CORRECT REPETITION DUE TO TYPOGRAPHICAL ERROR IN NUMBERING Athens, 13-01-2020 Prot. No.: G/EX/8885/13-01-2020 PERSONAL DATA PROTECTION AUTHORITY 43/2019 (Department) The Authority of Personal Data Protection met as a Department composition at its headquarters on Wednesday 24.7.2019 at the invitation of its President, in order to examine the case referred to in the present history. The Deputy President Georgios Batzalexis, obstructing the President of the Authority Constantinos Menoudakos, and the alternate members of the Authority Panagiotis Rontogiannis, Evangelos Papakonstantinou and Grigorios Tsolias, as rapporteur, in place of the regular members Antonio Symbonis, Konstantinos Lambrinoudakis and Charalambos Anthopoulos, respectively, were present, who , although they were legally summoned in writing, they did not attend due to disability. Present without the right to vote were Kalli Karveli, specialist scientist-lawyer, as assistant rapporteur, who left after the discussion of the case and before the conference and decision-making, and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary . The Authority took into account the following: 1 With the no. prot. C/EIS/7748/01.10.2018 his complaint to the Authority A complains that his employer company "ALLSEAS MARINE SA" processed without informing him and continues to process personal data of himself and his family, including sensitive , violating his right as an employee to his personal data. In particular, as stated in his complaint and in the documents attached to it, the complainant worked for the complained-about company for ... years. He announced his resignation on ... and his resignation according to his agreement with the employer owner of company B, would be valid for ... . However, as he claims, the owner of the company, citing an incident of violation in the company, which he did not notify, as he should have, to the Authority within 72 hours of its discovery, and while the complainant was absent abroad a) conducted an investigation and processed without the prior information of the complainant, his personal data, in the "electronic communication systems" that he handled in the company, b) prohibited him from entering the company, placing him on compulsory leave and denied him access to both the "electronic means of communication" that he handled as a general director of the complained-about company (company e-mail and remote telephone access to the company's server), as well as the personal files he kept on his computer (personal financial details of his bank accounts, health data of himself and his family, such as medical results exams, personal correspondence and social media, etc.). He also complains that in addition to his personal computer, there were his personal files on the computer of his private secretary, who was fired, and who was forbidden from receiving her personal files, with the result that he does not have access to them either. Following this, with his out-of-court statement to the company from ..., he requested a) to attend any inspection regarding the

objects in his workplace as well as the inspection of the electronic means of communication that he handled as an employee, so that the legal and necessary separation of his personal from the purely professional files and b) to be informed 2 in writing about his being declared on compulsory leave and the observance of the legal formalities thereof, as well as for which act he is being audited. The company in its out-of-court response from ... stated that the complainant received all his personal belongings and files from the company upon his departure and that from ... no legal relationship connects the company with him, without, as the complainant states, responding to the his request for access to the data included in the computer he uses and which concern him. He also complains that the company does not have a privacy policy nor a breach incident management policy and an internal regulation for the proper use and operation of the equipment and the IT and communications network with the employees, from the content of which it would appear, on the one hand, that the use was prohibited of computers for personal purposes, on the other hand, the possibility and possibility of checking them, the conditions, the conditions, the procedure, the extent and the guarantees of checking would be expressly provided for, while video surveillance systems are maintained in all workplaces even for leisure (cafeteria) without the knowledge of the employees. With his second out-of-court statement from ... the complainant declares that he will make a complaint to the APDPH and that there are still his personal data within the company that are illegally not attributed to him. For these reasons, the complainant requests the intervention of the Authority, so that the processing of his personal data is stopped, his personal data is returned to him electronically and in physical form, and the appropriate sanctions are imposed on the complained company. The Authority, in the context of investigating the complainants, sent on 18.10.2018 under no. prot. C/EX/7748-1 document to the complainant to provide clarifications regarding the complaint, which in no. prot. C/EIS/8933/13.11.2018 its response stated that the company on ... after ascertaining the deletion of a significant number of electronic files and e-mail messages of the company from its proprietary systems, carried out an internal investigation in the context of which, recovered them with the help of a technical company and discovered the commission of illegal acts by the complainant. In particular, as stated in the memorandum filed with the Authority, B established that during the period of time ... , the complainant and C, an employee of his company of interests in ..., were complicit in the performance of 3 criminal acts, as they transferred sums of money of the company to third parties or to the complainant. For this reason, the owner and shareholder of company B submitted from ... an application for injunctive measures with a request for a temporary injunction, which was accepted, and the application for injunctive measures was heard on ... before the Single-Member Court of First Instance of Athens. Following

the aforementioned, the Authority, with calls No. C/EX/7748- 2/7.12.2018 and C/EX/7748-3/7.12.2018 respectively, invited the complainant and the company ALLSEAS MARINE S.A., to attend the meeting of the Department of the Authority on 19.12.2018, in order to have a hearing of the company on the possible violation of the current legislation for the protection of personal data, in accordance with the provisions of articles 57 and 58 GDPR in combination with the provisions of articles 19 and 21 of law 2472/1997, as well as with those of article 14 par. 10 of the Civil Code (law 2690/1999). During the hearing of 23.01.2019 postponed from 19.12.2018, the complainant A appeared after the attorneys of Theodoros Giannatsis and Georgios Pantazis and on behalf of the company ALLSEAS MARINE S.A. Sofos Themistokles, attorney-at-law, Gritza Zafiria Legal Advisor of the company and B, main shareholder and owner of the company, who, after developing their opinions orally, then submitted their relevant memoranda to the Authority. The complainant during the hearing of 23.01.2019 postponed to 19.12.2018, but also with the no. prot. C/EIS/1178/12.02.2019 his memorandum to the Authority stated that a) the reported company ALLSEAS MARINE S.A. and B illegally processed his personal data as data controllers, b) the employer of the complainant was the company and not B, nor is any of his legitimate interests affected in order to process his personal data, even disclosing it to partners, internal, external as well as and before a court, c) for ... years his employer was ALLSEAS MARINE S.A., in which B had the simple status of a shareholder, d) the alleged operation of video surveillance systems was never notified to the Authority, e) ALLSEAS failed to notify the incident of violation within 72 hours to the Authority without justifying why it was so late and without submitting any additional 4 documents proving the violation, f) failed to record the incident in the records of processing activities that it is obliged to keep, to inform the persons involved and did not conduct an impact assessment study to assess Mr risks that will be created by the control of his personal data without the knowledge and without the consent of the complainant, g) the controlled company methodically characterizes the consequence of the incident of violation as minor, in order to benefit from the exception of the law and to justify the late filing of the notification incident violation, h) B admitted that he informed the complainant for the first time with the serving of the injunctions, i) the audited company has not yet explained why it proceeded with the illegal processing of the complainant's personal data, why he was never informed about the audits being carried out to his personal data, as well as why they cut him off from any access to his data and did not previously address a competent administrative or judicial authority to carry out the investigations they wanted and finally j) with the no. ... decision of the Single Member Court of First Instance of Athens rejected as indeterminate the application by ... for injunctive measures of B, with which he requested the seizure of the complainant's immovable and

movable property due to tort. The controlled company during the hearing of 23.01.2019, but also with the no. prot. C/EIS/1176/12.02.2019 her memorandum to the Authority stated that a) no data was extracted from the complainant's personal e-mail account, but everything retrieved, from the deleted files on the company server, came from the company account electronic mail of the complainant, b) it was found from the security cameras that the complainant had arbitrarily entered the file of the legal department of the company, night hours of ... and midnight hours of ... and was looking for files and data of the company, and the relevant material was attached with printouts of photos in the audited memorandum of the audited company, which had shown part of it during its hearing without objection from the complainant, c) from the moment suspicions of illegal acts appeared, everyone was excluded from remote access, and it was immediate and imperative the need to check the server without being present a of the complainant, without it being possible to choose a 5 less burdensome measure, d) the search and retrieval of files was done only on the company's server and not on the computer used by the complainant, e) the incident of violation of the company's files of the company by the person in charge of it, i.e. the complainant, was notified to the Authority when it came to his knowledge after an investigation carried out by the specialized consultants, f) the installation of a video surveillance system has been notified to the company's employees and in particular is included in the information manual of the employees for the processing of their personal data, and which the complainant was also aware of, g) the manual in question expressly mentions the obligation to use electronic communications exclusively for professional purposes and not for personal ones, as well as the obligation of employees not to post material or photos on personal pages in social media online networking, h) contrary to the claim of the complainant, the company has a privacy policy and a breach incident management policy as well as an internal regulation for the proper use and operation of equipment and communications with employees and, finally, i) the company has an access policy and control of the company computers used by the employees, which describes as a minimum the relevant purposes of access and control, respecting the principle of proportionality, the nature and extent of the control, the procedure, the manner and the conditions of access both in case of presence as well as any absence of the employee, the procedural guarantees regarding access and control, the way of informing the employee about the findings of the control, the procedure followed after the completion of the control with which personal data may be processed, the previous notification of the employees for the eventual acc assistance and control over the company computers they use as well as the cases of exemption from the obligation to inform and the foreseen possibility of recourse for employees to legal protection. Also, with the under no. prot. C/EIS/2384/28.03.2019 his application the attorney

of the complainant G. Pantazis notified the Authority under no. ... decision of the Single-Member Court of First Instance of Athens, by which the application by B for injunctive measures to freeze the complainant's immovable and movable property due to tort was rejected as indeterminate. 6 Following the submission of the memoranda after the hearing, the Authority deemed it necessary, in view of the diametrically opposed claims of the two sides and the documents submitted as evidence, to provide additional supplementary clarifications and with no. prot. C/EX/4780/5.7.2019 and C/EX/4781/5.7.2019 its documents, requested the provision of these, respectively, from the complainant and from the audited company, in order to make a decision. Following this, the complainant in no. prot. C/EIS/5119/22.07.2019 his supplementary memorandum argued that: a) during his absence on leave, the complainant, after searching his company computer, removed the hard drive for further inspection, without having previously was informed about it himself, without having given his consent and without being present during the removal of the hard drive and its control b) the complainant illegally retrieved his personal data after checking his electronic e-mail, his personal physical correspondence , of his private documents that were in his workplace as well as the personal mobile phone of his private secretary c) the company computer also included his personal data, to which he wished to have access, but the defendants refused to satisfy his request, they had blocked his access to the workplace, declaring him on compulsory leave d) in the complained the company maintains a backup file for storing the deleted files (back up), which proves the violation of the principle of proportionality in the disputed processing of his personal data e) the company operates a video surveillance system that was never notified to the Authority f) there is no special, overriding legal interest of the complainants, which justifies their intervention in the personal data of the complainant, as also inferred from the rejection as indefinite of the request for injunctive measures with the later case no. ... decision of the Single Member Court of First Instance of Athens g) the audited company is lying with the claim that during the hearing before the Authority he confessed that he stored the company's files on a hard disk, while the truth is that he stored part of his personal data on a hard disk (back up) for reasons of security of the files and the same files were also kept in a back up, stored on a disk by Department 7 of the company's IT department h) the audited company falsely stated that he himself was responsible for the company's security policy, despite that he himself signed it. In all the company's manuals it is stated that the managing director, i.e. B, is responsible for the company's security policy, and not the complainant, who as general manager is responsible for implementing what B approves i) the complainants (company and B) they do not invoke and do not provide any evidence to confirm their non-interference in the complainant's computer and to prove the complainant's prior information and consent to

the processing of his personal data j) in the Security Policy provided by the complainants, the conditions for monitoring of employees' communications are vague and unclear in terms of their criteria, creating a risk for their privacy and k) in the unsigned draft "Information and protection for the processing of personal data for office workers" filed with the Authority, no specific reference is made to video surveillance systems, what origin they write, for how long and in what places. The controlled company under no. prot. C/EIS/5110/22.07.2019 its supplementary memorandum asserted that: a) the complainant was the legal representative of the company and its Data Protection Officer (DPO) -DPO, b) in the 4th Section of the Business Manual from 2.01.2017 The company's Policy Manual, which the complainant himself had signed, explicitly states that all electronic communications must be used for business purposes only and that the company reserves the right to monitor all electronic communications in which the equipment is used , the company's software and systems, within the limits of applicable national law, and therefore employees should not expect privacy when using the company's systems c) in the PolicySecurity of the company's IT systems, which was drawn up on 5/12/2012 and amended on 5.11.2013 and 19.6.2015, as updated and valid until today, and bearing the complainant's signature, states that all messages sent via of the IT and communication systems of ALLSEAS MARINE S.A. is its property and that the company will monitor, access, retrieve, read and/or disclose employee communications when there is a legitimate corporate 8 need that cannot be met by other means, the employee is unavailable, and the timing is critical to the company's business, there is reasonable cause for suspected criminal activity or a violation of internal policy, or the surveillance is required by laws, regulations or third-party agreements d) the processing was absolutely necessary to satisfy the company's overriding legitimate interest pursuant to application of art. 5 par. e' of Law 2472/1997 and of No. 34/2018 of the Authority's decision, as well as the decision of the ECtHR Barbulescu v. Romania of 05-9-2017, e) the fact that the request for interim measures was rejected for formal reasons does not affect the essence of the case, which will take the criminal path of investigation f) the search and retrieval of the files was done only on the server of the company which belongs to the exclusive ownership of the company and is used only for the maintenance and processing of data related exclusively to the activities of the company g) no data was extracted from a personal account of the complainant's e-mail, but everything retrieved from the deleted files on the company server came from his company e-mail account, h) as the complainant himself confessed before the Authority, he has received a back up of the company's file until ... and other times earlier, so he has received all his personal data i) the complainant is suspected of of illegal data processing and financial offenses for this reason was notified to the Authority on … by ALLSEAS MARINE S.A. personal data breach

incident j) the withdrawn e-mails did not relate to the complainant's personal data, but to the company's data which he illegally processed, i.e. stored in his own electronic file storage system and then deleted with the help of company employees , who were acting under the orders of k) no processing was done on the personal computer of the complainant to suspect illegal processing of his personal data that was kept on the desktop of the personal computer under the personal folder, the creation and maintenance of which was against with the company's policies that expressly prohibited it l) the complainant's right to information was satisfied with the company's out-of-court statement from ... m) the complainant had to prove what personal data he had stored on the company computer that he 9 operated and finally n) the company has placed cam security measures in areas that are critical workplaces within the meaning of art. 7 of Directive 1/2011 (Crew management department, human resource management department, accounting department, legal department), and has posted in a sufficient number and in a visible place clearly visible signs, where the company as the controller and the purpose of their operation are indicated. The Authority, from the hearing procedure, from the elements of the case file, as well as from the memoranda submitted to the Authority, apart from the material obtained from the video surveillance system of the audited company, part of which was shown during the hearing (without objection from of the complainant) and was subsequently submitted by the audited company in paper form (photo prints), which the Authority does not take into account according to art. 19 par. 3 S., as detailed in reference no. 20 recital of the present, and after hearing the rapporteur and the assistant rapporteur, who left after the discussion of the case and before the conference and the decision-making, after a 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, 5A, 9, 9A, 19 par. 3, 17, 22, 25 and 28 2. The provisions of the European Convention on Human Rights of 04.11.1950 which was ratified with the 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) under no. 679/2016 10 7. The provisions of Law 2472/1997 insofar as they do not contradict the GDPR (see GDPR 46/18 and 52/18) 8. The provisions of Directive no. 115/2001 of the Personal Data Protection Authority regarding employee files 9. The no. 1/2011 Directive of the Personal Data Protection Authority for the use of video surveillance

systems for the protection of persons and goods 10. The Guidelines of the European Data Protection Board [EDPB] no. 3/2019 "on processing of personal data through video devices" of 10-7-2019 under public consultation 11. Under no. 2/2017 Opinion of the Article 29 Working Group on the processing of personal data at work (WP 249) 12. The Working Document of the Article 29 Working Group dated 29-5-2002 on the surveillance of electronic communications at the workplace (WP55) 13. The under no. 8/2001 Opinion of the Article 29 Working Group on the processing of personal data in the context of labor relations (WP 48) 14. The under 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 15. 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 16. The under no. 2/2006 Opinion of the Article 29 Working Group on privacy in the provision of e-mail screening services (WP 118), insofar as it is interpretatively useful in the context of this 17. The approved 21-11-2000 Working Document of Article 29 Working Group on the Protection of Privacy on the Internet (5063/00/OE37), insofar as it is interpretatively useful in the context of this 18. The August 1996 report and recommendations of the International Working Group on the Protection of Personal Data in the field of 11 telecommunications (IWCDPT) on telecommunications and privacy in labor relations 19. The Code of Ethics of the International Labor Organization for the protection of personal data of employees of 1997 20. The no. 2015/5 Recommendation of the Council of Ministers of 01-4-2015 on the processing of personal data in the context of labor relations 21. The no. R (89)2 Recommendation of the Council of Ministers of 18-01-1989 on the protection of personal data processed in employment relations 22. The revised Guidelines regarding the Data Protection Officer (DPO) of the Article 29 Working Group (WP 243 rev. 01 of 05-4-2017) CONSIDERED ACCORDING TO THE LAW 1. With article 94 of the General Data Protection Regulation (GDPR) no. 679/2016, Directive 95/46/EC was repealed from 25.5.2018, when the GDPR came into force according to art. 99 par. 2 thereof. Law 2472/1997 is still valid insofar as its provisions do not conflict with the GDPR (see GDPR 46/18 and 52/18). 2. The processing of personal data should be intended to serve humans. The right to the protection of personal data is not an absolute right, it must be assessed in relation to its function in society and weighed against other fundamental rights, in accordance with the principle of proportionality (Rep. 4 GDPR). 3. Recital 39 of the GDPR explains the conditions for legal processing of personal data. 4. In order for personal data to be lawfully processed, i.e. processed in accordance with the requirements of the GDPR, the conditions for applying and observing the principles of article 5 par. 1 of the GDPR must be cumulatively met, as can be seen from the recent decision of

the12 Court of Justice of the European Union (CJEU) of 16-01-2019 in case C-496/2017 Deutsche Post AG v. Hauptzollamt Köln1. The existence of a legal basis (art. 6 GDPR) does not exempt the data controller from the obligation to observe the principles (art. 5 par. 1 GDPR) regarding the legitimate character, necessity and proportionality and the principle of minimization2. In the event that any of the principles provided for in article 5 paragraph 1 of the GDPR is violated, the processing in question is considered unlawful (subject to the provisions of the GDPR) and the examination of the conditions for applying the legal bases of article 6 GDPR3 is omitted. Thus, the illegal collection and processing of personal data in violation of the principles of Article 5 GDPR is not cured by the existence of a legitimate purpose and legal basis (cf. GDPR 38/2004). In addition, the CJEU with its decision of 01-10-2015 in the context of 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 prior to the processing thereof4 . 5. Furthermore, the controller, in the context of the observance of the principle of legitimate or fair processing of personal data 1 "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 (cf. judgments ... C-465/00, C-138/01, C-139/01, C -131/12".. 2 Relatedly, see L. Mitrou, the general regulation of personal data protection [new law-new obligations-new rights], Sakkoula ed., 2017 pp. 58 and 69-70). 3 Compare StE 517/2018 par. 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 Law 2472/1997 are cumulatively met 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". 4 "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". 13 character, must inform the data subject that he is going to process his data in a legal and transparent manner (regarding see CJEU C-496/17 op. para. 59 and CJEU C-201/14 of 01-10 -2015 par. 31-35 and especially 34) and be in a position at any time to prove his compliance with these principles (principle of accountability according to art. 5 par. 2 in combination with articles 24 par. 1 and 32 GDPR). The processing of personal data in a transparent manner is a manifestation of the principle of legitimate processing and is linked to the principle of accountability, providing the right to the subjects to exercise control over their data by holding the controllers accountable (see Guidelines OE 29, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, pp. 4 and 5). The collection and processing of personal data should not, as a rule, take place secretly or with its concealment from the data subject, as well as with concealment of all necessary information, unless provided for by law, in compliance with the conditions of Article 8 ECHR , as interpreted with the decisions of the ECtHR and always in the light of the principle of proportionality. 6. In addition, 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 is in accordance with the relevant legislative provisions. 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 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" regarding the legality of the processing (and in general compliance with the principles of article 5 par. 1 GDPR), shifting it to the data controller,5 so that it can be validly argued that 5 Relatedly see L. Mitrou, The Principle of Accountability in Obligations of the Controller [G. Giannopoulos, L. Mitrou, G. Tsolias], Collected Volume L. Kotsali – K. Menoudakou "The GDPR, Legal Dimension and Practical Application", ed. Law Library, 2018, p. 172 ff. 14 he bears the burden of invocation and proof of the legality of the processing6. Thus, it constitutes the obligation of the data controller, on the one hand, to take the necessary measures on his own in order to comply with the requirements of the GDPR, and on the other hand, to demonstrate his compliance at all times, without even requiring the Authority, in the context of research - of its audit powers, to submit individual - specialized questions and requests to ascertain compliance. It should be pointed out that the Authority, due to the fact that the first period of application of the GDPR is passing, is submitting questions and requests in the context of exercising

its relevant investigative and audit powers, in order to facilitate the documentation of accountability by data controllers. The data controller must, in the context of the Authority's audits and investigations, present on his own and without relevant questions and requests from the Authority the measures and policies he adopted in the context of his internal compliance organization, as he is aware of them after planning and implementing the relevant organization. 7. The European Court of Human Rights (ECtHR) has made it clear that the protection of "private life" based on Article 8 ECHR does not exclude the professional life of employees and is not limited to life within the place of residence (see APDPX 34/ 2018 and OE29 Working paper on the surveillance of electronic communications in the workplace of 29-5-2002, WP55, p. 8). 8. Employees have a reasonable expectation of privacy in the workplace, which is not abrogated by the fact that they use equipment, communication devices or any other professional facilities and infrastructure (e.g. electronic communications network, Wi-Fi, corporate e-mail addresses, etc.) of the employer (see APDPX 34/2018, 61/2004, Working Group of article 29 WP55, ibid. p. 9, L. Mitrou, ibid. in collective volume Kotsali, ibid., p. 204). 6 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. 15 The fact that the employer can be the owner of electronic means of communication (e.g. computers, tablets, telephone devices, corporate communications network, servers, corporate email addresses, etc.) or that an electronic letter has been sent from a corporate email address does not lead to a waiver of the right in private life (see ECtHR, First Section, George Garamukanwa v. UK decision of 14-5-2019 on admissibility, para. 25), the right of employees to the protection of personal data, the right to the protectionof the confidentiality of communications and related location data (see OE29 Opinion 2/17, p. 22 and OE29, WP55, ibid., p. 22), nor certainly can it be accepted that the personal data of employees who generated through the use of corporate communications are the "property" or "property" of the employer because they are the owner of the said communications or corporate electronic mail addresses, an approach adopted by some US court jurisprudence; but not of the European Union. In addition, the fact that personal data is processed in the workplace and related to professional activity, does not negate their characterization as personal (see CJEU C-398/2015 Salvatore Manni decision of 09-3-2017 para. 34), nor does it entail an exemption from the relevant protection. In view of the above, it should be clarified that electronic communication-correspondence (e-mails) is subject to the protection of personal data legislation, even when it takes place in the context of a professional relationship, as long as the address of the electronic communication (e-mail address) to include information in relation to the natural person-user, which makes it possible to identify him according to art. 4 par. 1 GDPR.

Thus, the electronic communication address e.g. johnsmith@ikea.sk constitutes personal data, but not, in principle, that which directly concerns the legal entity, e.g. ikeacontact@ikea.com 7. 7 For details see the content of the 21-02-2018 response given by the European Commission to question E-007147/17 in the context of no. 16 9. As recently decided by the decision APDPX 34/2018 the access by the employer to stored personal data on the employee's computer constitutes processing of personal data (see also APDPX 61/2004). The above applies in case of access to personal data contained in any storage medium or electronic communications system, as well as on a server. Therefore, any argument in which personal data contained in a computer used by the employee is protected, but not in those contained in the company server, finds no basis in the current legislation and is in complete contradiction to the nature of personal data character and purpose of their protection. 10. The employer exercising his managerial right to protect the property and the orderly operation of the business, under the self-evident condition of compliance with the principles of article 5 par. 1 GDPR8 and on the basis of the specific procedures and guarantees provided for before the processing in the context of the organization of internal compliance in accordance with the principle of accountability, is entitled to exercise control over the electronic means of communication that it provides to employees for their work, as long as the relevant processing, respecting the principle of proportionality, is necessary for the satisfaction of the legal interest that seeks and under the condition that this obviously takes precedence over the rights and interests of the employee, without affecting his fundamental freedoms according to art. 6 par. 1 sec. in the GDPR and after the latter has been informed even about the possibility of a related control (see in detail GDPR 34/2018). The same legal basis and approach is adopted by the ECtHR's recent jurisprudence (see Barbulescu v. Romania decision of 05-9-2017 in a broad composition, para. 127). http://www.europarl.europa.eu/doceo/document/E-8-2017-007174-ASW_EN.html?redirect 8 Relatedly see Article 29 Working Group, Opinion 2/2017 on data processing at work, WP 249, p. 7 ff. and L. Mitrou, The data protection of employees in Leonida Kotsali (ed.), Personal Data, Analysis-Comments-Implementation , Law Library, Athens 2016 p. 185 ff., especially 197 ff. 17 In this case, a fair and necessary balance should be achieved between the purposes of achieving the legitimate interests pursued by the data controller on the one hand (see OE29, Opinion 2/2017 "on data processing at work", p. 4) and respecting the reasonable and legitimate expectations of employees for the protection of personal data in the workplace, on the other hand. The legal and reasonable expectations of the employees in this case are based on the principles of lawful and legitimate or fair processing of these personal data in a transparent manner, correspondingly creating the relevant obligations for the data controller. 11. In particular, the satisfaction of the legal interest (for the relevant meaning, see

Article 29 Working Group Opinion 6/2014) sought by the employer may consist, among other things, in the exercise of the managerial right, from which the collateral obligations of loyalty to him derive9 and from these the obligation to provide information to him, as well as the control of the leakage of know-how, confidential information or commercial/business secrets (see L. Mitrou, Labor Law Review, 76th volume, 2017, p 137 ff., especially 146-147). In particular, such a legitimate interest can be constituted by the employer ensuring the orderly operation of the business by establishing employee control mechanisms (see APDPX 34/2018, ECtHR Barbulescu v. Romania, ibid., para. 127) as well as the need to protect the company and its property10 from significant threats, such as preventing the transmission of confidential information to a competitor or ensuring the confirmation or proof of the employee's criminal actions (regarding see APDPX 34/2018, Article 29 Working Group Working Paper on the surveillance of electronic communications in the workplace of 29-5-2002 WP55, p. 18), to the extent of course that the employer, in 9 Relatedly see AP (All) 1/2017 "From the provisions of articles 652 and 288 of the Civil Code and 16 of Law 146/1914 it follows that the employee, who has a duty of loyalty to his employer, is obliged not to engage in competitive acts, which harm the interests of the employer. Such acts, among others, are the carrying out on one's own account, without the knowledge of the employer, of commercial activities, similar to the acts of the latter, as well as the servicing of the employer's customers directly by the employee (AP 1285/1984)". 10 The employer's managerial right is guaranteed by article 17 of the Civil Code in conjunction with the provisions of articles 5 par. 1, 9, 9A, 22 par. 1, but also 106 par. 2 of the Civil Code (see Fereniki Panagopoulou-Koutnatzis, The new technologies and the protection of the private sphere in the workplace, European States 2/2011, p. 325 ff., 331 ff.), from which the principle of the objective interest of the company is deduced, which allows the judge to weigh the conflicting interests when reviewing a decision of the employer. 18 in the latter case, it does not enter into the exercise of investigative actions which are reserved by law exclusively to the competent judicial-prosecution authorities and the services that act under their direct supervision, and in particular to those carried out under secrecy11. However, in the case where the company's internal policies and work regulations provide for the possibility of checking and investigating especially the electronic communications and records of employees based on specific procedures and guarantees and if the employees have been previously informed, even of the relevant possibility, then there can be no talk of carrying out investigative actions which are reserved by law exclusively to the competent judicial-prosecution authorities and the services that act under their direct supervision12. 12. The employee's use of networks, electronic communication systems or data storage media belonging to the employer and for which he has previously been expressly informed that their use is

prohibited for non-professional (i.e. non-corporate) reasons does not in itself constitute (that is, without the existence of well-founded suspicions) a legal reason for continuous surveillance or universal control of the personal data processed by the employee, but more specific information is required (regarding ECtHR, Barbulescu v Romania, op. cit., para. 77). Of course, the case of a specific and targeted control when there are reasonable suspicions of an illegal act is different. In the event that internal company policies prohibit the use of electronic means of communication or the corporate network, storage systems, servers, etc. for private (personal) purposes and the employee has been informed of both the relevant prohibition and thepossibility of the employer, in the context of an internal investigation, to gain access to the relevant systems and therefore to the personal data held 11 For details see N. Livou, Organized Crime and Special Investigations, volume I, issue a', Law & Economy P.N. Sakkoulas, p. 9. 12 Relatedly see and no. 17 par. 16 et seq. of the proposal for a draft law on the protection of personal data in application of GDPR 679/2016 under consultation of 02-20-2018 http://www.opengov.gr/ministryofjustice/?p=9314 19 nature, then the employee's expectation of non-intervention by the employer constitutes an important, but not necessarily exclusive, factor (see ECtHR, Barbulescu, op. para. 73 last ed.). 13. 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 GDPR 34/2018 as well as Directive 115/2001 ch. C' para. 3 and E' para. 8). The surveillance and control by the employer of personal data and communications stored in the company's systems without the knowledge and absence of the employee cannot be excluded a priori, but is reserved for exceptional cases, provided that such an action is either foreseen, or does not contravene national legislation and provided that the necessary measures and procedures are in place for access to professional electronic communication (see document WP 55, ibid. in particular pp. 5, 15, 16, Code of Ethics of the International Organization of Labor for the Protection of the Personal Data of Employees 1997, in particular articles 6.14 and 11.8, Recommendation 2015/5 of the Council of Ministers of 01-4-2015 on the processing of personal data in the context of employment relations, in particular articles 14.1-14.5 and 15.6). In accordance with article 11.8 of the International Labor Organization's Code of Ethics for the Protection of Employees' Personal Data of 1997, the employer is entitled, in the event of a check carried out on personal data for security reasons, to temporarily deny the employee access to them until the end of the audit, in order not to jeopardize the conduct of the investigation. In addition, any control of the computer or the server (server) of the company where the electronic

correspondence of the employees is stored, without the existence of an internal policy according to the above or in the absence of a relevant internal policy, without prior information 20 of the employees and without the presence during the audit could be judged as legal, necessary and appropriate for the achievement of the intended purpose, if there was a compelling reason of force majeure (see APDPX 37/2007) and if the principle of proportionality was met. Any prior notification of the monitoring or interception of the employee's communications by the employer does not automatically mean that Article 8 ECHR is not violated (OE29 WP55, op. p. 9), when the conditions of the exceptionally legal restriction are not met of the relevant individual right. On the other hand, the employer has the right to take the necessary, legal and proportional measures in order for the company to operate properly and efficiently and to protect itself from the damage or harm that can be caused by the actions of the employees (see APDPX 34/2018, OE29 , WP55, ibid., p. 4). Already the European Court of Human Rights, after the Barbulescu decision (see above) with the Libert v. France13 and George Garamukanwa v. United Kingdom14 decisions, considered in the examined cases as in accordance with Article 8 ECHR the carrying out of control by the employer in electronic mail and other electronic files kept by the employee on his computer and mobile phone, while the reconsideration of the case of Lopez Ribalda and others v. Spain15 is pending in the Plenary Session at the request of the Spanish Government, where the case of secret surveillance of employees by the employer with the installation of cameras in order to ascertain the commission of criminal acts. 14. In order to examine the legality of the access of the data controller no. 5 and 6 par. 1 GDPR in the personal data of the subjects kept in its corporate systems for purposes of corporate internal control, the art. 5 and 6 par. 1 GDPR 13 No. appeal 588/2013, decision of 22-10-2018. 14 No. appeal 70573/17, decision on admissibility of 5-14-2019. 15 No. appeal 1874/2013 & 8567/13, on which the 3rd Department had issued a decision from 09-01-2018 decision which found a violation of Article 8 of the ECHR. 21 legality of the initial collection and retention of personal data. The illegal initial collection and retention of personal data e.g. on the company's computer or server, similarly makes illegal any subsequent or further (i.e. with a different purpose to the original according to art. 6 par. 4 GDPR) discrete and independent processing of the same personal data as in the case of copying and their storage on another digital storage medium (e.g. usb stick, server, pc, etc.), but also in that of their transmission and use, even in the case in which the conditions for the application of a legal basis of article 6 par. 1 GDPR, such as e.g. that of paragraph f, since non-compliance with the processing principles of article 5 par. 1 GDPR is not cured by the existence of a legitimate purpose and legal basis (see recital no. 4 of this and cf. GDPR 38/2004) . 15. The storage and transmission of a facial image, which is collected by a video

surveillance system (see also CJEU C-212/13 Rynes decision of 11-12-2014 par. 22) that operates permanently, continuously or at regular intervals, in closed or an open place of gathering or passage of persons, constitutes processing of personal data, to the extent that it provides the possibility of identifying a natural person (For details see under no. European Data Protection Board [EDPR] under no. 3/2019 Guidelines "on processing of personal data through video devices" of 10-7-2019 under public consultation and CJEU C-345/2017 Sergejs Buividis decision of 14-02-2019 par. 31 and 34). The installation and operation of the relevant system is legal, as long as the conditions of articles 5 (general principles) and 6 (legal basis) of the GDPR as well as Directive 1/2011 GDPR are met cumulatively, and the relevant obligation to prove legality rests with the controller ' application of the principle of accountability in the context of internal compliance and its documentation, which must take place in time before the installation and operation of the system. The transmission of the material recorded through the system constitutes a distinct and independent act of processing personal data and therefore should be carried out by the data controller, corresponding to the initial legal collection and retention of the material, a check of legality 22 pursuant to art. 5 and 6 ECHR, taking into account the possible change of the original purpose of processing according to art. 6 para. 4 GDPR (for details see ESPD 3/2019 ibid. para. 48 et seq.). It goes without saying that the illegal initial collection and retention of said material containing personal data likewise renders illegal any further processing of the same data in violation of Article 5 para. 1 GDPR, even in the event that the application conditions would be met a legal basis of article 6 par. 1 GDPR, such as e.g. that of paragraph f, since non-compliance with the processing principles of article 5 par. 1 GDPR is not cured by the existence of a legitimate purpose and legal basis (see recital no. 4 of this and cf. GDPR 38/2004) . 16. In this case, the audited company, ALLSEAS MARINE S.A., as data controller in the context of this procedure, through the owner-shareholder of B, who as a natural person did not acquire the status of data controller, rejected the complainant's claim , prohibited on ... the complainant, its General Manager, A from entering its premises due to what it characterized as a security incident for which an audit was carried out by external partners, namely the deletion of a file by the legal department and the information that they had been deleted , under the responsibility of the complainant, from servers of e-mail messages and electronic documents (hereinafter "electronic files"). Subsequently, an external partner checked the servers owned by the company on ..., at which point the information and the suspicion were confirmed by finding that electronic files had been deleted. The initiative and direction of the deletion of the electronic files was attributed by the audited company to the complainant as according to the same, in this way he intended to disappear, on the one hand, evidence of embezzlement at the expense of the audited company and,

subsequently, of dealing in the embezzled sums of money, on the other hand, the concealment of other evidence of illegal collaboration with other involved persons. From the control of the servers, deleted electronic files were recovered, from the content of which it was proved that 23 of the complainant had committed criminal acts (especially embezzlement) according to the claims of the audited company, and these indicatively included electronic correspondence for the transfer of sums of money, purchase of art paintings with money of the attributed embezzlement, analysis of bank movements, etc. The complainant in the out-of-court statement-protest to the audited company complained about the investigation of the company's "company electronic means of communication (company devices, laptop/stationary computer, company phone, etc.) carried out without his presence and with his knowledge . and at [his] workplace", he expressed his concern about the risk of falsification of the personal files he kept on his computer and requested to be summoned by the audited company to attend any inspection regarding the objects located at his workplace, but also during the control of the "electronic means of communication" that he handled as an employee, in order to make the legal and necessary separation of his personal from the purely professional files. On ... the owner-shareholder of the audited company B submitted before the TA subpoena against unknown perpetrators for removal and possibly falsification of documents in physical and electronic form response to the out-of-court response of the audited company, the complainant with the out-of-court declaration-protest requested that "personal items and data within the company" be attributed to him. The audited company submitted on ... before the Single-Member Court of First Instance of Athens an application for injunctive measures against the complainant to maintain the granted temporary injunction prohibiting the alteration of his property, the granting of permission for the preventive seizure of all movable and immovable property and the issuance of a court order escrow of the complainant's works of art. On the above request, the no. ... decision of the Single-Member Court of First Instance of Athens by which the related request was rejected as inadmissible due to vagueness "given that it does not mention, in a specific and individualized manner, what constitutes the urgent situation or the imminent danger, which make necessary at the present time the taking the requested security measures". The complainant on ... submitted his complaint against the mentioned as legal representative of the controlled company and B, 24 owner-shareholder of the same company for the criminal offenses of articles 22 par. 4 of Law 3472/1997 and 370A PK. 17. The complainant with his supplementary memorandum dated 14-12-2018 (ADPCH no. prot. C/EIS/10.117/14.12.2018) repeats his original complaint (APDPCh no. prot. C/EIS/7748/01.10. 2018) and in particular that he was never informed about the control of the "electronic means of communication handled by him as general manager", that the

audited company does not have any privacy policy, breach incident management policy, internal regulation for the correct use and operation of the equipment and the network information technology and communications by the employees, that they have not been informed of their rights from the processing of personal data, nor has their legal consent been secured for the processing of these by the company. It also maintains that the audited company did not have an overriding legal interest, nor was there any reason for urgency, in order to carry out a control of the complainant's personal data and that it overlooked other apparently available milder means. In his memorandum from 12-02-2019 with a hearing (ADDPH no. prot. 1178/12.02.2019) the complainant repeats the above complaints and clarifies that "[...] while I also objected to any control of my personal data (let alone without my presence!), requesting that any control be limited to my purely professional files..." (p. 6) as well as that "[...] From the moment I had informed the accused through my extrajudicial I agree to attend any audit of corporate data after separating it from the data of a private nature that existed in the telecommunications systems..." (p. 16). 18. However, contrary to the complainant's claim that the company did not have internal policies for the management of employees' personal data, the use of electronic communication systems, etc., during the period in question, it appears from the documents that he initially presented the audited company with its memorandum from 12-02-2019 with hearing (APDPX 1176/12.02.2019) that it not only had an indicative Employee Handbook and related Policies (IT Systems & Security Policy 25 05.12.2012, 20.11 .2013, 19.6.2015), but also that these were signed by the complainant himself, who was aware of their content. After the above finding and the diametrically opposed positions of the parties on the issue, the Authority with the under no. prot. C/EX/4780/5.7.2019 and C/EX/4781/5.7.2019 in her documents requested further clarifications from the audited company as well as the complainant's views on the allegations and the evidence presented by the audited company, i.e. especially in relation to the allegation of the non-existence of internal corporate policies, which, however, were said to exist and were signed by the complainant himself. The audited company with its memorandum of 22-07-2019 (ADDPX 5110/22.07/2019) did not provide any evidence in relation to the time of supply, installation and operation of the video surveillance system, nor did it provide any relevant internal documentation of the legality of the system , as will be shown below. On the contrary, it provided additional material of its compliance with the legislation on personal data, from which it follows the prohibition of the use of their systems by employees for personal (non-corporate) purposes, as well as the possibility of searching the related systems and data for the purposes of investigating illegal acts and i.e. Policies which were similarly signed by the complainant (see Policy Manual of 02-01-2017 chapter D of the Code of Ethics) as well as the now complete Employee Regulations of 10-10-2007

approved by the complainant himself. Accordingly, the complainant in his memorandum of 22-7-2019 did not repeat the claims initially supported by him regarding the non-existence of policies and regulations of the company, he finally accepted the existence of the security policies signed by him, clarifying that he had not as general manager their responsibility (apparently their pension) but was responsible for implementing those approved by B (p. 10) and reiterated that "the accused do not provide any evidence to prove my previous lawful information and the securing of my consent » (p. 12). From all of the above it follows that, on the one hand, the audited company had in force and applied internal corporate policies and internal employee regulations according to art. 24 par. 1 and 2 GDPR (see also Petition Sec. 78 GDPR), according to the content of which the computing and communication company systems are provided only for professional purposes, their use for personal private purposes is prohibited, the company has the right to access the communications and personal data of employees for expressly provided reasons, among which the satisfaction of the necessary legal interest of the business that cannot be satisfied in any other way or the existence of a suspicion of committing a criminal offence. On the other hand, the complainant was aware of the above corporate policies and regulations, which he had signed and in fact, according to his statement, he was responsible for their implementation. Therefore, the claim of the complainant that he was unaware of the existence of the right of control and access to electronic files concerning him stored on the company's server cannot be accepted, in fact at the time when what he referred to as personal electronic records had been stored by him and had similarly been by the same is being processed in the company's IT and communication systems, without its knowledge and in fact in violation of the company's corporate rules and policies, which the complainant was not only aware of but was responsible for implementing, despite his initial denial before the Principle. In addition, the audited company, in its e-mail from ... via the Chairman-shareholder of B, informed the complainant in response to his e-mail from ... that an audit is being carried out in the company. But the complainant himself admits that he was aware of the general fact of the investigation, as can be seen from his out-of-court statement-protest from 20-9-2018 to the audited company ("[...] I was informed that searches within my office space and on my company personal computer..." In addition, from the same out-of-court statement-protest it appears that he requested to be summoned in order to be present during the control of the "electronic means of communication that he handled as an employee, in order to the legal and necessary separation of [his] personal from [his] purely professional records", but without exercising the rights of erasure, restriction of processing and opposition with the relevant extrajudicial statement, to which he later referred in the context of 01-10 -2018 complaint of 27 before the Authority (prot. no. APDPX G/EIS/7748/01.10.18), filling

in the corresponding fields of the form. On the contrary, with the above extra-judicial statement, Ms. complainant admissibly and validly exercised the right of access and information in relation to the personal data included in the electronic computer owned by the controlled company, which was used by the complainant as will be shown below. 19. Of the criteria accepted by the Authority with the no. 34/2018 decision (see also recitals no. 8-12 hereof) regarding the control of the employee's computer by the employer, and which both the complainant and the audited party refer to in support of their claims company, despite the fact that its reality is substantially different, in this case it appears that the audited company legally and in accordance with the provisions of articles 5 and 6 GDPR gained access to deleted electronic files that were recovered from its server and which included personal data of the complainant as: i. According to the company policies and employee regulations, on the one hand, the use of information and communication systems by employees for private purposes was prohibited, on the other hand, the right of the company and the possibility of conducting relevant controls were foreseen. It should be noted that in the context of this, the Authority does not examine the issue of the employer's obligation to make available the possibility of using storage space on the computer owned by it (cf. APDPX 61/2004) given that the controlled processing took place on the server (server) of the company and in any case is not the subject of the complaint. ii. The complainant, despite his initial allegations before the Authority, according to which the company lacked relevant internal policies and work regulations, not only was he aware of their content, but in addition, as its General Manager, he was responsible for their implementation and had signed. 28 iii. The controlled company's access to the recovered, not permanently deleted, electronic files that contained personal data of the complainant and their processing met the principles of article 5 par. 1 GDPR as: - it was provided for in the internal policies and work regulations with the knowledge of the complainant - the complainant knew that an investigation was being carried out against him and requested his presence without objecting to the control, without requesting the restriction of processing or the deletion of the personal data concerning him (cf. also ECtHR Libert v. France of 22-02- 2018 application no. 588/13 by which the employer's access to the employee's PC in his absence was deemed to be in accordance with Article 8 ECHR) - from the application no. ... from the 27-9-2018 affidavit of D, the complainant's secretary at the audited company, which was presented by the complainant, it appears that the audited company's claim to delete files from the server was not fake in order to carry out the audit server, but was responding to the fact that access to the server was denied for all employees until the end of the investigation (and not just the complainant), that an order was given to change the passwords for the server, that valuable documents and files were lost from the archives and had to be recovered, that there were bodyguards everywhere, private

police and B's personal guard, even patrol cars - the audited company had a legal right to block remote or close access of any person, including the complainant, in the electronic files that included personal data until the end of the audit in order not to jeopardize the conduct of the investigation (see No. 11.8 Code of Ethics of the International Labor Organization op. and APDPX 34/2018), taking into account the fact that the records were deleted - it served a defined, express and legal purpose, provided for in the internal policies and employee regulations, i.e. the control of the possible commission of criminal offenses against the company - the processing (control) did not receive country in the entirety of the complainant's electronic records, but only those identified and marked as 29 redacted, as those gathered the most suspected connection to the alleged illegal acts, in order to meet the principle of data minimization. It must be taken into account that the audited company, before the creation of suspicions against the complainant for the performance of alleged illegal acts, had not carried out an investigation and control of his electronic files (cf. ECtHR KÖPKE v. Germany of 05/10/2010, decision on of admissibility, no. pr. 420/07 p. 11). After creating suspicions against the complainant and establishing the existence of deleted files on the company server, the audited company decided that an on-site ad hoc investigation and control should take place only on the deleted electronic files of the complainant, while it was not found that in permanent, lasting and stable control of all files of the complainant or all employees (cf. ECHR KÖPKE op. p. p. 12) with the installation and permanent operation of electronic communication monitoring software (see respectively ECHR Barbulescu op.) - The control was not general, preventive, permanent and lasting, as in the cases of installation of monitoring software e.g. of electronic communications, but specific, targeted, on-site, of short duration and therefore in accordance with the principle of proportionality, without the Authority establishing the existence of a necessary, but less burdensome measure which could be chosen - The control, in accordance with the affidavit of the secretary of the complainant D (see above) was limited to the 2nd and 3rd floor of the controlled company and related to its server - the subsequently deleted files were initially collected and stored by the complainant in the company's systems, without his knowledge and in violation of the company's internal policies and employee regulations - the access and control of the electronic files was not carried out by the audited company by unqualified personnel e.g. by simply copying them, but by a third specialized company, based on a special methodology, technique and use of forensic tools which, according to its statement, are harmonized with international standards, so that the principle of safe processing is met and guarantees are also provided in terms of the process control 30 iv. The claim of the complainant according to which the access and control of the company's electronic files that included his personal data took place without his consent must be rejected, as the audited

company correctly applied the legal basis of art. 6 par. 1 sec. in the GDPR. However, even if the complainant had given his consent for the company to conduct checks on his electronic records, it would have been illegal due to an imbalance of power between employer and employee. As the Authority has already judged with reference to ECtHR jurisprudence and the Opinions of the Working Group no. 29 – current European Data Protection Board (see in detail GDPR 34/2018) the employer is entitled to process the personal data of employeesin the context of related controls without obtaining their consent if the processing in question is necessary for the purposes of the legitimate interests pursued, as in this case, the orderly operation of the business and the protection of its property (cf. CJEU C-13/ 16 Rigas decision of 04-5-2017 para. 29 where it was judged that the damage to the property and its restoration falls under the pursuit of legal interest) by ensuring the confirmation of evidence in the context of checking suspicions of committing illegal acts (see ECtHR KÖPKE op. . p. 1216, OE 29 WP 55, p. 18 ibid.). In this case, the decision to carry out a targeted audit (in accordance with the above) on the initially deleted and subsequently recovered electronic files of the complainant met the conditions for the legal application of the legal basis of processing for the purposes of the controller's superior legal interest pursuant to art. 6 par. 1 sec. in the GDPR, as it was necessary in order to protect the company's property and ensure the necessary evidentiary material, but without entering into the 16 "The domestic courts further gave weight to the fact that the employer, on the other hand, had a considerable interest in the protection of its property rights under Article 1 of Protocol no. 1. It must be considered essential for its employment relationship with the applicant, a person to whom it had entrusted the handling of a till, that it could rely on her not to steal money contained in that till. The Court further agrees with the labor courts' finding that the employer's interest in the protection of its property rights could only be effectively safeguarded if it could collect evidence in order to prove the applicant's criminal conduct in proceedings before the domestic courts and if it could keep the data collected until the final determination of the court proceedings brought by the applicant. This also served the public interest in the proper administration of justice by the domestic courts, which must be able to establish the truth as far as possible while respecting the Convention rights of all individuals concerned. Furthermore, the covert video surveillance of the applicant served to clear from suspicion other employees who were not guilty of any offense". 31 carrying out private investigative acts, which by law are exclusively reserved for the competent judicial-prosecution authorities and the services that act under their direct supervision and are characterized by secrecy in corresponding cases. It should be pointed out that, of course, the critical time for making the decision to carry out the audit is that of the appearance of the suspicions, which should be well-founded and sufficient. In

addition, the above-mentioned legal interest of the audited company was superior to the interest or the fundamental rights and freedoms of the complainant that require the protection of personal data, taking into account his legitimate expectations based on his relationship with the company (see App. Sk. 47 GDPR), as the relevant processing was aimed at protecting the company's property and investigating suspicions of alleged offenses by the complainant. Besides, as the ECtHR ruled in this regard in the Barbulescu case (see recital no. 12 above), the employee's expectation of non-intervention by the employer constitutes an important, but not necessarily, exclusive factor, so that any expectation of the non-investigation of the employee's electronic records (when it is carried out legally), from the processing of which may result in the commission of offenses against the company, to conflict and must be weighed against other fundamental rights, in accordance with the principle of proportionality, given that the relevant protection is not absolute (see Art. 4 GDPR). Otherwise, each data subject will invoke the protection of his personal data in order to avoid being held responsible. Likewise, it cannot be a legitimate expectation of the complainant not to investigate electronic files that include his personal data, when these are included in a system whose use for private-personal purposes, in accordance with the company's internal regulations and policies, appears to be known to him prohibited. Finally, it is taken into account that the control and access by the audited company took place in deleted files, which were recovered following the use of special forensics tools. 32 From the above it follows on the one hand that the general processing of personal data of the company's employees that took place on the server was in accordance with Articles 5 and 6 GDPR, on the other hand, that the processing specifically examined by the Authority in the context of the present complaint cumulatively fulfills the conditions of articles 5 and 6 par. 1 sec. in GDPR and, therefore, the processing (access and control) by the controlled company of the electronic files that were included in the company server (server) and contained personal data of the complainant was legal. 20. Regarding the complainant's exercise of the right to information and access, the following should be noted: The provisions of Articles 13 and 14 GDPR include the information provided by the data controller to the data subject when personal data is collected. In accordance with the provisions of article 15 para. 1 GDPR, the data subject has the right to receive from the data controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right of access to the personal data and the information detailed in the sub-cases of the said paragraph, while par. 3 of the same article stipulates that the controller provides the data subject with a copy of the personal data being processed. In order to satisfy the right to information and access, it is not necessary to invoke a legal interest or the related reasons since this exists and is the basis of the subject's right of access in order to obtain

knowledge of information concerning him and which have been registered in a file, which is kept by the data controller, so that the basic principle of the law for the protection of personal data is carried out, which consists in the transparency of the processing as a condition for any further control of its legality on the part of the data subject (see GDPR 16/2017). 33 If the data controller does not act on the data subject's request, he shall inform the data subject within one month of receiving the request of the reasons why he did not act and of the possibility of submitting a complaint to a supervisory authority and bringing legal action (Article 12 par. 4 GDPR). It is pointed out that even when the data controller does not keep a record of the subject's data, he is not exempted for this reason from his obligation to respond even negatively to a relevant request for information and access (StE 2627/2017). In addition, the data subject has no obligation to indicate to the data controller which of his data are specifically kept, in order to exercise the right of access and information, as in that case the burden of maintaining the record is reversed and impermissibly transferred (StE 3154/2017) and therefore the obligation of accountability according to art. 5 par. 2 GDPR. Finally, according to paragraph 4 of article 13 GDPR the obligation to inform according to paragraphs 1-3 does not apply when and as long as the data subject already has the information (see also Petition 62 GDPR) In this case, the controlled company violated the complainant's right to information and access in relation to the personal data it kept on the computer used by the complainant. In particular, the complainant with his out-of-court statement-protest from 20-9-2018 and especially from 28-9-2018 requested access to the personal data kept in the personal files that were stored on the computer he used and belonged to the company. It should be noted that the Authority ruled above (par. 19) that the control carried out by the company concerned the electronic files that were stored on the company's server and therefore in that case no violation of the right of access and information was found during the elaborately extrapolated. The audited company with the out-of-court response to the complainant, on the one hand, did not provide any specific information in relation to therequest for access and information, on the other hand, he replied that "Therefore, you have received all your personal items and have not left anything with the company, 34 on the contrary, you must give us an account of the documents you have transferred into your possession." From the above response of the audited company, it follows that the latter considered that the complainant's personal data files no longer exist because he received them himself and transferred them outside the company, moreover, he did not specify whether he was referring to the files kept on his personal computer that used by the complainant. In any case, the above response does not constitute satisfaction of the right of access, moreover, the audited company did not respond at all to the same request of the complainant, which was submitted through his ... out-of-court statement-protest, nor

did it inform him of the art. 12 para. 4 GDPR his rights (possibility of submitting a complaint to a supervisory authority and bringing legal action). The above is not negated by the statement of the audited company during its hearing before the Authority (see APDPX 1176/12-02-2019 its Memorandum, p. 8) according to which "During the proceedings conducted before you, on 23/ 1/2019 we clarified, (a) that the applicant's PC is at his disposal at all times, in order to establish whether there is any personal data of his". Therefore, the audited company violated the provisions of articles 12, 13 and 15 GDPR. 21. The complainant claims that the audited company installed a video surveillance system (closed circuit cameras) in the facilities where it worked, without a permit from the Authority during the period of validity of Law 2472/1997 but also continued to operate it after 25-5-2018, when the GDPR came into force according to art. 99, without the legal conditions of processing in violation of those defined by Directive 1/2011 of the Authority as well as under no. 5/2017 Her opinion. In addition, according to the same complaint, through the illegally installed video surveillance system, he recorded the complainant and subsequently proceeds with further illegal processing of said material by presenting it before courts, the Authority in the context of the present proceedings, etc. According to ESPD Guidelines 3/2019 in order to judge the legality of the installation and operation of the system, the conditions of articles 5 and 6 par. 1 GDPR must be cumulatively met 35, it should be prior to the installation and operation of the system to document the legality of the processing internally, 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. Every audited company is obliged, within the framework of the principle of accountability, to prove in principle the legality of the installation and operation of the video surveillance system. A critical element is the time of installation of the system, as if it has been installed and operated before 25-5-2018 it should have been notified to the Authority in accordance with article 10 par. 1 of Directive 1/2011 APDPH in combination with article 6 n. 2472/1997, and in case the processing concerned sensitive personal data, permission from the Authority was required according to art. 7 par. 2 of Law 2472/1997. In this case, the audited company, in violation of the principle of accountability, failed to prove the legality of the installation and operation of the video surveillance system, as in principle it did not provide documents (e.g. invoices, receipts) or other documents (e.g. responsible declarations of the installer) from which the time of purchase, installation and operation of the system can be proven, moreover, she avoided in her memoranda to specify the time of installation and operation of the system, which would result in the obligation to notify or not to the Authority of the installation and operation of the system under the rule of Law 2472/1997. Also, the audited company did not provide information on the number of cameras included in the system, on their technical

capabilities, on the way of recording and maintaining the recording material, nor on the exact places where the cameras are placed, while it did not provide any relevant evidence element. In addition, from the Registry of Files and Processing maintained by the Authority pursuant to art. 19 par. 4 para. a' of Law 2472/1997 it appears that the audited company had not notified the Authority of the installation and operation of a video surveillance system. Also, from the complainant's memorandum (APDPX no. prot. 1178/12-02-2019) it appears that "Regarding the installation of the video surveillance systems, which are present in almost all areas of the company (even in the cafeteria), in obvious and hidden points (!), I clarify that 36 have been installed since the year 2007, which B also confessed before you and that these are recording cameras with extended capabilities" (p. 31). It should also be noted that the audited company provided a fragmentary translation into Greek from English as relevant 1A in its Memorandum (APDPH no. pr. 1176/12-02-2018) part of the "employee information manual for the processing of personnel data nature" with reference to "the collection and processing of personal data through closed circuit television (CCTV) carried out in accordance with the company's security policies and procedures in compliance with the Regulation (EU 2016/679) and the requirements of Greek legislation", in it did not include the original part in the English language, although the Authority with no. C/EX/4781/5.7.2019 document requested from the controlled company relevant clarifications, which were not provided. The fact of the complainant's prior knowledge of the installation of the system and the recording of its image (even of what he refers to as hidden cameras) does not negate the admission of a violation of the above provisions. However, even if the complainant had given his consent, it would not be free and valid due to the imbalance of power between employer and employee. Consequently, the audited company operated an illegal video surveillance system, as it did not carry out internal documentation of the legality of the relevant operation in accordance with the principle of accountability under Art. 5 par. 2 GDPR and for this reason did not bring to the attention of the Authority relevant written documentation of the legal operation of the system pursuant to art. 5 and 6 GDPR, but also Directive 1/2011 GDPR, but neither the provided corporate policies or employee regulations include any relevant provision, in order to demonstrate compliance with Articles 5 and 6 GDPR in combination with the provisions of Directive 1/2011 APDPH. Given that overall the installation and operation of the video surveillance system to date violated Art. 5 par. 1 sec. 1 GDPR the principle of legality as well as the principle of accountability according to art. 5 par. 2 GDPR, the examination of the other principles of processing of the same article, the application of the principle of proportionality as well as the examination of the application of the 37 appropriate legal basis according to art. 6 par. 1 GDPR in combination with the provisions of Directive 1/2011 GDPR. Finally,

given that the installation and operation of the video surveillance system, through which relevant visual material containing personal data (the image and recorded activity of the complainant) was collected, was illegal according to the above, it is submitted that any subsequent or even further (i.e. with a different purpose) discrete and independent processing of the same personal data such as copying and storing them on another digital storage medium (e.g. usb stick, server, pc, etc.), their transmission and use, such as the latter was carried out by presenting the relevant material before the Authority, violated the provisions of no. 9A S. Therefore, in order to issue this decision, the Authority does not take into account and does not evaluate evidence according to art. 19 par. 3 S. the relevant material presented during the hearing (without objection by the complainant) and subsequently presented by the audited company in printed form (prints of photographs), nor any direct or indirect reference to it (cf. STE 3922/ 2005 and Supreme Court [All] 734/2008). 22. Finally, on the allegations submitted by the audited company and based on what was accepted above, the Authority: i. It rejects the claim that it had a right to control and access the complainant's electronic files because the IT and communications systems were owned by it and therefore that the related electronic files (especially the e-mails) are also owned by it, according to what were mentioned above in no. 8 recitalof the present. ii. It rejects the claim that the complainant was burdened with the obligation to take the appropriate organizational and technical measures for the security of the data, because he himself took care of the security policies which he signed and that he was in essence (de facto) the Data Protection Officer (YPD) of the audited company as: From the Authority's register it appears that the audited company never announced according to art. 37 par. 7 GDPR the definition of the complainant as a DPO. However, even if the complainant had been appointed as DPO, the coincidence of the General Director's status with 38 that of DPO would violate the provisions of Article 38 para. 3 GDPR on the independence of DPO and Article 38 para. 6 final sec. GDPR on conflict of interest (see OE 29 Guidelines for the data protection officer, op. p. 22). In any case, the responsibility for the definition of the DPO and therefore the relevant responsibility for compliance with the requirements of the GDPR rests with the data controller, who alone is imposed by the Authority the relevant administrative sanctions according to art. 83 par. 4 para. a GDPR, so that the relevant claim is unfounded but also invalid. 23. 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 infringements, or if the potential fine would impose a disproportionate burden on an individual, a reprimand could be imposed instead of a fine. The Authority after establishing the

violation of the provisions of the GDPR in accordance with the above, taking into account in addition, in addition to the above, in particular: The Guidelines for the implementation and determination of administrative fines for the purposes of Regulation 2016/679 issued on 03-10 - 2017 by the Working Group of Article 29 (WP 253) and after having duly taken into account the provisions of Articles 58 para. 2 and 83 GDPR to the extent that they are applied in the specific case and in particular those of the criteria provided by paragraph 2 of the same article concern the specific case examined by the Authority: A. Regarding the case of violation of Articles 12, 13 and 15 GDPR in relation to the violation of the right to information and access, the Authority after taking into account a) the nature, gravity and the duration of the breach, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the amount of damage suffered and specifically: i. the fact that the company violated the right of one (1) data subject regarding the updating and access of his personal data stored on a computer owned by the company, without its knowledge and in violation of its internal policies and regulations ii. the fact that from the provisions of article 83 par. 5 para. b of the GDPR it follows that the violation of the rights of the subjects falls under the higher prescribed category of the classification system of administrative fines, if it is deemed necessary to impose them, except in this case it is not a violation due to data processing (cf. article 58 par. 2 para. a' and b' GDPR) but about non-satisfaction of the right to information and access of one (1) subject, so that the related violation is judged to be less serious and minor duration iii. The fact that, from the information brought to the attention of the Authority, no material damage occurred to the data subject – the complainant from the non-satisfaction of his right, nor did the complainant claim relevant damage b) the fraud or negligence that caused the violation From the out-of-court response of the audited company to the complainant, it appears that in response to the complainant's request for access and information, he understood that "Therefore, you have received all your personal items and have not left anything with the company, on the contrary, you must hold us accountable as to the documents which you have transferred into your possession.' From this answer, which was already judged to be unsatisfactory, it follows that the audited company, considering that the complainant's personal data no longer exists on its computer, wrongly did not provide a satisfactory answer, even a negative one. In view of the 40 above, the unsatisfactory answer provided was the result of insufficient knowledge and application of the provisions of the GDPR and is therefore attributed to negligence. c) any actions taken by the controller to mitigate the damage suffered by the data subjects and d) as to the degree of cooperation with the Authority to remedy the breach and limit its possible adverse effects In addition to that as mentioned above no material damage was found to the complainant from the violation of the right

of access and information, nor was such a claim invoked by the complainant, the audited company with its hearing memorandum before the Authority (APDPH no. first 1176/12-02-2019) stated: "During the procedure conducted before you, on 23/1/2019, we clarified, (a) that the applicant's PC is at his disposal at all times, in order to establish whether his personal data exists." The above statement, which the Authority recognizes as a mitigating circumstance, constitutes sufficient action in order to satisfy even later the complainant's already violated right to information and access, regardless of whether the latter responded to the relevant invitation. e) with regard to any relevant previous violations of the data controller, it follows from a relevant check that no administrative sanction has been imposed by the Authority to date f) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as the financial benefits that were obtained or damages avoided, directly or indirectly, from the violation The Authority, in addition to the above, recognizes as an additional mitigating circumstance from the elements brought to its attention and on the basis of which it established the violation of the right to information and access, that on the one hand the person responsible processing did not obtain a financial benefit, nor did it cause material damage to the data subject, on the one hand, that the personal data in question were stored by the complainant on a computer owned by the audited company, without its knowledge and in violation of the internal policies and work regulations her. B. Regarding the case of illegal installation and operation of a video surveillance system as well as the subsequent or further processing of the material in violation of the principle of legality according to art. 5 par. 1 sec. 1 GDPR as well as the principle of accountability according to art. 5 para. 2 GDPR, in conjunction with the provisions of Directive 1/2011 GDPR, the Authority after taking into account: a) the nature, gravity and duration of the violation, taking into account 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, specifically: i. the fact that the company violated the provisions of article 5 par. 1 sec. 1 GDPR principles of legality, objectivity and transparency as well as the obligation (principle) of accountability according to art. 5 para. 2 GDPR, i.e. violated fundamental principles of the GDPR for the protection of personal data ii. the fact that the observance of the principles provided by the provisions of article 5 par. 1 sec. a' and par. 2 GDPR is of capital importance, primarily, the principle of legality, so that if it 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 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 data controller, who has been provided by the GDPR with the necessary compliance tools iii. the fact that the controller failed

to comply with the requirements of the processing authorities of article 5 par. 1 sec. a' GDPR, moreover, failed to document in the context of internal compliance the legality of the video surveillance system and 42 inevitably also the subsequent or further processing of the same material iv. the fact that the violation of the above principles took place during the processing of personal data of subjects in the field oflabor relations, where it is characterized by an imbalance of power between employer and employees. The importance attached by the GDPR to the processing of personal data in employment relations is demonstrated by the fact that Article 88 thereof provides the national legislator with the possibility of establishing special rules in order to ensure the protection of the rights and freedoms of employees, including appropriate and specific measures to safeguard the human dignity, legitimate interests and fundamental rights of the data subject, with particular emphasis on processing transparency, intra-group data transmission and workplace monitoring systems. Therefore, the observance of the principles provided by article 5 par. 1 sec. a' and par. 2 GDPR acquires in this case a special and weighty importance for the respect of the right to the protection of the personal data of employees v. the fact that the violation of the above principles falls under the provisions of article 83 par. 5 sec. a' GDPR in the highest prescribed category of the classification system of administrative fines vi. the fact that the video surveillance system also included hidden cameras, regardless of the fact that the complainant was aware of their installation and operation vii. The fact that the illegal installation and operation of the video surveillance system lasted for a long time, according to what was accepted by this decision viii. The fact that, from the information brought to the attention of the Authority, no material damage occurred to the data subject – complainant 43 from the non-satisfaction of his right, nor was any related damage claimed ix. the fact that the violation of the principles of article 5 par. 1 sec. a' and par. 2 GDPR did not concern, based on the information brought to the attention of the Authority, personal data of articles 9 and 10 GDPR x. The fact that the violation of the principles of article 5 par. 1 sec. a' and par. 2 GDPR, in addition to the complainant, it concerned almost all the staff for the entire duration of their work, so that it is not an individual or opportunistic violation against some of the employees, but a violation that has a systemic (structural) nature as it concerns the controller's policy. b) the fraud or negligence that caused the violation According to the complainant's additional clarifications from ... (p. 10) he informed the owner-shareholder of the complained-about company about the need to comply with the GDPR and it is alleged that he convinced him with great difficulty in hiring compliance consultants, with whom it subsequently ceased working. In the context of the present procedure, the audited company submitted documents from which it appears that in the time before the complaint, they restarted GDPR compliance procedures. Therefore, the controller's installation and operation of

the video surveillance system as well as the subsequent or further processing of the same material in violation of the principle of legality and accountability was the result of insufficient knowledge and application of the provisions of the GDPR and, therefore, is attributed in negligence. c) any actions taken by the controller to mitigate the damage suffered by the data subjects and d) as to the degree of cooperation with the Authority to remedy the breach and limit its possible adverse effects 44 Beyond the presentation of documents in the context of the present procedure, from which it appears that the audited company took actions to comply with the requirements of the GDPR, it was not established that it took other actions to mitigate any (non-material) damage suffered by the complainant, such as e.g. to the deletion of the recording material. e) with regard to any relevant previous violations of the data controller, it follows from a relevant check that no administrative sanction has been imposed by the Authority to date f) the categories of personal data affected by the violation and in particular that it is not personal data of the articles 9 and 10 GDPR, according to the information brought to the attention of the Authority. THE AUTHORITY Having taken into account the above Because it decided according to art. 58 para. 2 GDPR exercising its corrective powers in the specific cases a' and b' for which a violation of the GDPR was found. Because he decided according to art. 58 par. 2 in combination with art. 83 para. 2 GDPR that in the first case for the exercise of corrective measures to achieve the purposes of compliance with the provisions of the GDPR, it is sufficient to impose the corrective measures of case c of para. 2 of article 58 GDPR, without the need to impose administrative fine. Because pursuant to the provision of article 58 par. 2 sec. 3 GDPR the Authority decided for the first case to instruct the company "ALLSEAS MARINE S.A." to comply with complainant A's request to exercise his right to access and be informed of the personal data stored on the company's proprietary computer, which was used by the complainant. 45 Because he decided according to art. 58 par. 2 in conjunction with art. 83 para. 2 GDPR that in case b for the exercise of corrective measures to achieve the purposes of compliance with the provisions of the GDPR, in addition to the imposition of the corrective measure of case d of para. 2 of article 58 GDPR, it also becomes necessary to impose administrative fine according to art. 58 par. 2 sec. i' in conjunction with Article 83 GDPR. Because pursuant to the provision of article 58 par. 2 sec. d GDPR the Authority decided for the second case to instruct the company "ALLSEAS MARINE S.A." to make the processing operations that take place through the video surveillance system it maintains compliant with the provisions of the GDPR. Because in particular with regard to case b', the company should restore the correct application of the provisions of article 5 par. 1 sec. a' and par. 2 of the GDPR in accordance with the considerations contained herein. Because in particular with regard to case b', the company should subsequently restore the correct

application of the other provisions of article 5 par. 1 sec. b-f GDPR to the extent that the identified violation affects the internal organization and compliance with the provisions of the GDPR, taking all necessary measures within the framework of the principle of accountability. Because the above order should be executed within one (1) month from the receipt of this, informing the Authority accordingly. Because in case b', the above corrective measure is not sufficient by itself to restore compliance with the violated provisions of the GDPR. Because the Authority considers that in this particular case, based on the circumstances established, it should, pursuant to the provision of article 58 par. 2 sec. i GDPR to impose an additional and effective, proportionate and dissuasive 46 administrative fine according to art. 83 GDPR, both to restore compliance and to punish this illegal behavior17. Because the violation found by the Authority of the provisions of article 5 of the GDPR falls under the provisions of article 83 par. 5 sec. 1 GDPR. FOR THESE REASONS THE AUTHORITY A. Orders the company "ALLSEAS MARINE S.A." to immediately comply with the request of the complainant A for the exercise of his right to access and update him on the personal data kept stored on the electronic computer owned by the company, which was used by the complainant, informing the Authority accordingly. B. Gives an order to the company "ALLSEAS MARINE S.A." as within one (1) month from the receipt of this notice, informing the Authority: i. to make the processing operations that take place through the video surveillance system it maintains compliant with the provisions of the GDPR. ii. to restore the correct application of the provisions of article 5 par. 1 sec. a' and par. 2 of the GDPR in accordance with the considerations contained herein. iii. to subsequently restore the correct application of the other provisions of article 5 par. 1 sec. b-f GDPR to the extent that the identified violation affects the internal organization and compliance with the provisions of the GDPR by taking all necessary measures within the framework of the principle of accountability. C. Enforces the company "ALLSEAS MARINE S.A." the effective, proportionate and dissuasive administrative fine appropriate to the 17 See OE 29, Guidelines and the application and determination of administrative fines for the purposes of regulation 2016/679 WP253, p. 6 47 specified under B' case in accordance with its more specific circumstances,

in the amount of fifteen thousand (15,000.00) euros.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou