipulates that the data must be collected and processed in a legitimate and legal manner, for clear and legal purposes... If the conditions of article 4 par. 1 of Law 2472/1997 (lawful collection and processing of data) are met for clear and legal purposes), it is further examined whether the conditions of the provision of article 5 par. 2 of

Law 2472/1997 [legal bases] are met. Also, see SC in Plenary 2285/2001 par. 10: "[...] Only if the above basic conditions are met, the provisions of articles 5 and 7 of Law 2472/1997 apply, which impose as a further additional, in principle, condition of legal processing of personal data of a specific person, his consent". 8 "31. the person responsible for processing the data 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 concern or not, and this without prejudice to the exceptions provided for in Article 13 of that Directive [...] 34. Consequently, the requirement for lawful data processing provided for in Article 6 of Directive 95/46 obliges the administrative authority to inform the persons who concern the data related to the transmission of said data to another administrative authority for the purpose of their processing by the latter as the recipient of said data". 10 to process his data in a legal and transparent manner (regarding see CJEU C-496/17 ibid. para. 59 and JJC C-201/14 of 01-10-2015 para. 31-35 and especially 34) and to be in a position at all times to prove his compliance with these principles (principle of accountability according to article 5 par. 2 in combination with articles 24 par. 1 and 32 GDPR). 6. The processing of personal data in a transparent manner constitutes an expression of the principle of legitimate processing and is linked to the principle of accountability, granting the right to the subjects to exercise control over their data by making the controllers accountable (see Guidelines OE 29, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, pp. 4 and 5). 7. With the GDPR, a new model of compliance was adopted, the central dimension of which is the principle of accountability, in the context of which the data controller is obliged to plan, implement and generally take the necessary measures and policies in order for the data processing to be compliant with the relevant legislative provisions. In addition, the data controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. It is no coincidence that the GDPR includes accountability (Article 5 para. 2 GDPR) in the regulation of the principles (Article 5 para. 1 GDPR) governing the processing, giving it the function of a compliance mechanism, essentially reversing the "burden of proof" as to the legality of the processing (and in general the observance of the principles of Article 5 par. 1 GDPR), shifting it to the data controller,9 so that it can be validly argued that he bears the burden of invoking and proving the legality of processing10. Thus, it constitutes an obligation of the data controller on the one hand to take the necessary measures in order to comply with the requirements of the GDPR, 9 Relatedly see L. Mitrou, The principle of Accountability in Obligations of the controller [G. Giannopoulos, L. Mitrou, G. Tsolia/s], Collected Volume L. Kotsali – K. Menoudakou "The GDPR, Legal Dimension and Practical Application", published by Law Library, 2018, p. 172 ff. 10 P. de

Hert , V. Papakonstantinou, D. Wright and S. Gutwirth, The proposed Regulation and the construction of a principles-driven system for individual data protection, p. 141. 11 on the other hand, to demonstrate at all times the above compliance, without it is required that the Authority, in the context of exercising its investigative and audit powers, submit individual - specialized questions and requests to establish compliance. 8. From the provisions of article 5 par. 1 sec. a GDPR and those of articles 12-15 GDPR, the obligation of the employer (controller) to inform the employee (data subject) in advance in an appropriate and clear manner about the introduction and use of control and monitoring methods during the stage of collection of his personal data (see APD 34/2018 as well as Directive 115/2001 ch. C' para. 3 and E' para. 8). 9. In article 27 par. 7 of Law 4624/2019 it is provided that "The processing of personal data through closed-circuit visual recording within workplaces, whether they are publicly accessible or not, is only permitted if it is necessary for the protection of persons and goods . Data collected through closed-circuit visual recording may not be used as a criterion for evaluating employee performance. Employees are informed in writing, either in writing or in electronic form, about the installation and operation of closed-circuit visual recording within the workplaces. From the above provision it immediately follows that, with the exception of the purpose of protecting persons and property, video recording within workplaces is prohibited. and the legality of the operation of the installation 10. According to the Guidelines 3/2019 of the EDPS, in order to judge the video surveillance system, the conditions of articles 5 and 6 par. system to document internally the legality of the processing and in fact, when determining the purpose of the processing, a relevant assessment may be needed for each camera separately, depending on where it is placed. 11. The Authority has issued Directive No. 1/2011 on the issue of the use of video surveillance systems for the purpose of 12 the protection of persons and goods, the provisions of which must be applied in conjunction with the new provisions of the GDPR and the 4624/2019, which defines GDPR implementation measures. This applies in particular to the obligations of the data controller included in chapter C' thereof (articles 10 to 13 of Directive 1/2011). For example, data controllers no longer have an obligation to notify the Authority11 of the processing, but must take the necessary measures to comply with the requirements of the GDPR and ensure the satisfaction of the enhanced rights provided for by the GDPR. 12. According to article 1 of Directive 1/2011, video surveillance systems, which include in particular closed circuit television, are defined as systems that are permanently installed in a place, operate continuously or at regular intervals and have the ability to receive or / and transmission of video and/or sound signals from this space to a limited number of projection screens and/or recording machines (cf. also No. 2/2010 Opinion of the Authority, paragraph 8). The transmission of the image can be done by directly

connecting the camera to the projection screen and/or to the recording machine or via an internal network or via the Internet for a limited number of legalized recipients. 13. A basic condition for the legality of processing through a video surveillance system is compliance with the principle of proportionality, as specified in articles 6 and 7 of Directive 1/2011, but also in its Special Part, on the self-evident condition that the conditions are met of articles 5 and 6 of the GDPR. In particular, in article 7 of the aforementioned Directive, it is stated that, in principle, surveillance is prohibited in workplaces where the video surveillance system should not be used for the surveillance of employees, except in special exceptional cases as specified in the said Directive. In particular, in a typical office space 11 See and the Authority's announcement regarding the abolition of record keeping/editing notices and the granting of licenses (decision 46/2018). 13 business, video surveillance should be limited to entry and exit areas, without monitoring specific office rooms or corridors. An exception may be specific areas, such as cash registers or areas with safes, electromechanical equipment, etc., provided that the cameras focus on the goods they protect and not on the employees' areas. In addition, article 19 paragraph 4 of Directive 1/2011 provides that, among other things, the operation of cameras in places of catering and recreation is prohibited. 14. In this case, from the correspondence of the complained company to the Authority, the following are supported: - The video surveillance system a. in the areas of the 4th floor of the apartment building where it has its offices and b. in the common areas and around the perimeter of the same apartment building, on the floors of which exclusively business areas are housed, is a single unit. - The cameras of the 4th floor were installed around the spring-summer of 2008, when only the members of the company were working and no one else, especially employees since no staff had been hired at that time, for security reasons because some of the members spent the night in the office premises. Since then and before they started hiring the cameras were turned off and remain turned off to this day. According to the installer D's report dated 07-10-2020 "Cameras in the interior spaces, they exist but have been out of order since 2008. They were never uninstalled mainly to avoid the problems that will arise in the space, as well as the case of change the use of each space and the possibility of their re-operation, if and when it is deemed necessary". - The decision to install the cameras in the common areas and perimeter of the apartment building was taken on 10-03-2015 according to the minutes of the general assembly provided. - Inside the 4th floor there are five (5) installed cameras in office areas 1 and 2, in the secretariat, in meeting room 14 and in the kitchenette as well as one (1) camera in the balcony, which have not been in operation since 2008 and they are isolated and locked through the recorder menu and only receive a "black" image. - The same person, E, who is the administrator of the complained-about company (according to its response document and the

relevant registration number 122437238000 in GEMI) as well as the administrator of the apartment building (according to the minutes submitted on 10-03-2015) monitors the images of the cameras of the unified video surveillance system from his computer, from the screen of which he captured, in real time, the image captures in photos with the "printscreen" feature, which he sent to the Authority to confirm the claims that a "blackened" image is obtained. From the above and in the absence of contrary evidence, the Authority finds that first the video surveillance system was installed on the 4th floor when the complained company started operating and then the cameras were installed in addition to the already existing system in the common areas and around the perimeter of the apartment building. Although it is a single video surveillance system, the person in charge of processing the cameras on the 4th floor is the complained company since the decision to install them was taken by it, which also has control over the means of processing, the cameras, the recorder and the monitoring screen . 15. According to the above allegations of the complained company and in the absence of contrary evidence, the Authority finds that from the year 2008 until today, the five (5) cameras in the office areas and the kitchenette on the 4th floor (as well as the one (1) camera on the balcony of this floor) remain permanently installed in their place and connected to the recorder of the video surveillance system, receiving an image, which, however, does not appear when the unit is in operation on the screen due to a related setting from the menu of the recorder with the result the screen to be "blacked out". In other words, it is established that while the image is being collected and transmitted, it is received on the screen, however, it is covered by a "black canvas", based on system settings. In addition, at any time and based on a reverse setting, the "black canvas" is removed and it is possible to view the image of the space or the persons without being "masked". Also, despite the complainant company's claims that there is no monitoring screen of the video surveillance system, the ability of administrator E to monitor all the cameras in the system on his personal computer screen constitutes the use of a projection screen, regardless of the security and access control measures on the computer such as the alleged use of strong passwords. Therefore, the cameras in question are part of a fully functional video surveillance system, they receive and transmit the image signal from their installation area to the projection screen, which image, due to the above related setting, can be projected with a "black" display and not in the original form of the original collection, depending on the setting chosen by the system operator at any time. That is, the image of the data subjects that may enter or are already within the range of the system in question is collected and normally transmitted to the recipient, who has the technical ability to display the full image on the screen or cover it by blacking out the screen, even and if for this the assistance of the installer is needed according to the allegations of the

complained company. Therefore, through this system it becomes possible to identify natural persons, depending on the system operator's setup. 16. Consequently, the above system falls within the definition of video surveillance systems based on article 1 of Directive 1/2011 since it is permanently installed in the area of the 4th floor and has the ability to receive and/or transmit a video signal from this area to the display screen of E's computer and/or connected recording machine, which is located in a shared area. The reception and transmission of the signal of the 16 images from the office and kitchen areas, where the cameras are installed, to the display screen, even without recording or storing in the recorder, constitutes automated processing of personal data and specifically the collection and transmission of received image (see paragraph 12 of this, APD 87/2015, APD Opinion 3/2020), either appears on the screen, or chooses not to appear using the relevant setting so that it is covered by a "black canvas" on the screen. And the configuration from the menu of the recorder so that the received image is displayed on the screen with a "black" display does not undo the initial processing of the collection and transmission. In fact, this parameterization can be changed at any time and in an easy way, also from the system and recorder settings, so that the image taken by the cameras is displayed on the projection screen without coverage or with coverage of part of it (cf. APD 87/2015). The company's claim that the cameras were originally placed in positions opposite to the workplaces, does not negate the capture of images from office spaces where and when employees enter or leave and generally move to and from their offices. 17. Regardless of the above, and the complained company itself, with the written explanations and the evidence presented during the pre-hearing stage, accepts the operation of the video surveillance system on the 4th floor as: a) it has permanently installed cameras in the office areas and the kitchenette and b) has posted informational signs in prominent places of its office premises informing the entrants and employees that the premises are being videotaped. Specifically, the complained-about company states in its document No. G/EIS/5388/31-07-2020, that "(..) 6. In any case, we have ensured and there are posted in visible places in the entrance areas- at the exit of the building and our offices informational signs with which those entering our offices are clearly and explicitly informed that the area is being videotaped and we provide you with relevant photos for your support. (…)" and "(…) In each case there are placed 17 information signs at visible points of the entrances and exits of the building and our offices for the information of those entering and working in our offices and the relevant material is automatically destroyed after 14 days (the system is properly set up to automatically delete files beyond of these days) (…)". According to the photos provided, the posted information signs read, until their recent update: "Caution. The area is videotaped by closed circuit television (law 2472/1997)". From the content of these information signs, although incomplete

because it did not include the required information based on article 12 of Directive 1/2011, i.e. the controller, the purpose and the person with whom the interested parties can contact to exercise their rights, combined with the existence of the installed cameras, it becomes clear that the video surveillance system is in operation and the area is videotaped. the above against the company, informative 18. According to the document No. C/EIS/6886/09-10-2020 of the complainant, the plates were replaced by the updated ones based on the Authority's 2/2020 recommendations regarding the models to satisfy the right to information, data processing through video surveillance systems in the context of GDPR implementation. The updated signs were posted in the premises of the offices of the complained company and inform the employees that a video surveillance system operates in the premises for the purpose of protecting persons and goods as well as that they can contact the complained company to exercise their rights provided for in the GDPR. If the video surveillance system was disabled and non-functional, or the image transmitted on the capture and projection screen was exclusively "black" and there was no possibility to change the setting so that it was not possible to see the whole area and therefore to identify the natural persons, there would be no reason to post informational signs about videotaping the site. Furthermore, if indeed the 18 system was not working, the company should have informed its employees of the fact that it was not working, given that the existence of installed cameras in the area creates a reasonable belief that the cameras are working, with whatever consequences it causes this feeling (including the "chilling effect")12, which is enhanced by the posting of warning signs informing about the operation of the cameras. Therefore, not only were the above-mentioned signs posted with the incomplete content in accordance with the provisions of Law 2472/1997 but later, they were updated, as explained above, so that even if a claim had been made that they had been "forgotten" and were not posted, it could not to be accepted. Moreover, the complained company itself confirms that the system is functional, that it records personal data and that the relevant material is kept for 14 days, according to its first response document, or 48 hours, according to its second response document, and then it is deleted automatically. Finally, the fact that the complained-about company invokes the provisions of article 27 par. 7 of Law 4624/2019 to argue in favor of the non-use of the material to evaluate the efficiency of the employees, presupposes the functionality and use of the system and the processing of personal data data. 19. Finally, it follows from the above that the complained-about company, as a data controller, did not provide written documentation of its compliance with the rules and principles deriving from the articles 5 and 6 GDPR but also from Directive 1/2011 of the Authority (e.g. internal assessment of the necessity and legality of the installation of the system and of the personal cameras, video surveillance system operation policy, personal data security policy), nor

however, it had and brought to the attention of the employees as well as every incoming or outgoing person in the scope of the system, detailed information 12 The voluntary (even automatic) adjustment of the person's behavior due to the fact of the monitoring. 19 for the operation of the system and the rights of data subjects. In no case, the posted video surveillance system operation warning signs or the certifications of the system installer sent to the Authority as part of the audit cannot replace the aforementioned compliance requirements. 20. Therefore, it is established that the complained company proceeds, according to the above, in illegal and non-transparent processing of personal data through the video surveillance system in the office areas and the kitchen, in violation of the principle of legality according to article 5 par. 1(a) GDPR , objectivity and transparency without documenting and proving, in accordance with the principle of accountability according to article 5 par. 2 GDPR, that it is carried out on the basis of a legal reason, namely the existence of reasons for the safety of persons and property, for which the employees have in advance be informed, in an appropriate and transparent manner and finally, without providing any kind of written documentation of its internal compliance with the GDPR in order to demonstrate compliance with Articles 5 and 6 of the GDPR in combination with the provisions of Directive 1/2011 of the Authority. Also, the complained company violates the principle of limitation of purpose according to article 5 par. 1(b) of the GDPR since it was established that the data processing is carried out without having determined a legal purpose of processing and with the intention of future determination of purpose in the event of a possible change of use of space13. The processing in question excessively violates the rights of employees since in principle, based on the legislation and Directive No. 1/2011 of the Authority, video surveillance is prohibited in an office area or in the area where employees prepare or eat their food. 21. Furthermore, the complained company did not examine, as it should have, the legality of the installation of the video surveillance system, which precedes, presupposes and is required of the legality of the processing of personal 13 See Handbook on European legislation on the protection of personal data, section "3.2. The purpose limitation principle', page 157, 2018 edition, European Union Agency for Fundamental Rights and Council of Europe, 2019. 20 data so as not to install cameras at all in office spaces and in an employee dining area taking into account the preliminary weighting of Directive 1/2011 in favor of the superior rights of the data subjects over the legal interests of the data controller, according to which cameras are not allowed in standard office space (Article 7 of Directive 1/2011) nor in dining areas (Article 19 par. 4 of Directive 1/ 2011). In addition, after the initial installation, the company did not re-evaluate the legality of the processing in order to meet the requirements of the institutional framework, which was amended (GDPR and Law 4624/2019) introducing more obligations for controllers. This obligation rests with the complained-about company both

before the establishment, when the relevant decision was taken, and at a later time of its re-evaluation, in the context of the ongoing obligation to comply with the legislation and now, after the implementation of the GDPR and for documentation of the legality of the processing. If the complained-about company did not operate the installed video surveillance system, it should have uninstalled it (cf. CoE 1137/2020 sc. 9) or at least informed its employees about its non-operation. 22. Regarding the specific issue of the specific complained of video surveillance ("targeting") of the complainants during the time of their work, from the data available to the Authority and in view of the fact that the system operator has the possibility at any time , depending on the choice of setting, either to view the image, or to see a "black" image, cannot establish beyond doubt that they were specifically monitored. The first of the complainants in support of the allegation that surveillance took place during working hours provides a printout of an image (printscreen) from the mobile phone screen, which shows an exchange of short text messages (sms) on April 11 and time from 6:04 pm until 7:34 pm between himself and C, Head of ... of the complained company, who asks him to "sit better", probably 21 in his office and the complainant allegedly replies: "Please no comments of this kind. I was sitting fine" to receive a further response: "not fine at all, we will discuss it in private". Although the content of the above messages shows without doubt that there was monitoring of the complainant, it does not appear without doubt that said monitoring took place through the video surveillance system and not in another way, e.g. in a natural way, i.e. by viewing from a close point of the same or the other premises since it is not known whether the Person in charge ... was at the company premises on the specific day and during the exchange of the messages or is able to view the images of the video surveillance system on his mobile phone or was informed by anyone who has such an ability to view the images. In any case, since the Authority has already established that in general the installation and operation of the video surveillance system violated the provisions of the GDPR, Law 4624/2019 and Directive 1/2011, it is submitted that any subsequent and more specific processing of image data using of the system in question at the expense of a specific natural person becomes illegal (see APD 44/2019 sc. 32 viii par. 3) and therefore the Authority considers that the issue of any specific monitoring of complainants through the system does not require further investigation. 23. The issue of the legality of the cameras of the unified video surveillance system which are located outside the premises of the company being complained about is not the subject of the complaint under consideration and for this reason the Authority reserves the right to examine ex officio the legality of its installation and operation. 24. According to the GDPR (App. Sk. 148) in order to strengthen the enforcement of the rules of this Regulation, sanctions, including administrative fines, should be imposed for each violation of this Regulation, in addition to or

instead of the appropriate measures imposed by the supervisory authority in accordance with this Regulation. In cases of minor violations or if the fine that may be imposed would constitute a disproportionate burden on a natural person, a reprimand could be imposed instead of a fine. 25. Based on the above, the Authority considers that it is appropriate to exercise its corrective powers under Article 58 para. 2 of the GDPR in relation to the identified violations and to order the complained company to remove the cameras in accordance with the provisions of order within one (1) month from the receipt of this order and to inform the Authority in writing of the execution of this order. 26. The Authority further considers that the above corrective measure is not sufficient to restore compliance with the provisions of the GDPR, Law 4624/2019 and Directive 1/2011 APD that have been violated and that it should, based on the circumstances established , to be imposed, pursuant to the provision of article 58 par. 2 sec. i of the GDPR, an additional and effective, proportionate and dissuasive administrative fine according to article 83 of the GDPR, both to restore compliance and to punish illegal behavior14. 27. Furthermore, the Authority took into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR, paragraph 5 of the same article which is applicable in this case and the Guidelines for the application and determination of administrative fines for purposes of Regulation 2016/679 issued on 03-10-2017 by the Article 29 Working Group (WP 253), as well as the facts of the case under consideration and in particular: a) the nature, gravity and duration of the violation, in view of the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage they suffered, namely: 14 See OE 29, Guidelines and the application and determination of administrative fines for the purposes of Regulation 2016/679 WP253, p. 6 23 i. ii. iii. iv. v. vi. vii. the fact that the complained company violated the provisions of article 5 par. 1 sec. a' of the GDPR principles of legality, objectivity and transparency, in addition the principle of limitation of purpose according to article 5 par. 1 sec. b' as well as the obligation (principle) of accountability according to article 5 par. 2 of the GDPR, i.e. it violated fundamental principles of the GDPR for the protection of personal data, the fact that the observance of the principles provided for by the provisions of article 5 par 1 p. a' and para. 2 of the GDPR is of capital importance, primarily, the principle of legality, objectivity and transparency so that if this is missing, the processing becomes illegal from the beginning, even if the other processing principles have been observed. Of equal capital importance is the principle of purpose limitation and the principle of accountability in the context of the new compliance model introduced with the GDPR, where the burden of compliance and the related responsibility rests with the controller, which has been provided by the GDPR with the necessary compliance tools, the fact that the complained company failed to comply with the requirements of the processing

authorities of article 5 par. 1 sec. a' and b' GDPR, moreover, he failed to document in the context of compliance the legality of the video surveillance system, the fact that the violation of the above principles falls under the provisions of article 83 par. 5 sec. a' of the GDPR in the highest prescribed category of the classification system of administrative fines, the fact that, from the data brought to the attention of the Authority, no material damage occurred to the data subjects - complainants, the fact that the violation of the principles of article 5 par. 1 sec. a', b' and par. 2 of the GDPR did not concern, based on the information brought to the Authority's attention, personal data of articles 9 and 10 of the GDPR, the fact that the system in question and the cameras were installed and operating illegally since the year 2008. b) the degree of culpability of the accused 24 The installation and operation of the video surveillance system by the accused company in violation of the principle of legality, objectivity and transparency, the limitation of purpose as well as accountability was the result of insufficient knowledge and application of the provisions of the GDPR which is attributable to negligence and is therefore taken into account in mitigation in relation to the possibility that it had taken place with intent. c) any actions taken by the complainant to mitigate the damage suffered by the data subjects and the degree of cooperation with the Authority to remedy the violation and limit the possible adverse effects of the the Authority, not in general and indefinite but specifically for the remedy of the violation and the limitation of its possible adverse effects. Therefore, when the data controller does not accept that it is responsible for the alleged violation of the GDPR and the applicable legislation, it consequently does not take any action and cooperate with the Authority in order to remedy the violation and limit its possible adverse effects, e.g. to proceed voluntarily and before the hearing before the Authority to uninstall the cameras or to delete the illegally obtained video recording material. As the Working Group of article 29 (now ESPD) points out on 03-

10-2017 Guidelines for the application and determination of administrative fines for the purposes of Regulation 2016/97, on the one hand the degree of cooperation of the controller is taken into account in relation to the amount of the administrative fine when it concerns the remedy of the violation and the limitation of possible adverse effects, on the other hand, does not fall under the case of the mentioned cooperation and "[…] it would not be appropriate to take into account the cooperation already required by law e.g. in case the entity is obliged to provide access to the supervisory authorities to its premises for the purpose of checks/inspections'. 25 d) any relevant previous violations of the complainant. From a relevant audit, it appears that no administrative sanction has been imposed on the company complained against by the Authority to date. e) the categories of personal data affected by the breach This is not personal data under Articles 9 and 10 of the GDPR, according to the

information brought to the attention of the Authority. f) the fact that the complained-about company did not immediately respond to the Authority's requests to provide answers to questions in the control framework and to send documents, but a reminder letter was needed from the Authority g) the unfavorable economic situation that has been created as a consequence of the COVID19 pandemic h) the size of the company. 28. Based on the above, the Authority unanimously considers that the administrative sanction referred to in the decree should be imposed on the complained company as controller, which is judged to be proportional to the gravity of the violation. FOR THESE REASONS THE AUTHORITY A. Orders the complained company named PURPLE SEA MONOPROSOPI IKE, as controller, as within one (1) month from the receipt of this notice, to remove the five (5) cameras that are 26 placed inside the 4th floor of the apartment building on 10A Messolongiou Street in Piraeus where it maintains its offices and specifically from the areas: conference room, office 1, office 2, secretariat, kitchenette, completely destroy any material that may have been collected up to then through the above cameras as well as to inform the Authority in writing about theabove.

B. Enforces the defendant company under the name PURPLE SEA
SINGLE PERSON IKE the effective, proportional and deterrent administrative
monetary fine that is appropriate in the specific case, according to
special circumstances thereof, amounting to fifteen thousand (15,000.00) euros for the
violations of articles 5 par. 1(a), 5 par. 1(b) and 5 par.
2 GDPR.

The Deputy President

George Batzalexis

The Secretary

Irini Papageorgopoulou