GREEK REPUBLIC PERSONAL DATA PROTECTION AUTHORITY Athens, 12-19-2019 Prot. No.: G/EX/8907/12-19-2019 A P O F A S I NO. 44 /2019 (Department) The Personnel Data Protection Authority Charaktira met as a Department composition at its headquarters on Wednesday, July 24, 2019 at the invitation of its President, in order to examine the case referred to in the present history. Georgios Batzalexis, Deputy President, in the absence of the President of the Authority, Constantinos Menoudakos, attended, the alternate members Panagiotis Rontogiannis, Grigorios Tsolias as rapporteur, and Evangelos Papakonstantinou, replacing the regular members Antonios Symvonis, Charalambos Anthopoulos and Konstantinos Lambrinoudakis who, although elected legally in writing, they did not attend due to disability. The meeting was attended by order of the President, Georgios Rousopoulos, specialist scientist - auditor as assistant rapporteur and Irini Papageorgopoulou, employee of the Administrative Department of the Authority, as secretary, while the other assistant rapporteur, Eumorfia - Iosifina Tsakiridou, did not attend due to disability. expert scientist examiner. The Authority took into account the following: The company AEGEAN BUNKERING SERVICES INC (hereinafter "ABS") submitted to the Authority the personal data breach incident number C/EIS/5432/18-06-2018, according to art. 33 of Regulation (EU) 2016/679 (General Data Protection Regulation - hereinafter "GDPR") together with additional 1-3 Kifisias St., 11523 Athens, Tel.: 210-6475600, Fax: 210-6475628, contact@ dpa.gr, www.dpa.gr memorandum. At the same time, the same company submitted its report No. G/EIS/5414/18-06-2018 (itself described it as a complaint) regarding a breach of personal data against the companies Aegean Marine Petroleum Network Inc (hereinafter " AMPNI") and ERNST & YOUNG HELLAS CERTIFIED AUDITORS-ACCOUNTANTS (hereinafter "EY HELLAS"), with which he claims that persons related to the above two companies entered ABS space (data room) without right and illegally copied on portable media storing all the digital content of the server which contains electronic files as well as e-mails and other communications of both ABS employees with third parties and employees of third parties by "cloning" the original server and thus creating a new file (clone server) by copying the original server (server). With the under no. 2/2018 Temporary Order of its President (prot. no. C/EX/5432-1/22-06-2018), the Authority banned, until the issuance of a final decision, AMPNI and EY HELLAS as well as any other company or natural person to whom all or part of the copied file mentioned in the case (clone server) was transmitted, to process in any way the personal data and in particular the e-mails included in the copied file (server) which were attached as list at the end of the said Interim Order forming an integral part thereof. It should be noted that with the same decision it was clarified that the above provision suspending the processing of the personal data contained in the clone server does not prevent the continuation of

the operation of the original server of the same company, under the self-evident condition of course that the processing of personal data takes place legally under no. 5 and 6 par. 1 GDPR. The Authority with no. prot. C/EX/5414-1/26-6-2018 her document invited the companies AMRNI, ABS and EY HELLAS to provide information as well as to provide specific documents as well as any necessary information for making a final decision on the case under consideration. On the above document: i. The EY HELLAS company, with its Memorandum dated 28-6-2018 to the Authority (prot. no. APDPCH C/EIS/5824/29-6-2018) stated that it has nothing to do with the case under consideration, nor was it even aware of alleged illegal processing of personal data. In addition, she requested the revocation of the temporary order insofar as it concerns her as a non-involved party and requested to be excluded from 2 any investigation or audit carried out by the Authority in relation to the case in question. The Authority requested further clarifications from the company in question with its document No. G/EX/5824-1/06-07-2018, in particular in relation to two persons who allegedly declared themselves representatives of the company "Ernst & Young" and are involved in server replication. EY HELLAS responded with its document No. C/EIS/6424/24-07-2018 denying any relationship with the natural persons in question. ii. The company ABS with its report of 28-6-2018 (prot. no. C/EIS/5825/29/06/2018) and its letter of 03-7-2018 (prot. no. C/EIS/5935 /04-07- 2018) presented documents to the Authority, among which the Policies of an organization with the name "AEGEAN", which did not bear the date of drafting and implementation, did not bear the signatures of competent persons for the drafting and approval, while with the same document the company provided information in response to the Authority's questions. iii. The company AMPNI with the Treatment Application of 13-7-2018 (no. APDPX prot. C/EIS/6211/13-7-2018) requested the cancellation and suspension of validity, in whole or in part, of the Temporary Order no. . 2/2018 of the President of the Authority for the reasons detailed therein. In that application, the company denied all allegations made against it by the complainant ABS, pointed out that ABS had been a wholly-owned subsidiary of ABS and claimed, among other things, that it had lawfully gained access to the e-mail accounts of certain current or former employees. AMPNI Group as well as other relevant data in the context of an internal investigation in relation to important financial matters of the company, including suspected fraud against the company, that access to them was necessary in order for the company to be able to comply with its obligations regarding the submission reports and disclosures to the US Securities and Exchange Commission (SEC) under applicable laws and regulations, including US securities law and New York Stock Exchange regulations, as well as in order to protect the Group from further damage and loss of data, the that the internal investigation being carried out has been obstructed by persons who are

suspected of possessing important information in relation to the matters of internal control, that the extracted e-mails were professional (corporate) and therefore do not constitute personal data, that there was to download a backup copy (back up) of all system data, i.e. also data concerning employees of third-party companies who used the same server 3 (server) because the installation and operation of deletion software was found and therefore the said processing was absolutely necessary to to protect the integrity of the AMRNI Group's data from those who attempted to destroy them without authorization, that the data in question coming from the searched e-mail is necessary for the external auditors PriwaterhouseCoopersS.A. (“PwC”) in order to sign the company's annual report for the financial year 2017. Furthermore, 11 complaints by natural persons were submitted to the Authority against AMPNI and EY HELLAS and in relation to the above-mentioned incident, namely the no. prot. C/EIS/5648/26-06-2018, C/EIS/5650/26-06-2018, C/EIS/5651/26-06-2018, C/EIS/5653/26-06-2018, C/EIS/5679/26-06-2018, C/EIS/5680/26- 06-2018, C/EIS/5681/26-06-2018, C/EIS/5682/26-06-2018, C/ IES/5683/26-06-2018, C/EIS/5684/26-06-2018 and C/EIS/5685/26-06-2018, complaints by A, B, C, D, E, F, Z, H, Θ, I and K respectively, who appealed to the Authority for a violation of their personal data that was kept on the original server and which was illegally copied in its entirety by the controlled company AMPNI given that some of the complainants there were employees of third-party companies, unrelated to AMPNI and its Group companies, such as D and I worked for "AEGEAN OIL", the K worked at "AEGEAN NET FUELS", Z worked at "AEGEAN PETROLEUM INTERNATIONAL", and B worked at "AEGEAN SHIPPING MANAGEMENT" The Authority, after studying the above answers and the attached documents, sent: i. to the company AMPNI with no. prot. C/EX/6211-1/14-8-2018 document in which he invited her to provide additional clarifications and informed her about the complaints submitted against her, in order to state her views on them. ii. to ABS company with no. prot. C/EX/5935-1/16-8-2018 document by which she was invited to provide additional clarifications and documents.The company ABS with its Supplementary Memorandum dated 11-9-2018 to the Authority (prot. no. APDPX C/EIS/7522/20-9-2018) provided additional clarifications and documents and in particular: that the initially submitted security policies were drawn up outside the EU in the USA and are applied to AMPNI and its subsidiaries, that in the internal work regulations of AMPNI's subsidiaries in Greece there is no reference to the control of employees' corporate e-mails or the 4 way that the company can carry out internal checks under the sole responsibility of AMPNI, that on the original server, the content of which was illegally copied by AMPNI, personal data of third companies to the AMPNI Group was kept, such as indicative of the companies "Aegean Net Fuels Ltd Fze", "Aegeon Oil A .E.”, “Aegean Lubes” and “Aegean Gas”, that all the above companies, together with ABS,

AMPNI and its subsidiaries use informally and without any written contract the infrastructure and servers of the ABS company and provided relevant written documentation. The company AMPNI with its documents dated 10-09-2018 (…) and 17-9-2018 (…) (no. prot. -9-2018 respectively) provided additional clarifications and in particular that: The server from which data was extracted is located in the computer room on the ground floor of the building on Aktis Kondili, in which the companies of the AMPNI Group lease space for their facilities. In the computer room, as far as the audited company knows, in addition to the server, there are also servers of other companies whose offices are housed in the same building, which are not related to the AMPNI Group. AMPNI Group does not have access to said servers. Also the audited company argued that the server really belongs to the AMPNI group, it is owned by the complainant ABS, which however does not process personal data on behalf of AMPNI, repeated its claims of legal and necessary data processing for the purposes of its internal investigation and on the occasion of the accidental detection with approved erasure software in order to protect AMPNI Group data, which was not personal and therefore no breach had taken place, that any extraction of personal data by EY LLP took place by downloading appropriate measures to secure the data, that the extraction of e-mails concerned a limited number of persons, that the EY LLP team did not gain physical access to the server, that the local AMPNI Group IT staff created five (5) accounts for the members of the EY LLP team in order for them to have access to AMPNI's systems, that he did not inform previously the persons whose electronic accounts were checked and access was gained by copying the server in order to avoid the risk of preventing or obstructing the investigation no. 14 par. 5 sec. b GDPR, that legally and pursuant to article 6 par. 1 sec. c' and in the GDPR the processing of the data took place through the 5 copying of the server, and that the copied file is located at the offices of EY in Manchester, United Kingdom. The AMRNI company, with its application dated 10-10-2018 (ADPPH no. prot. C/EIS/8044/11-10-2018) requested the urgent consideration of its request for the removal of the under no. 2/18 of a Temporary Order citing the US Department of Justice's subpoena of her before a Grand Jury in connection with an official criminal investigation for a possible criminal offense, in the context of which (subpoena) she was ordered to ship to the US and testify competently, until on ..., data concerning, among other things, e-mails included in what it refers to as a "back up", the processing of which has been prohibited by the Authority until its final decision is issued. In particular, with its above application, the AMRNI company repeats the allegations it develops in its Treatment Application dated 13-7-2018 arguing that the professional (corporate) email accounts were legally extracted and therefore the no. 2/18 Temporary Order to then forward the data (e-mail) to the U.S. The Authority proceeded with a summons for the hearing of the companies ABS, AMPNI and EY

HELLAS with the first cases No. C/EX/8303/18-10-2018, C/EX/8302/18-10-2018 and /8301/18-10-2018 documents, respectively, while with No. 3 Temporary Order of the President of the Authority (No. Prot. C/EX/8345/19.10.2018), he rejected the request for treatment – revocation of the no. 2/2018 Temporary Order considering that a condition for cross-border transfer of personal data to the U.S. recommends compliance with the general principles of processing, i.e. Articles 5 and 6 GDPR, so that in case the data subject to cross-border transmission has been collected illegally, their cross-border transmission is prohibited. During the meeting of the Authority's department on 07-11-2018, lawyers Panagiotis Bernitsas with AMDSA ..., Marina Androulakakis with AMDSA ... and Areti - Tania Patsalia with AMDSA ... attended on behalf of AMPNI. L, legal representative of ABS, also attended, stating that he is represented by lawyer Leonidas Kotsali with AMDSA.... Lawyer Eleftheria Rizou with AMDSA appeared on behalf of the complainants. At the meeting, AMPNI submitted documents No. C/EIS/8790/07-11-2018 and C/EIS/8791/07-11-2018, from which it appears that the Board of Directors of ABS, by decision of ..., decided that the legal representative of the company L is not authorized to appoint or relieve 6 lawyers from their duties, dismissed the lawyer L. Kotsali until then and appointed P. Bernitsa and H. Anagnostopoulos as the company's new lawyers. An objection was also filed by the lawyer P. Bernitsa against the representation of the ABS company by L and the lawyer L. Kotsalis (prot. no. C/EIS/8816/08-11-2018). The Authority adjourned the hearing of the case in order to consider the issue of ABS representation. Following ABS document No. G/EIS/9207/21-11-2018 from which it appears that the Board of Directors of the company replaced ... its representative with M the Authority proceeded with new calls of the companies ABS, AMPNI and EY HELLAS with the first numbers C/EX/9445/27-11-2018, C/EX/9449 /27-11-2018 and G/EX/9448/27-11-2018 its documents. Furthermore, the former legal representative of ABS N. L filed the complaint No. G/EIS/9771/04-12-2018, claiming that his personal data was also affected by the incident. At the meeting of the Authority's department on 05-12-2018, the lawyers Panagiotis Bernitsas with AMDSA ..., Marina Androulakakis with AMDSA ... and Areti - Tania Patsalia with AMDSA ... attended on behalf of the companies AMPNI and ABS, on behalf of the company ERNST & YANG (GREECE) CERTIFIED ACCOUNTANTS S.A. Ioli Katsirouba with AMDSP ... and Alexandra Vraka with AMDSA .... Complainants L and F were represented by Leonidas Kotsalis with AMDSA ... while Eleftheria Rizou with AMDSA appeared on behalf of the other complainants. It is noted that after the meeting the companies ABS and AMPNI submitted the petition no. 42/2019 decision of the Authority. The representatives of the companies and the complainants were given a deadline and filed briefs. In particular: i) EY HELLAS filed the document No. G/EIS/10252/19-12-2018, with which they repeat their claims, that it has nothing to do

with the case. ii) The companies AMPNI and ABS submitted the memorandum No. C/EIS/10259/19-12-2018, which was supplemented by the memorandum No. C/EIS/10398/28-12-2018 document while with the first letter No. C/EIS/10316/24-12-2018 they expressed objections to the extension of the deadline for submission of briefs until 15-01-2019, for which the Authority's department decided and overall for the procedure followed. In particular, the company ABS during the hearing process, but also with its above memorandum, withdrew the complaint against AMPNI and was jointly represented with ABS. Subsequently, he invoked the following claims: by decision 7 of the US court, the adoption of any measures against the bankruptcy estate of AMPNI is automatically suspended worldwide and therefore the proceedings before the Authority against the company should also be suspended, that ABS's complaint is inadmissible as it was exercised by a legal person and not a natural person in violation of Article 77 para. 1 GDPR, that the complaints of natural persons are inadmissible as the relevant rights were not exercised before the data controller, that the GDPR does not apply in the case of AMPNI as it has not establishment in Greece, that it had the right to carry out an internal audit on professional e-mails that do not comply with the protection of the legislation on personal data, that the processingof e-mails was necessary for the purposes of the legal interests of AMPNI no. 6 par. 1 sec. to the GDPR, that it refers to the documents and information that ABS had provided as a complainant against AMPNI, before withdrawing the complaint, that the company's e-mails are the property of AMPNI, that in the context of the internal investigation it was decided to copy the e-mails of specific persons, but during the process of copying them, the software function of deleting the entire server appeared and the company was forced to make a complete copy of it by creating a backup copy (back up) so that there was no time to update the data subjects beforehand, that although the finding of the operation of the deletion software constitutes a violation of personal data, there was no obligation on the part of the company to notify the Authority because it did not concern personal data but corporate (professional) e-mails and therefore no reasonable expectation could be created for the employees privacy, otherwise the necessary security measures were taken that even if the corporate e-mails constitute personal data, it was not proven that there was personal data in them, that no access was attempted to the personal (private) e-mail accounts of the employees in question but they were extracted from the company's server, and that in the case of the Novartis case, the Authority had judged that there was a legitimate interest in complying with the request of the US public authorities and granted permission to transmit the relevant data to the US, that it should take cognizance of any new evidence presented by the complainants, that it would not there was an obligation to inform the former and current employees of the AMPNI Group and finally that in the event of administrative

sanctions by the Authority not to order the destruction of the copied material as it includes critical documents and information in order to be handed over to the US authorities. 8 iii) The eleven original complainants jointly filed the memorandum No. C/EIS/268/15-01-2019, while L filed the No. C/EIS/272/15-01 - 2019 memorandum, in which it is argued that: AMPNI never submitted to ABS a request for access to personal data in a legal way, but preferred direct contact with Mr. N, ... , with a proposal of complicity in illegal acts, even offering him amnesty, that the finding of the existence of deletion software does not correspond to reality but was a pretext to justify the copying of the entire server given that from electronic letters between N and X an employee of EY LLP it appears that the copying of the entire server had been requested) several days before the detection of deletion software operation, that corporate data always contain personal data, that professional e-mails include personal data in accordance with the CJEU jurisprudence, that the same ownership and possession of a server does not imply the ownership of the personal data contained in the server, that no data has been separated and that no processing contracts have ever been signed no. 28 GDPR, that none of the principles of Article 5 GDPR have been observed so that the processing is unlawful and that AMPNI's claims for not informing the subjects was contradictory. After the filing of the memoranda, AMPNI and ABS informed the Authority (G/EIS/452/22-01-2019) that they are in the process of relocation and that the company "Apothekis Aigeiou AEVE", with which they shared facilities, will not delivers the original hard disk of the ABS server in operation, despite the fact that it was not part of the Authority's temporary order, as confirmed by the Authority with the original number C/EX/452-1/29 -01-2019 her document. According to the companies AMPNI and ABS, the processing of the backup copy (back up) located in Manchester, United Kingdom and containing professional e-mails, is the only way to ensure that key evidence will not be permanently destroyed and any decision of the Authority ordering the destruction of the backed-up business e-mails for any reason would be disproportionate and would irreparably interfere with AMPNI Group's property and defense rights. As informed by AMPNI and ABS (C/EIS/757/30-01-2019) the relevant request was discussed at the Piraeus Magistrate's Court with an injunction procedure, initially with 9 issuance of a temporary order (see C/EIS/757/30-01-2019). Finally, as the Authority was informed with the document No. C/EIS/2883/16-04-2019 of AMNPI and ABS, the aforementioned court issued its decision No. 14/2019, ordering the return of the mobile equipment at ABS. On this issue, the AEGEAN WAREHOUSE company filed the request No. C/EIS/2111/19-03-2019 requesting to clarify whether the performance of the servers includes their content, i.e. the personal data - stored e-mails, while the Authority, with document no. prot. No. 2/2018 and 3/2018 Temporary Orders, but they concern matters of interpretation and execution of the ... Decision of the Piraeus

Magistrate's Court which do not fall under the competence of the Authority. AMPNI and ABS also filed a series of documents related to the active proceedings in a US bankruptcy court. and in particular a) under No. C/EIS/740/30-01-2019 entitled "NOTICE OF DEADLINE REQUIRING SUBMISSION OF PROOFS OF CLAIM ON OR BEFORE 21-02-2019" b) under No. C/EIS/1467/25-02-2019 entitled "NOTICE OF HEARING TO CONSIDER CONFIRMATION OF THE CHAPTER 11 PLAN FILED BY THE DEBTORS AND RELATED VOTING AND OBJECTION DEADLINES", c) under No. C/EIS/ 2678/09-04-2019 entitled "NOTICE OF (A) ENTRY OF ORDER CONFIRMING THE JOINT PLAN OF REORGANIZATION OF AEGEAN MARINE PETROLEUM NETWORC INC. AND ITS DEBTORS AFFILIATES PURSUANT TO CHAPTER 11 OF THE BANKRUPTCY CODE AND (B) OCCURRENCE OF EFFECTIVE DATE'. Finally, AMPNI and ABS, after (with the Authority's document no. prot. C/EX/2214/21-03-2019) became aware of the allegations of the complainants through the memoranda of 15-01-2019, they submitted the No. Prot. C/EIS/2616/05-04-2019 supplementary memorandum which in principle questions the legality of the extension of the deadline given for the submission of a memorandum after hearing. Subsequently, they argue, refuting the complainants' memorandum, that they did not carry out any illegal processing of personal data, that there was no intention from the beginning to copy the server, nor that they invented the existence of the deletion software as a justifying reason, that the purpose of of the procedure followed was the extraction of professional e-mails of a specified number of former and 10 current employees of the AMPNI group, that access to personal (private) e-mail accounts was not attempted, that some of the complainants only provide some e-mails that contain personal data them, that subsequent to the complaint, new information is presented concerning in particular electronic mail and exchange of e-mails from an address of PAE AEK, which is not included in the list of addresses attached to the temporary order 2/2018 of the Authority, that the complainants knew very well that their company e-mail accounts destination were for professional use only, that to the extent that the backup eventually contains personal data of natural persons not connected to the AMPNI group then the company would be willing to separate or delete the data concerning said natural persons, that the business e-mails are not personal data, that the copying of the original server was lawful due to force majeure due to the detection of the erasure software function and that personal correspondence should not have been exchanged through company e-mail accounts in the first place . The Authority, from the hearing procedure, from the elements of the case file, as well as from the memoranda submitted after the attached documents, after hearing the rapporteur and the clarifications of the assistant rapporteur G. Roussopoulos, who left after the debate and before from the conference and the decision-making, and 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 n.d. 53 of 19.9.1974, as it applies today and in particularthose 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 against Automatic Processing of Personal Data of 28.1.1981 ("Convention 108"), ratified by Law 2068/1992, as 11 in force today and in particular those of articles 5 and 6. 6. The provisions of the General Data Protection Regulation (GDPR) no. 679/2016. 7. The provisions of Law 2472/1997 insofar as they do not conflict with 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. 3/2010 Opinion of the Article 29 Working Group on the principle of accountability (WP 173/13-7-2010) 10. The under no. 2/2017 Opinion of the Article 29 Working Group on the processing of personal data at work (WP 249) 11. The Working Document of the Article 29 Working Group dated 29-5-2002 on the surveillance of electronic communications in the workplace (WP55) 12. 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) 13. The under no. 06/2014 Opinion of the Article 29 Working Party on the concept of legitimate interests of the controller (WP 217), insofar as it is interpretatively useful in the context of this. 14. The Guidelines of the Working Group of article 29 "Guidelines on transparency under Regulation 2016/679", WP260 rev.01, insofar as they are interpretatively useful in the present context. 15. The under no. 2/2018 Guidelines of the European Data Protection Board "regarding the derogations provided for in article 49 of Regulation 2016/679". 16. The document of the Article 29 Working Group under no. 18/EN/WP 262 of 06-02-2018 entitled "Guidelines on Article 49 of Regulation 2016/679" 17. The Guidelines of the Article 29 Working Group on Personal data breach notification under Regulation 2016/679 WP 250 rev. 1) 18. The Guidelines (under consultation) under no. 3/2018 of the European Data Protection Board on the territorial scope of GDPR 12 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. According to Article 3 para. 1 GDPR "this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place within the Union". In No. 22 Rationale of the GDPR, it is specified for the concept of establishment that it "... presupposes the substantial and actual exercise of activity through fixed arrangements. From this point of view, the legal type of these arrangements, whether it is an annex or a subsidiary with legal personality, is not decisive". 4. According to Article 4, paragraph 1 GDPR, "personal data" is defined as "any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an ID number, location data, an online identifier…". A similar broad definition for the concept of personal data previously existed in article 2 par. a of Law 2472/1997, pursuant to Directive 95/46/EC. In this context, the e-mail address (e-mail) of a natural person constitutes personal data since it can function as an element of indirect or direct identification of its owner, allowing communication with him. When the e-mail address (e-mail) bears the name or related identifier of the identity of the natural person - user (e.g. johnsmith@ikea.sk) then it is a matter of direct identification and therefore constitutes personal data in contrast to the address concerning a legal person (e.g. ikeacontact@ikea.com), which in principle does not constitute personal data1. 5. According to the jurisprudence of the Court of Justice of the European Union (CJEU), the fact that the processing of information is related to the content of a professional activity, does not influence and negate their characterization as personal data2, nor does it imply an exception from the relevant protection3, even when the data controller acts in the exercise of his public duties4, and the "distinction of the data in question according to whether they fall into the private sphere or the public sphere manifestly results from confusion between those who fall under personal data and those who fall in private life"5. According to the jurisprudence of the European Court of Human Rights (ECtHR), the protection of "private life" based on Article 8 of the European Convention on Human Rights (ECHR), which includes the protection of personal data, does not exclude professional life and is not limited to life within the place of residence (see APDPX 34/2018 and OE29 Working document on the surveillance of electronic communications in the workplace of 29-5-2002, WP55, p. 8). Moreover, according to the same jurisprudence, electronic letters (e-mails)6 are subject to the protection of Article 8 ECHR, 1 For details see the content of the 21-02-2018 response given by the European Commission in the context of question no. E-007147/17 http://www.europarl.europa.eu/doceo/document/E-8-2017 -007174-ASW_EN.html; redirect 2 See CJEU C-345/2017 Sergejs Buivids decision of 02-14-2019 para. 46, CJEU C-398/2015

Salvatore Manni decision of 03-09-2017 para. 34, CJEU C-615/13 Client Earth decision of 16- 7-2015, paras. 30, 32, CJEU C-92/09 & C-93/09 decision Volker und Markus Schecke GbR & Hartmut Eifert v. Land Hessen of 09-11-2010 para. 59. 3 See European Union Agency for Fundamental Rights (FRA), Handbook on European legislation on the protection of personal data, 2014 edition p. 50 and 2018 edition (English) pp. 86-87. 4 General Court EU T-496/13 McCullough decision of 11-6-2015 on the inclusion of the names of the data subjects in the minutes of the meeting regardless of the fact that they exercise public authority par. 66 or that they have already been made public see CJEU C-127/13 decision Guido Strack of 02-10-2014 in particular para. 111. 5 See and T-639/15 to T-666/15 and T-94/16 Maria Psarra et al. v. European Parliament para. 52, see and paras 50, 53. 6 George Garamukanwa v. UK decision of 14-5-2019 on admissibility, para. 25, Copland v. United Kingdom of 3-4-2007. 14 including the electronic correspondence of letters (e-mails) of commercial content7. Therefore, not accepting that the above information (especially e-mails) constitute personal data "would have the consequence of not requiring at all, with regard to the information in question, the observance of the principles and guarantees provided for in area of personal data protection and, in particular, the principles concerning the quality of the data and the legality of their processing... as well as the respect for the rights, access, correction and opposition of the interested party..., but also the control exercised by the control authority..." (CJEU C-434/16 decision Peter Nowak v Ireland Data Protection Commissioner of 20-12-2017, para. 49). 6. Data subjects, whether they are employees or senior management or are in any way connected to the controller have a reasonable expectation of privacy in the workplace, which is not detracted from the fact that they use equipment, devices communications or any other professional installations and hardware or software infrastructures (e.g. electronic networkcommunications, Wi-Fi, corporate e-mail addresses, servers, etc.) belonging to the property of the data controller (see GDPR 34/2018, 61/2004, Article 29 Working Group WP55, op. p. 9) . The fact that an electronic letter (e-mail) has been sent from a corporate mailing address does not lead to a deprivation of the right to private life (see ECtHR, First Section, George Garamukanwa v. UK decision of 14-5-2019 on the admissibility , par. 25), the right to the protection of the personal data of the data subjects, especially the employees (see APDPX no. 2072/2018 License8 for cross-border transmission of personal data of current and former employees of the applicant company), the right in the protection of 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 of data subjects produced using the 7 Copland v UK of 03-7-2007, Amman v Switzerland of 16-02-2000, Kopp v Switzerland of 25-3-1998, Halford v United Kingdom of 25-6-1997 , Aalmoes and 112 others v the Netherlands a

decision on the admissibility of 11-25-2004. 8 See Press Release C/EX/1728/01.3.2018 regarding the granting of the under no. 2072/2018 Transfer License APDPX. 15 corporate communications are the controller's "property" or "property" because they are the owner of the said communications or corporate email addresses, an approach adopted by some US court case law, but not by The European Union. 7. According to Recital 39 GDPR "any processing of personal data should be lawful and fair. It should be clear to natural persons that personal data concerning them is collected, used, taken into account or otherwise processed, as well as to what extent the data is or will be processed. This principle requires that all information and notices regarding the processing of such personal data be easily accessible and understandable and use clear and plain language. This principle concerns in particular the information of data subjects about the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in relation to the natural persons in question and their right to receive confirmation and to achieve communication of the personal data related to them that are subject to processing. Natural persons should be informed of the existence of risks, rules, guarantees and rights in relation to the processing of personal data and how to exercise their rights in relation to this processing. In particular, the specific purposes of the processing of personal data should be clear, lawful and determined at the time of collection of the personal data. Personal data should be sufficient and relevant and limited to what is necessary for the purposes of their processing. This requires in particular to ensure that the storage period of personal data is limited to the minimum possible. Personal data should only be processed if the purpose of the processing cannot be achieved by other means. To ensure that personal data are not kept longer than necessary, the controller should set deadlines for their deletion or for their periodic review. Every reasonable step should be taken to ensure that personal data that is inaccurate is corrected or deleted. 16 8. According to Recital 60 GDPR "The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The data controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and the context in which the personal data is processed." 9. According to the last paragraph of Recital 39 GDPR "Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to this data personal data and the equipment used to process them or the use of such personal data and such equipment." 10. According to article 4 par. 12 GDPR, personal data breach means "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or submitted by otherwise

processed". According to the Working Group Guidelines of Article 29 of Directive 95/46/EC (currently European Data Protection Board – EDPB) dated 06-02-2018 on Personal data breach notification ("Guidelines on Personal data breach notification under Regulation 2016 /679 WP 250 rev. 1) one of the types of breach of personal data is that which is categorized based on the security principle of "confidentiality", when unauthorized access to personal data is found ("confidentiality breach"). The breach of personal data also takes place with illegal access to a server, and taking technical and organizational security measures on a server is necessary from the outset to prevent the related risk due to the large amount of personal data it contains9, 9 Relatedly see detailed Guide of the French Authority for the Protection of Personal Data (CNIL) "Security of Personal Data" which mentions both the need to take prior security measures for 17 in accordance with the European Agency for Network and Information Security (ENISA)10. The collection and retention of personal data in the context of the operation of a server without the prior taking of such necessary technical and organizational security measures constitutes a violation of the principles of article 5 par. 1 sec. and GDPR. 11. According to Article 5 para. 1 GDPR ("Principles governing the processing of personal data") "personal data shall be processed in a way that guarantees the appropriate security of personal data, including its protection from unauthorized or illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"), while article 32 par. 2 GDPR provides for the consideration of the risk in the context of assessing an appropriate level of security arising in particular from unauthorized access to data, where an indicative list of security measures is listed11. The GDPR mandates the submission of personal data that have already been processed in accordance with the principles of article 5 par. 1 a' to e' "in a way that guarantees appropriate security" (article 5 par. 1 f) so that in a case in which the other principles are met except that of security, the processing ultimately becomes illegal. Correspondingly, if from the beginning the intended processing is to take place in a way that does not guarantee appropriate security, the examination of the fulfillment of the principles provided for by paragraphs a' to e' of par. 1 of article 5 GDPR is omitted, as it will be about unsafe and therefore illegal processing. Furthermore, the obligation of the controller to "guarantee" the security of the processing by taking the appropriate technical and organizational measures stems from the risk based approach adopted by the GDPR in order to "make the degree risk of each processing the main servers in the context of compliance with the GDPR as well as the risk of illegal access to personal data kept on the servers, 10 Relatedly see "Reinforcing trust and security in the area of electronic communications and online services", December 2018, chapter 7 "Server and DataBase Security" p. 38 ff. 11 Related see L. Mitrou to L. Kotsali - K. Menoudako,

GDPR- Legal dimension and practical application,chapter VI. Notification of data breaches, p. 218 ff. 18 criterion for determining the extent of the relevant obligations"12 (see also APDPX 51/2015 request. sc. 4). In the same direction, the European Court of Human Rights in the case of I. v. Finland13 examining an appeal on the basis of whether the data controller managed to "guarantee" the security of personal data found a violation of Article 8 ECHR from the non-application of security measures that led to unauthorized access to them. Under the GDPR, "integrity and confidentiality" have been reduced to basic principles and conditions for the processing of personal data no. 5 par. 1 sec. in GDPR14 so that the mentioned "appropriate technical and organizational measures", among others, prevent, if implemented, any unauthorized access or use of the data and the equipment used for processing (see Ref. 39 GDPR and European Agency for Network and Information Security-ENISA15). Consequently, two of the three main objectives of information systems security (ie availability is excluded) have been reduced to principles and conditions of legal processing of personal data. The measures must be more specific (see article 32 GDPR) while as required by the principle of accountability and determined by the provisions of article 24 par. 2 GDPR, appropriate policies must be applied, depending on the processing activities (see GDPR 67/ 2018). The existence of appropriate policy documents, approved by the management of an entity (responsible or processing) that are implemented and implemented in practice (a contrario APDPX 98/2013 par. 5), is a key criterion for proving compliance with the principle of integrity and confidentiality (see APDPX 98/2013 request. s. 3. especially for information systems), to the extent that other types of evidence are absent such as the observance of an approved code of conduct or an approved certification mechanism. 12 L. Mitrou, GDPR, op. cit., p. 96 and footnotes 270 and 271 with references to concurring positions of CIPL and ENISA. 13 Decision of 17-7-2009, no. application 20511/2003 para. 37 to 46. 14 See L. Mitrou, op. p. 219, which states that "Security is a prerequisite for the effective protection of personal data. However, as a preliminary point, it should be pointed out that this is a necessary but not sufficient condition for the protection of data, as their protection from unauthorized access, disclosure and in general use does not mean of course that they are the subject of legal processing" but also of itself, the GDPR, new law-new obligations-new rights, Sakkoulas 2017, p. 108 ff. 15 “Handbook on Security of Personal Data Processing”, December 2017, especially p. 8 as well as “Guidelines for SMEson the security of personal data processing", December 2016, in particular p. 12 19 12. According to Reason 78 GDPR "The protection of the rights and freedoms of natural persons against the processing of personal data requires the adoption of appropriate technical and organizational measures to ensure that the requirements of this regulation are met. In order to be able to demonstrate compliance with this regulation, the data controller should establish

internal policies and implement measures which respond in particular to the principles of data protection by design and by default.' 13. According to Recital 82 GDPR "In order to demonstrate compliance with this Regulation, the controller or processor should keep records of the processing activities under their responsibility." 14. According to Recital 83 GDPR "To maintain security and avoid processing in breach of this regulation, the controller or processor should assess the risks involved in the processing and implement measures to mitigation of said risks, such as through encryption. These measures should ensure an appropriate level of security, which includes confidentiality... When assessing the risk to data security, attention should be paid to the risks arising from the processing of personal data..." . 15. According to Reason 87 GDPR "It should be ascertained whether all appropriate technological protection measures and organizational measures have been put in place for the immediate detection of any breach of personal data and the immediate notification of the supervisory authority and the data subject ", as detailed in the OE 29 Guidelines for the notification of a data breach from 06-02-2018 (WP 250 rev. 1). 16. Appropriate accountability measures for compliance with the principles of article 5 par. 1 GDPR may include (as recommended by the Article 2916 Working Group before the implementation of the GDPR) the following non-exhaustive list of measures: enactment 16 Opinion no. 3/2010 regarding the principle of accountability of 13-7-2010 (WP 173) p. 13 et seq. and p. 14 footnote. 7 for the international standards approved in Madrid by the competent authorities for the protection of personal data. 20 internal procedures before the creation of new processing tasks, establishing written and binding data protection policies available to the data subjects, mapping the processes, maintaining a list of all data processing tasks, appointing a data protection officer and other persons with responsibility for data protection, providing appropriate education and training to employees in data protection, establishing procedures for managing access, rectification and deletion requests, which must be transparent to the data subjects, establishing an internal handling mechanism complaints, establishing internal procedures for the effective management and reporting of security breaches, conducting privacy impact assessments in special cases, implementing and overseeing verification procedures to ensure that all measures not only exist on paper, but implemented and operating in practice (internal or external controls, etc.). The Authority, in the context of GDPR implementation, has already referred to the controller's obligations regarding security and his more general responsibility for determining appropriate technical and organizational measures, proposing "appropriate" measures which may be documented in individual procedures or in more general security policies17, clarifying that "in any case, before defining the security measures to be adopted, the correct assessment of the risks and their possible consequences18 for the data subjects takes precedence...the implemented

measures must be submitted to periodic, at least, a review, but also to be demonstrably validated by the management of the controller or processor19". Similarly, appropriate technical and organizational measures for the security of the processing of personal data in the context of the GDPR are also proposed by the European Organization for Network and Information Security (ENISA).20 17 www.dpa.gr Section Security and in particular "Security Policy , Security Plan and Disaster Recovery Plan" with reference to the minimum content of the security policy regarding the description of the basic protection and security principles applied (organizational security measures, technical security measures, physical security measures, definition of roles, responsibilities, responsibilities, tasks etc.) 18 See and G. Roussopoulou, special scientist APDPX, "Processing security and notification of incidents of violation" in EKDDDA Report "GDPR: the new landscape and the obligations of the public administration", Athens, January 2018, pp. 20 ff. available at www.ekdd. gr/images/seminaria/GDPR.pdf 19 www.dpa.gr "Security" section. 20 See footnote 11, Appendix A p. 55 ff. 21 17. In order for personal data to be subject to legal processing, i.e. processing in accordance with the requirements of the GDPR, the conditions for applying and observing the principles of article 5 paragraph 1 must be cumulatively met GDPR, as also emerges from the recent decision of the Court of Justice of the European Union (CJEU) of 16-01-2019 in case C-496/2017 Deutsche Post AG v. Hauptzollamt Köln21. The existence of a legal basis (art. 6 para. 1 GDPR) does not exempt the controller from the obligation to comply with the principles (art. 5 para. 1 GDPR) regarding the legitimate character, necessity and proportionality, the principleof minimization22. In the event that any of the principles provided for in article 5 para. 1 of the GDPR are violated, the processing in question is considered illegal (subject to the provisions of the GDPR) and the examination of the conditions for applying the legal bases of article 6 of the GDPR23 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 case C-201/14 (Smaranda Bara) considered as a condition of the legitimate and legal processing of personal data the information of the subject of the data before the processing thereof24 . 21 "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".. 22 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. 23 Cf. 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, which, among other things, stipulate that data must be collected and processed in a fair and lawful manner, for clear and lawful purposes. .. If the conditions of article 4 par. 1 of Law 2472/1997 (legal collection and processing of data for clear and legitimate purposes) are met, it is further examined whether the conditions of the provision of Article 5 par. 2 of Law 2472 are also met. /1997 [legal bases]'. 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". 24 "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". 22 18. Furthermore, the controller, in the context of the observance of the principle of legitimate or fair processing of personal data, must inform the data subject that he is going to process his data in a legal and transparent manner (see . CJEU C-496/17 cit. para. 59 and CJEU C-201/14 of 01-10-2015 paragraphs 31-35 and especially 34) and be in a position at any time to prove its 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 an expression of the principle of fair processing and is linked to the principle of accountability, giving the right to subjects to exercise control over their data by holding controllers accountable, according to the Article 2925 Working Group. As an exception and pursuant to article 14 par. 5 sec. b GDPR ("Information provided if the personal data has not been collected from the data subject"), paragraphs 1-4 of the same article do not apply and the relevant information is not provided by the data controller if it is likely to harm to a large extent the achievement of the purposes of said processing. A condition for the application of the said provision in accordance with the Article 2926 Working Group recommends that the processing (collection) of said personal data has been carried out legally, i.e. in accordance with the principles of Article 5 para. 1 GDPR. 19. 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 processing of data 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" as to the legality of the 25 Guidelines on transparency under Regulation 2016/679 of 11-4-2018 (WP 260 rev.1), pp. 4 and 5. 26 Guidelines on transparency under Regulation 2016/679 of 11-4-2018 (WP 260 rev.1), p. 31 par. 65. 23 processing (and in general the observance of the principles of article 5 par. 1 GDPR), transferring it to the data controller,27 so that it can be validly argued that he bears the burden of invoking and proving the legality of the data processing28. 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 internal organization. 20. Access by the data controller, in the context of internal corporate control, to personal data stored in a hardware and software computer system (server) constitutes processing of personal data, as in the case of access and control of an electronic computer used by the subject (APDPH 34/2018). The employer exercising his managerial right, under the self-evident condition of compliance with the principles of article 5 par. 1 GDPR and on the basis of specific procedures and guarantees provided 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 absolutely necessary for the satisfaction of the legitimate interest it seeks and on the condition that this clearly outweighs the rights and interests of 27 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", published by Law Library, 2018,

p. 172 ff. 28 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. 24 of the employee, without affecting his fundamental freedoms under no. 6 par. 1 sec. in the GDPR and after having been informed even about the possibility of a related control (see GDPR 34/2018). 21. An essential element of the legal operation of information systems and other infrastructure and communication systems during the processing of personal data is the taking of appropriate security measures, in particular measures of physical and logical separation of hardware, software and data29. 22. In order to examine the legality of the access of the data controller no. 5 and 6 par.1 GDPR in their personal dataof subjects kept in its corporate systems in the context of internal control, the no. 5 and 6 para. 1 GDPR legality of the initial collection, processing and retention of personal personal data in the systems. The illegal initial collection, processing and retention of personal data e.g. on the company's computer or server, similarly renders illegal any subsequent or further (i.e. with a different purpose to the original according to no. 6 par. 4 GDPR) discrete and independent processing of the same personal data as in the case of copying and storing them on another digital storage medium (e.g. usb stick, server, pc, etc.), but also further in that of their transmission and use, even in the case in which 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. 17 of this and cf. GDPR 38/2004) . 23. A condition for the transmission of personal data outside the European Union, as long as the general principles, procedures, conditions and guarantees of Chapter V of the GDPR (Articles 44-50) are met, is the initial legal collection, processing and retention of the same personal data according ' No. 5 and 6 par. 1 GDPR 30 29 See APDPH 186/2014 request sk. 2, "D. Security measures - Techniques for the separation of applications", APDPX 51/2015 p. 11 and for the relevant concepts see Joint Act APDPX-ADAE 1/2013 Official Gazette B'3433/31-12-

2013. 30 See under no. 2/2018 Guidelines of the European Data Protection Board "regarding the derogations provided for in article 49 of Regulation 2016/679", page 3, Working Group of article 29 of Directive 95/46/EC with document no. 18/EN/WP 262 of 02-06-2018 entitled "Guidelines on Article 49 of Regulation 2016/679", p. 3. 25 (see in this regard the No. 3/2018 Temporary Order of the President of the APDPH) , so that if the initial collection was illegal, their subsequent cross-border transfer would also become illegal31. As the Authority did not judge, under the implementation state of no. 9 Law 2472/1997 in the framework of licensing a company for the cross-border transmission of personal data of its former and current employees,

in addition to the previous legal collection and processing of such personal data, prior to the transmission, the information of the data subjects is required in order to exercise the rights of access and objection if there are legitimate reasons32 and of course the conditions of Chapter V of the GDPR (Articles 44-50) are met. 24. The ABS company, a subsidiary of AMPNI (parent company of the AMPNI Group), notified the Authority of a data breach incident no. 33 GDPR which consisted of the unauthorized access and copying from the ABS server of its full content. The ABS company pointed out the parent company of the same Group, AMPNI and the company EY Hellas, as being responsible for the illegal copying of its server. In addition, the ABS company filed a complaint for violation of the legislation on personal data against the companies AMPNI and EY Hellas, while it requested the issuance of an act of suspension and prohibition of the processing of the copied content of its server. The audited company AMPNI briefly argued that it legally gained access to the ABS company's server because the latter was its subsidiary and owned 100% of its share capital, that the e-mails contained were corporate and therefore on the one hand belong to the property - property on the other hand, they are not subject to the protection of personal data legislation, that the access took place in the context of internal corporate control and therefore the provision provided by article 6 par. 1 sec. in the GDPR legal basis of the overriding legal interest that granted it the right of access and control as well as that the copying of the entire server content of the ABS company became necessary, despite the fact that the initial planning of the control concerned targeted access in small e-mails 31 See the position of the European Data Protection Supervisor (EDPS) according to which in case the data being transferred cross-border has been collected illegally, the cross-border https://edps.europa.eu/data-protection/data-protection/reference - library/international-transfers_en) 32 See Press Release C/EX/1728/01.3.2018 regarding the granting of the under no. 2072/2018 Transfer License APDPX. their transmission (see 26 numbers of specific employees and executives of the AMPNI Group, because it was accidentally found during the day of the audit, the operation of illegal software to delete already deleted files on the server and thus a total backup copy was taken. The company ABS , before withdrawing the complaint against AMPNI, briefly objected that from the beginning the target of the audited AMPNI was the copying of the entire server (server) which also included personal data of employees and executives of third companies as it emerged from relevant letters that had been sent to it by AMPNI and not the targeted copying of e-mails of specific natural persons, that the controlled company AMPNI illegally copied the entire content of the server (server) due to the refusal of ... (...) N to accept the request of copying because it relied on a relevant legal opinion from which the illegality of such copying arose work and that the illegality of the request to copy the server (server) results from the sending of a letter by

the controlled company AMPNI declaring in advance the exemption ("amnesty") of N from any kind of responsibility in the event of the initiation of legal proceedings against him because of copying. 25. In this case, it emerged at the discretion of the Authority that the company ABS, a subsidiary company of the parent company AMRNI of the same Group, was the owner of servers that were installed in the office premises of a building where companies of the Group were housed on the Kondyli Coast 10 in Piraeus under lease from the company "APOTHIKES AEGAIOU SA". On the aforementioned servers owned by the ABS company, the DANAOS software was installed and operated under a user agreement and on the basis of a license obtained by the company "AEGEAN SHIPPING MANAGEMENT" ("ASM"), which, however, did not belong to the AMPNI Group . It should be pointed out that on 30-10-2018 and after the control process by the Authority had already started in the context of this case, the ABS company entered into separate service and software maintenance contracts with the company that provided the DANAOS software in relation to the companies of AMRNI Group. In the same computing infrastructure (hardware and software) in addition to DANAOS (where e-mails were stored), the virtual file servers AMPFS1 (where fileshare and usershare files were stored) and AMPFS2 (where e-mail attachments were stored) were included which were stored in DANAOS), as appears in particular from the statements of ... of EY LLP Ξ dated 12-7-2018 and 17-12-2018 as well as from the statement of ... of ABS O dated 18-12-2018, which were presented by invoked AMPNI. The above hardware and software computing infrastructure (DANAOS, AMPFS1 and AMPFS2) was used to carry out e-mail communications both by employees and executives in AMPNI Group companies, as well as by employees and executives in third-party companies, outside the Group AMPNI as indicatively in "Aegean Shipping Enterprises", "Aegean Agency" and "Aegean Oil" (according to O's statement, ibid.), but also in "Aegean Net Fuels Ltd Fze", "Aegean Lubes" and " Aegean Gas”33. It is important that the ABS company, prior to its withdrawal of the complaint, had answered relevant written questions of the Authority that companies outside the AMPNI Group were using the infrastructure and servers of the ABS company informally and without any written contract (prot. no. APDPCH C/EIS/7522/20-09-2018), referring in fact to the letter dated 03/07/2018 of ... of the AMPNI N Group, which stated that the ABS company has not entered into hosting and service provision contracts with other companies. It should be noted that N, working on behalf of the AMPNI Group as ... (...), was hired by the company AEGEAN MANAGEMENT SERVICES" -"AMS", i.e. by another company of the AMPNI Group (see Supplementary Memorandum AMPNI-ABS of 19-12 -2018 pp. 9 and 10, APDPH C/EIS/10259/19-12-2018).Finally, from AMPNI's memoranda it appears that both companies belonging toin its Group, as well as third-party companies, outside the Group, used the same computing

infrastructure (hardware and software) to process the electronic correspondence of employees and executives, even accepting that it copied information of 34 third-party natural persons who had a relationship with companies outside the Group and they used the same computing infrastructure: "There was never any 33 According to the complaints of the employees as well as the printouts of the electronic e-mail addresses that were presented through ABS memoranda before the hearing before the Authority, in particular the one under no. APDPH C/EIS/5432/18-6-2018 supplementary memorandum. 34 As has been pointed out above and will be developed below, AMPNI claims that these are corporate-professional e-mails owned by it which do not constitute personal data. AMRNI's reference to personal data in its pleadings constitutes, according to it, an ancillary claim, not accepting that they constitute personal data. 28 intent to copy information other than the collection of specific data relating to the 18 users and related files relevant to the internal investigation described above. Any further copying of information that took place separately from the specific collection of research-related data was carried out for the sole purpose of protecting against the malicious permanent destruction of critical internal research evidence and important business records of the AMPNI Group" (see AMPNI Treatment Application no . prot. APDPH/G/EIS/6211/13-7-2018 pp. 16-17). Similarly, AMPNI stated that "[...] personal data of natural persons who are not connected in any way, now or in the past, with the AMPNI Group under any relationship of employment, service provision or otherwise or which are otherwise related to the pending criminal and/or civil investigations, then AMPNI would be willing to delete the data concerning the said natural persons and provide evidence of this" (see AMPNI-ABS Supplementary Memorandum of 19-12-2018 p. 23, APDPH C/EIS/10259/19-12-2018 as well as AMPNI-ABS Supplementary Memorandum of 05-4-2019 pp. 8 and 12 APDPH C/EIS/2616/05-4-2019). With the above copying of the entire content of the computing infrastructure, the audited company AMPNI created a new filing system, a copy of the original, which it transferred to Manchester, United Kingdom. Finally, AMRNI stated that in the same common area ("computer room") there were installed and operating several servers of other companies whose offices are housed in the same building and which are not related to the AMRNI Group (APDPH C/EIS/7306/10-9-2018 p. 2 paragraph 3). From all of the above, it follows that both the parent company AMRNI and subsidiary companies of its Group, as well as third parties, outside the AMRNI Group, used and had physical access to the same space where several company servers were installed and operated. AMPNI Group, as well as third-party companies and other legal entities outside the AMPNI Group, but also physical and logical access to the same computing infrastructure (DANAOS hardware and software, AMPFS1, AMPFS2) for processing the electronic mail of their employees and executives by processing the systems archiving of electronic communications. The

above accesses and processing of personal data took place without taking any measure of physical and logical separation, and the person designated as Responsible... (...) of the AMRNI Group was hired by a company of the Group in order to provide services for both 29 companies of the AMRNI Group, as well as for third-party companies outside the AMPNI Group, while the licensing and service contract with the software company DANAOS was concluded by a third company outside the AMPNI Group, so that it was finally established that any kind of personal data processing took place informally, without the existence of any agreement between the companies inside and outside the AMRNI Group that shared the same hardware and software infrastructure, without taking any essential technical or organizational measure of internal compliance with the provisions of the GDPR, without relevant demarcations, with the result, as it appears from the documents, that ultimately a matter of province of a specific server (server) and to be brought before the civil courts for resolution through the interim measures procedure (APDPX/G/EIS/733/30-01-2019). 26. The Authority in the context of the exercise of its audit powers, both before the hearing (see APDPH no. prot. G/EX/5414-1/26-6-2018 and APDPH no. prot. C/EX/6211- 1/14-8-2018), as well as during the hearing he asked the audited company AMPNI, among others, to document its compliance, as it had an obligation under no. 5 para. 2 GDPR principle of accountability to the provisions of the GDPR and in particular in relation to taking the required "technical and organizational measures that it maintains for the security of personal data and the infrastructure used that supports the processing by notifying us of any relevant policy document or internal regulation, whether it concerns the company itself or applies at Group level. For example, to mention the measures it observes regarding the physical access to the MAIL SERVER in question, the logical access to the MAIL SERVER application, the policy of correct use of company emails by its staff, the policy of controlling them (e.g. access and management rights of the subsidiary company in question and/or the parent company complained of, if the above is included in a text governing staff relations (e.g. Labor Regulations), as well as if and how it is informed by the staff in advance for the above and in particular for any control of company emails, the relevant conditions, the procedural guarantees of control, etc." p. 2).As to the legality of the copying of the content of the server (server), according to the data breach notification and the complaints, it was specifically requested by the Authority among others, both during the hearing and before a of him (see APDPH no. prot. C/EX/6211-1/14-8-2018 p. 2) to clarify "if and how 30 the staff of the group and in general the users of the e-mail accounts were informed in advance, about the right of your company to check the e-mails, the relevant conditions, the procedural guarantees of checking, etc.. as well as if, when and how the staff was informed about the specific check...". 27. The audited company AMRNI before the hearing and instead of

replying to no. prot. APDPH C/EX/5414-1/26-6-2018 document of the Authority submitted from 13-8-2018 the Application for Treatment for the revocation of the no. 2/2018 of the Temporary Order of the President of the Authority without ultimately responding to any of the detailed requests of the Authority, without documenting no. 5 para. 2 GDPR the legal operation of the infrastructure used (hardware and software - servers) that supports the processing of personal data (in particular e-mails), without providing any kind of written documentation of its internal compliance with the GDPR, in particular to the requirements for secure processing of personal data, without citing the necessary technical and organizational measures taken and without providing any personal data management policy, any security policy, any employee regulation as well as any kind of proof of informing the subjects about the processing of their data and the exercise of their related rights but also for the possibility of checking their e-mails. The then complainant ABS, in response to the same document from the Authority, submitted with no. prot. APDPX C/EIS/5935/04-07-2018 memorandum of political security documents, which, however, lacked a date, signature, approval as well as proof of their implementation, and moreover they were said to relate to an unspecified legal entity under the name " AEGEAN". Subsequently, the audited company AMPNI provided clarifications on the questions raised by the Authority with no. first APDPH C/EX/6211-1/14-8-2018 her document, but again without documenting under no. 5 para. 2 GDPR the legal operation of the infrastructure used (hardware and software - servers) and without providing any type of written documentation of its internal compliance with the GDPR. The then complainant ABS, in response to the same document of the Authority with no. prot.APDPX C/EIS/7522/20-9-2018 its document stated that the documents presented by31 the same Policies are drawn up outside the European Union and specifically in the USA as well as being implemented by the parent company AMPNI, without providing relevant evidence. In addition, he claimed that the "Internal Regulation of AEGEAN" submitted with the memorandum has been drawn up exclusively for the subsidiary companies of AMRNI and that it does not contain any reference to the control of employees' corporate e-mails or the way the company can proceed in the above act, an event for which the parent company is solely responsible and not itself. Finally, with the same memorandum, ABS stated that both companies of the AMPNI Group, as well as third parties outside the AMPNI Group, use the infrastructure and servers of the ABS company informally and without any written contract. 28. During the meeting of 05-12-2019 before the Authority, the ABS company, after replacing its legal representative and its attorney, withdrew its complaint, which has no legal consequences in terms of the continuation of its examination case before the Authority as it is not a private civil law dispute whose subject matter is disposed of according to the will of the parties. In addition, the Authority ex officio conducts checks

based on the information it receives regarding the breach of personal data of the subjects. The company AMPNI both during the hearing before the Authority during the meeting of 05-12-2019, and later with the no. prot. APDPH C/EIS/10259/19-12-2019 its supplementary memorandum (jointly with ABS) submitted clarifications as well as a series of claims and objections, but again without documenting under no. 5 para. 2 GDPR the legal operation of the infrastructure used (hardware and software - servers) and without providing any type of written documentation of its internal compliance with the GDPR. On page 14 of the above memorandum AMPNI states that "AMPNI Group has IT security policies (see attachments as Appendix D)". The document in question is entitled Information Systems Security Policy of Aegean Marine Petroleum Network Inc., bears the date of signature of approval of the latest version on … by … Director (…) P and was drawn up by … (…) N in non-compliance with the provisions of no. 679/2016 of the General Data Protection Regulation or Directive 95/46/EC but in compliance with provisions 32 of the US legislation "Sarbanes Oxley Act 2002" ("SOX") and in particular with section (hereinafter "section") 404, as is stated on each page of said policy. In particular, the specific US law was passed to deal with corporate financial scandals and concerns corporate governance and the disclosure of financial transactions in the context of which companies subject to the provisions of the law (whose securities are traded on US exchanges) are required to incorporate and implement internal control procedures as well as prepare annual financial reports ("financial reports") to the US Securities Exchange Commission (Security Exchanges Commission - "SEC")35, which include an internal controls report ("Internal Controls Report") for financial transactions and the reliability of financial statements ("financial statements"). This report is conducted based on the provisions of Article 404 SOX Act. Specifically, Article 404 SOX Act36 introduces the obligation and responsibility of the company's management to create, install and operate an internal control system of the procedures related to the preparation of the company's financial statements submitted to the US Securities and Exchange Commission ("SEC") and includes an internal control report that assesses the effectiveness and reliability of the internal control system during the previous annual management year37. From the above, in combination with the content of the said information systems security policy of Article 404 SOX Act USA, it follows that it has not taken into account the risks arising for the protection of the personal data of the subjects through the use of the computing infrastructure (hardware and software DANAOS, AMPFS1, AMPFS2) but is intended to secure the necessary corporate information to achieve the purposes described above in relation to the US Securities and Exchange Commission (SEC). 35 See the website of the US Securities and Exchange Commission in relation to Article 404 SOX at www.sec.gov/info/smallbus/404/guide/intro.shtml and

Sarbanes-oxley-101.com 36 For details see “Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners”, The Institute of Internal Auditors. 37 Companies subject to the SOX Act are required to file with the US Securities and Exchange Commission (SEC) Form 10-K, which includes an internal control report stating management's responsibility for the internal control structure and procedures with respect to financial figures and including the adequacy of internal controls. A statement is also submitted regarding corrections to the balance sheets by external auditors, recording of off-balance sheet transactions, changes in share ownership by management members as well as information regarding the existence of a code of ethics. 33 From the reading of the policy of article 404 SOX Act USA invoked by AMPNI, it is established that there is no provision for any reference to the protection of personal data pursuant to the GDPR or Directive 95/46/EC as well as any reference and measure internal organization of compliance with the principles of article 5 GDPR and the legal bases of article 6 GDPR, indicatively there is no provision in relation to: a) the rights of subjects (articles 12-22 GDPR), b) the application of appropriate techniques and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR (Article 24 par. 1 in conjunction with Articles 25 and 30 GDPR) and c) the implementation of appropriate technical and organizational measures for the security of the processing (article 32 GDPR). In addition, there is no provision regarding the permissibility or otherwise of the use of the company's electronic communication infrastructure by the employees and executives of AMPNI in relation to the possibility of surveillance, access and control of the electronic communications of employees and executives of AMPNI and, in a positive case, the conditions , procedures and guarantees for conducting relevant checks and investigations on their personal data. Finally, the policy of article 404 SOX Act USA presented and invoked by AMRNI does not address the risks that arise during the processing of personal data (see request s. 75 GDPR). Finally, the controlled company AMPNI submitted together with ABS the no. prot. APDPH C/EIS/2616/05-4-2019 supplementary memorandum to rebut the memorandums of the complainants and L, former legal representative of ABS, but again without documenting under no. 5 para. 2 GDPR the legal operation of the infrastructure used (hardware and software - servers) and without providing any type of written documentation of its internal compliance with the GDPR. 29. Besides, the audited company AMPNI, despite the requests and questions of the Authority, both before the hearing and during the hearing, did not answer and did not document as it should no. 5 para. 1 GDPR the legality of the processing of personal data in the context of the operation of the infrastructure used (hardware and software – "original servers"). 34 In particular, it follows from all of the above that the audited company AMPNI as data controller did not

take any internal compliance measure no. 5 para. 1 and 6 para. 1 GDPR in relation to the legal operation of the infrastructure used (hardware and software – "original servers" DANAOS, AMPFS1, AMPFS2) that supports the processing of personal data (especially e-mails) that are included in a filing system, nor did he provide any kind of written documentation of such internal compliance required by the GDPR under no. 5 para. 2 GDPR, in particular with regard to the requirements for secure processing of personal data, nor did it take the necessary technical and organizational measures pursuant to no. 5 par. 1 sec. in combination with no. 24 par. 1, 2 and 31 par. 1, 2 GDPR in order to guarantee the appropriate security of personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or deterioration ("integrity and confidentiality") , nor did it appear that he designed, prepared and implemented in compliance with the provisions of article 5 par.1 GDPR theany measure of accountability from those mentioned in the reasons under no. 11 and 16 hereof, including personal data management policies and security policies in accordance with the requirements of the GDPR, nor did it take physical or logical separation measures, nor did it provide an employee regulation or other internal document that includes provisions for the protection of personal data, nor did it provide any kind of proof of informing the subjects about the processing of their personal data during the operation of the used computing infrastructure (hardware and software - "original servers" DANAOS, AMPFS1, AMPFS2), the exercise of their relevant rights and also about the possibility checking their e-mails. On the contrary, the audited company AMRNI verbally focused its argumentation on the later or further stages of the processing of the same data, i.e. the stage of access to the e-mail control servers (stage 2), then copying (stage 3) and transmission to Manchester, United Kingdom (stage d) of the original servers' content ("copy server"), claiming that the conditions of article 6 par. 1 sec. to the GDPR for the processing of personal data, without again documenting by no. 5 par. 2 GDPR the no. 5 par. 1 GDPR legality of the processing of personal data, sufficient for the verbal invocation of article 6 par. 1 sec. in the GDPR on overriding legal interest. As, however, it was extrapolated in the 35th recital under no. 17 hereof, the processing of personal data in violation of the principles of article 5 par. 1 GDPR is not cured by the existence of a legitimate purpose and legal basis no. 6 par. 1 GDPR. In this case, the audited company AMPNI had the obligation, after proving that it was due under no. 5 para. 2 GDPR the adoption and implementation of compliance measures with the provisions of articles 5 para. 1 and 6 para. 1 GDPR regarding the legality of the processing of personal data that took place in the used computing infrastructure (hardware and software of "original servers » DANAOS, AMPFS1, AMPFS2), to prove subsequently by no. 5 par. 2 GDPR, also the legality under no. 5 para. 1 and 6 para. 1 GDPR, of subsequent (for the initial purposes) or further (for different purposes

according to no. 6 para. 4 GDPR) independent and distinct processing operations, namely: b) access and control in the e-mails kept on the servers, c) the creation of a new filing system after copying the original filing system and d) the transmission of the copy filing system (server - back up according to AMPNI) in Manchester, United Kingdom (see the documents of AMPNI with original no. In view of the above, given that the initial collection, retention and generally processing of the personal data included in the computing infrastructure's archiving systems (hardware and software of the "prototype servers" DANAOS, AMPFS1, AMPFS2) was already judged to be illegal and infringing the provisions of article 5 par. 1 GDPR and in particular those of articles 5 par. 1 sec. a' and f' and par. 2 in conjunction with articles 24 par. 1 and 2 and 32 par. 1 and 2 GDPR, it is submitted that the subsequent or further processing of the same personal data and in particular the access and control of e-mails, copying the contents of the "original servers" and thereby creating a new filing system, sending the new filing system - copy to Manchester, UK are also illegal and violate the entire principles of article 5 par. 1 and 2 but also Article 6 para. 1 GDPR, as inextricably linked and derived from the initial illegal processing of the personal data of the archiving system of the "original server". 30. As a result of the above shortcomings, the Authority further states, according to the facts accepted in the no. 25 recital, that the same 36 computing infrastructure (DANAOS, AMPFS1, AMPFS2 server hardware and software) was used for the subsequent or further processing of personal data (e-mails) of subjects who worked and were connected to both AMPNI Group companies, and with third-party companies, outside the AMPNI Group, without the necessary physical and logical separation measures having been taken, with the result that the administrator of the system-computing infrastructure has access to and processes on behalf of the AMPNI company personal data (e-mails) of data subjects that are not connected to it38. Therefore, from the lack of appropriate technical and organizational measures, in particular those that mandate physical and logical separation, the threatened risk to the confidentiality and integrity of personal data through access, copying and transmission in Manchester, United Kingdom . From the above, it follows that the subsequent or further processing, through access, copying and transmission to Manchester, United Kingdom, of the personal data of natural persons related to the AMPNI Group was unlawful because it concerned personal data that had not occurred in the first place legal processing, while regarding the personal data of natural persons related to third companies outside the AMRNI Group, in addition due to the lack of physical and logical separation measures. 31. In view of the above, the Authority considers that the audited company AMRNI as a data controller: on the one hand, did not apply all the principles of article 5 para. 1 GDPR and 6 para. 1 GDPR regarding the legality of the processing of personal data (in particular e-mails) that took place in the computing

infrastructure used (hardware and software of "original servers" DANAOS, AMPFS1, AMPFS2), but also in the context of any subsequent or further processing of the same personal data, nor proved by no. 5 para. 2 GDPR the observance thereof. on the other hand, he violated the provisions of articles 5 par. 1 sec. a' and f' and par. 2 in conjunction with articles 24 par. 1 and 2 and 32 par. 1 and 2 GDPR regarding the principle of secure processing (especially "confidentiality") of personnel data 38 See the printouts of the electronic e-mail addresses that were submitted through ABS memoranda before the hearing before the Authority, in particular of no. APDPH C/EIS/5432/18-6-2018 supplementary memorandum with a list of electronic addresses. 37 nature that took place in the computing infrastructure used (hardware and software of the "original servers" DANAOS, AMPFS1, AMPFS2) from not taking appropriate technical and organizational measures, but also in the context of any subsequent or further processing of the same personal data, in order to there is no need to examine compliance with the processing principles of subsections b', c', d' and e' of par. 1 of article 5 as well as of article 6 par. 1 GDPR, according to what was accepted in the no. 11 recital hereof. 32. On the objections and claims of the controlled company AMPNI: i. Regarding the objection that the GDPR does not apply in accordance with article 3 paragraph 1 thereof as “[...] AMRNI is a company based in the Republic of the Marshall Islands, is listed on the NY Stock Exchange and is headed by of AMRNI Group. AMRNI does not have an establishment in Greece but only maintains a postal address in Piraeus. ABS is a 100% subsidiary of AMPNI. Therefore, AMPNI does not itself have an establishment in Greece [...] the purpose of the data export/copy....had nothing to do with the activities of the AMPNI Group companies in Greece. That is, there is no relationship between the purpose for which the data was extracted and the activities of the Greek companies...” (see Supplementary Memorandum AMRNI and ABS APDPH no. prot. C/EIS/10259/19-12-2018 p. 5 -8). It follows from Article 3 para. 1 GDPR, Recital 22 GDPR and the European Data Protection Board's under consultation Guidelines 3/2018 on the territorial scope of the GDPR that the GDPR applies to the processing of personal data in the context of the activities of establishment of the data controller, which requires the substantial and real exercise of activity, which should not be interpreted narrowly and formulaically as with a criterion e.g. the place of registration of the company in the relevant registration registers (see CJEU C-210/2016 Facebook (fan page) decision of 05-6-2018 App. Sk. in particular 56 and 53-55, 57, C-230/14 Weltimmo v NAIH decision of 01/10/2015 Petitioner in particular29 as well as 31). In this case, the audited company AMPNI argues only on the subsequent or further processing of the access-control of the e-mails and the copying of the content of the servers, without making any claims on the legality of the initial collection, retention and processing of the of personal data included in the filing systems of the 38 computing

infrastructure (hardware and software of "prototype servers" DANAOS, AMPFS1, AMPFS2). The computing infrastructure in question (hardware and software of "prototype servers" DANAOS, AMPFS1, AMPFS2) during the critical time stage was installed in Greece, specifically in Piraeus on the Kondyli Coast no. 10, belongs to the property of ABS, a subsidiary company of AMPNI and according to a statement by AMPNI itself (see under prot. no. Server belongs to the AMPNI Group and in particular, it was purchased together with the required equipment, earlier in 2018, from ABS, a member of the AMPNI Group and a 100% subsidiary of the Company". In addition, it emerged that the use of the servers installed in Greece and the processing of personal data through them took place following the decisions of AMPNI, which determined the purpose and method of processing under no. 4 par. 7 GDPR both for itself and for its subsidiaries in the context of carrying out its activities. Furthermore, according to a statement by AMPNI itself (see pg. 2 under prot. no. APDPX C/EIS/7306/10-9-2018): "The Server belongs to ABS, a member of the AMPNI Group. That is, in terms of ownership, it has been bought by ABS. ABS, however, does not process personal data on behalf of the Company". In addition to the above and in the alternative, the claim-objection of AMPNI that it does not have a real but only a postal establishment in Greece and that it is based in the Republic of the Marshall Islands (Marshall Islands) should be rejected given that it declares the address of Aktis Kondyli 10 , in Piraeus as the address of establishment and actual operation of the first, before the Authority with the submitted Application for Treatment (see no. prot. APDPX/G/EIS/6211/13-7-2018 p. 1) and second, before the Committee of the US Capital Market (SEC), as can be seen both from the Annexes A and B that he submits as attachments to the above-mentioned Application for Treatment, and from the annual report of 16/5/201739 which he cites in Γ/EIS/7306/10-9- 2018 document to the Authority and from which the statement of the following information is derived: AEGEAN MARINE PETROLEUM NETWORK INC., 10, Akti 39 See it at www.aegeanmarine.gcs-web.com/static-files/ebca7627-4368-4e6c-9a75-45862ad60cac 39 Kondili (Address of Principal Executive Office), Piraeus 185 45, Greece (underlines and boldface from the Appendices), For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. ii. Regarding the objection that the United States Bankruptcy Court for the Southern District of New York issued a worldwide order no. 362 (a) of the US Bankruptcy Code in the context of AMPNI's bankruptcy petition, by which, according to its claims, it is prohibited, on the one hand, to continue the proceedings before the Authority, and, on the other hand, to exercise control over an asset of the bankruptcy estate, which according to the controlled AMRNI company includes "[...] some, if not all, of the data under discussion are assets of the bankruptcy estate" In this case, by no provision of national or European legislation, but not by any international or other bilateral-transnational

contract it follows that the invoked order of the US Bankruptcy Court produces legal effects in Greece, nor does the controlled company AMPNI invoke such legislation, nor does it produce a Greek court decision recognizing the enforceability of such foreign court order. In addition, the audited company AMRNI, through a misinterpretation of the national and European legislation on the protection of personal data, takes it as a given in order to submit the relevant objection - a claim that the personal data processed by the data controller constitutes its "property" and thus part of his "property", as will be shown below. For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. iii. Regarding the allegation-objection that the complaint against the controlled company ABS was submitted without right and therefore inadmissible by a legal person and not a natural person no. 77 par. 1 GDPR, i.e. the ABS subsidiary with the result that the issued under no. 2/2018 Temporary Order of the President of the Authority to suffer from invalidity as well as that ABS has withdrawn its complaint against the controlled company AMPNI, it is noted in addition to sub no. 28 recital of the present that the audit was carried out ex officio under no. 57 par. 1 sec. a and h 40 GDPR based on the information received by the Authority primarily with the 18-6-2018 Notification of a Data Breach Incident submitted by ABS (APDPX/G/EIS/5432/18-6-2018). In any case, even if the complaint was inadmissibly submitted by the ABS company, the Authority is entitled under no. 57 par. 1 sec. a and h GDPR in combination with no. 19 para. 1 para. h' of Law 2472/1997 to carry out ex officio checks and investigations with only the information he received about actual incidents of violation of the current legislation on the protection of personal data. In addition, the Authority is entitled under no. 19 par. 1 para. iii of Law 2472/1997, but is not obliged to file applications or complaints that are deemed obvious, vague, unfounded or submitted abusively or anonymously. Therefore, from the above provisions, which are applicable as they do not conflict with the GDPR (see GDPR 46/18 and 52/18), it follows that the Authority had the right to carry out an audit with only the information of the facts, regardless of the validity or not of the complaint. In addition, the President of the Authority, despite the ABS company submitting a request for a temporary injunction, ex officio issued the no. 2/2018 Interim Order, taking cognizance of the facts relied upon as it appears from the body of the Interim Order itself in which it is not stated that it accepts the said application. Therefore, sub no. 2/2018 Temporary Order of the President of the Authority does not suffer from invalidity. Finally, the ABS company's withdrawal of its complaint against the controlled ABS company, as well as the allegation of an inadmissible complaint by a legal entity, are not supported by any provision of the law, given that it is not a private civil law dispute whose object available according to the will of the parties, moreover, as stated above, the Authority investigates ex officio any

information about a violation of the legislation on the protection of personal data (ad hoc APDPX 136/2015 request. s. 6 par. a'). For these reasons, the Authority rejects the objections - claims of the audited company AMPNI. iv. Regarding the objection-claim regarding the inadmissibility of the individual complaints of natural persons because they did not previously address the data controller in order to exercise their rights under articles 15-22 GDPR, before appealing to the Authority, it should be noted that on the one hand, from the provisions of article 77 41 par. 1 GDPR, it follows that each data subject has the right to submit a direct complaint to the Authority, if he considers that the processing of personal data concerning him violates the GDPR. In this case, the natural persons reported the violation of the GDPR against them and not the unsatisfactory response of the controlled company AMPNI to the exercise of their rights under articles 15-22 GDPR. In addition, as stated above, the Authority undertakes ex officio and investigates every actual incident of violation of the existing legislation for the protection of personal data, regardless of whether or not the complainants bear the burden of proof of their allegations and whether or not they prove the validity of their claims. In the present case, the complainants complained about the alleged illegal copying of their personal data contained in the computing infrastructure's archiving systems (DANAOS, AMPFS1, AMPFS2 "original server" hardware and software). In order to check the legality of the copy in question, the Authority ex officio investigated the legality of the original collection, preservation and processing of the personal data contained in the "original servers".As already stated, the obligation of proof under no. 5 par. 2 GDPR of the legality of each processing under no. 5 para. 1 and 6 para. 1 GDPR is the responsibility of the data controller and not the data subject. For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. v. With regard to the objection-claim that corporate e-mails exchanged from corporate e-mail accounts do not constitute personal data and that they constitute an "asset" that belongs to the "property" of the company, the Authority has already rejected the relevant claim based on the recitals 4, 5 and 6 hereof in order to reach the conclusion that the audited company processed personal data included in the archiving system of the computing infrastructure (hardware and software of "original servers" DANAOS, AMPFS1, AMPFS2) without observing the principles of of article 5 par. 1 and 6 par. 1 GDPR as well as in violation of the principle of safe processing under no. 5 par. 1 sec. and GDPR. 42 In addition, in this case, the fact that the electronic addresses (e-mails) had as the first synthetic, identifying elements of the user's name, i.e. of the form name/eponymo@εταιρία.gr is sufficient for their characterization as personal data without having to check the content of the e-mails in order to establish whether they are business or private correspondence or whether they come from a corporate or private e-mail account, in accordance with what was accepted with

recitals 4, 5 and 6 hereof. Therefore, AMPNI's claim that complainants must produce "personal" e-mails sent from non-corporate (private) e-mail accounts containing personal data copied by AMPNI in order to prove the validity of their complaint, on the one hand, does not find support in the GDPR according to the above, on the other hand, the Authority considered that the principles of article 5 para. 1 GDPR and 6 para. 1 GDPR regarding the legality of the processing of personal data were not respected, that is, of all the e-mails that took place in the used computing infrastructure (hardware and software of "original servers" DANAOS, AMPFS1, AMPFS2), but also of any subsequent or further processing of the same personal data, so as to avoid or respond to the individual complaints by natural persons, as detailed below. Finally, as already accepted with no. 6 recital of the present the claim of the controlled company AMRNI according to which the personal data belong to its "property" or "property" is in complete contradiction with the national and European legislation and that the controller is not the "owner" of the personal data processed. If the data controller was the "owner" of the personal data it processes, the prohibition of the processing of personal data would not be introduced as a rule by Article 6 para. 1 GDPR so as to require one of the legal bases provided for there to be present in order to legitimize the processing, nor would the data subject be provided with a series of rights regarding the control of his personal data (art. 12-22 GDPR), in particular the rights of objection, restriction, deletion or portability. For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. 43 vi. Regarding the objection - claim of the audited company AMRNI that any consideration by the Authority of new evidence presented by the complainants after the end of the hearing infringes its right to be heard, it must be pointed out in principle that the audited company, on the one hand, became aware and copies of the documents submitted by the complainants after the end of the hearing as well as a deadline of 15 days in order to submit its views on them (ADDPH no. prot. C/EX/2214/21-3-2019), on the one hand and the itself presented new evidentiary material after the end of the hearing, but also placed itself on the allegations and evidential material presented by the complainants after the hearing (see Supplementary Memorandum AMPNI & ABS with prot. no. APDPX C/EIS/2616/05- 4-2019). In addition, no provision of the Civil Code or other legislation prohibits the presentation of new evidence after the end of the audited hearing or that all the evidence on which the Authority will make a decision must have been collected by the time the hearing is called, given that the conducting the hearing is intended to provide explanations and information to clarify issues that may even have arisen for the first time during the hearing, as is the case during the hearings conducted by other constitutionally protected independent administrative authorities such as the Authority for Ensuring the Privacy of Communications (ADAE). vii. With regard to the

allegation - objection of the audited company regarding the illegal extension of the granted deadline for submission of a memorandum after the hearing, it should be pointed out that the extension was legal since the audited company AMPNI together with ABS submitted a request for exemption of the case's rapporteur after the initiation and during the deadline for submitting a memorandum, with the result that the deadline is automatically suspended until a decision is issued on the exemption request and until a new deadline is provided. In no event could the initial post-hearing submission deadline apply if the Authority Division had not previously ruled on the exemption application. On the contrary, the submission by the controlled company AMPNI together with ABS, of a memorandum with a hearing while the request for exemption of the rapporteur that they had submitted and without waiting for the issuance of the decision on the request for exemption was pending, is in complete contradiction to the the exemption request itself as on the one hand the companies requested the 44 exception of the rapporteur, while on the other hand they submitted a memorandum to the Department of the Authority in which the rapporteur participated. For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. viii. The audited company AMPNI makes the following allegations: that it legally entered the used computing infrastructure (hardware and software of "prototype servers" DANAOS, AMPFS1, AMPFS2) in order to conduct an audit of the electronic mail of specific natural persons, former and current employees and executives of the AMPNI Group , that the controls in question were legal, that software for deleting already deleted files was accidentally discovered, with the result that it became necessary to copy the entire computing infrastructure used, including personal data (e-mails) of natural persons connected to third-party companies outside of Groups AMRNI, that there was no obligation to notify an incident of personal data breach to the Authority from the detection of the "malicious software" deletion, that as an employer he had according to article 6 par. 1 sec. in the GDPR overriding legal interest to check and copy the e-mails in the context of the control being carried out, that it had no obligation to inform the data subjects, either before the copying or after the copying of their e-mails. A condition for answering the above allegations is, as stated in the recitals no. 17, 18, 22, 29 and 30 hereof but also from the under no. 3/2018 Temporary Order of the President of the Authority, the proof of the legality of the initial processing (collection and retention) of personal data that took place in the used computing infrastructure (hardware and software of "prototype servers" DANAOS, AMPFS1, AMPFS2). Given that the Authority considered the initial collection, retention and general processing of the personal data contained in the computing infrastructure's archiving systems (hardware and software of the "original servers" DANAOS, AMPFS1) to be illegal and in particular in violation of the principle of secure processing , AMPFS2), it is submitted that the subsequent or further

processing of the same personal data and in particular the access and control of e-mails, the copying of the contents of the "original servers" to a "copy server" with which a new archiving system was created (back up according to AMRNI) and 45 the sending of the new filing system - copy to Manchester, United Kingdom are also illegal and violate all the principles of article 5 par. 1 and 2 as well as article 6 par. 1 GDPR, as inextricably linked and arising from the initial illegal processing of the personal data of the "original server" filing system so as to avoid the examination of both the complaints of the natural persons, as well as the refutation of the claims of the controlled company AMRNI which focus exclusively on the subsequent or further processing of personal data. In other words, even if the said complaints of natural persons (regarding subsequent or further processing) had not been submitted, it would have been illegal to copy the "original server" due to the non-fulfillment of the conditions for legal processing of the personal data contents . Thus, the invocation by the controlled company AMRNI of the legal basis of article 6 par. 1 sec. in the GDPR for the control, access, copying and sending of the content of the "original servers" (servers), but also the invocation of the need to copy due to the detection of "malware" cannot retroactively legalize the illegal processing at a previous stage of personal data in violation of Articles 5 para. 1 and 6 para. 1 GDPR in accordance with what was accepted in the reasons under no. 17 and 22 hereof. For these reasons, the Authority rejects the objection - claim of the audited company AMPNI. 33. On the contrary, from the information in the file and the hearing, it did not appear that the company "ERNST & YOUNG (GREECE) CERTIFIED AUDITORS ACCOUNTANTS S.A." participated or assisted in the controller's violation of the provisions of Articles 5 para. 1 and 6 para. 1 GDPR in particular during the stage of access, control, copying and transmission to Manchester, United Kingdom of personal data. 34. 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 46 possible fine would impose a disproportionate burden on a natural person, a reprimand could be imposed instead of a fine. The Authority after establishing the violation of the provisions of the GDPR as stated 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 Article 83 of the GDPR to the extent that they apply to the specific case and in particular those of the criteria provided for in paragraph 2 of the same article that pertain to the specific case under consideration by the Authority: a) the

nature, gravity and 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 degree of damage they suffered and specifically: i. ii. iii. iv. the fact that the company violated the principles from article 5 par. 1 GDPR as well as the obligation (principle) of accountability no. 5 para. 2 GDPR, i.e. violated fundamental principles of the GDPR for the protection of personal data. the fact that the condition of safe processing under no. 5 par. 1 sec. in the GDPR it has now been reduced to a basic principle of the processing of personal data so that, even if the other processing principles are respected, the processing becomes altogether illegal in a case where the controller does not guarantee appropriate security. the fact that the principle of accountability in the context of the new model of compliance 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, is also of paramount importance. the fact that according to no. 3/2010 Opinion of the Article 29 Working Party on the principle of accountability (WP173/13-7-2010) the establishment of internal accountability measures for compliance with the processing principles (paragraphs 39-51 and in particular para. 41 and 44) it provides high chances of implementing effective measures by reducing the chances of the controller to violate the law and therefore when assessing the sanctions compliance with the principle of accountability is taken into account (para. 38), while in case of violation substantial sanctions are required, as for example in the event that a controller does not comply with the statements contained in its binding internal policies, which are taken into account in addition to the actual breach of the essential data protection principles (para. 64). 47 v. vi. vii. viii. ix. the fact that the controller did not take any internal compliance measure in application of the principle of accountability to implement and implement the principles of personal data processing no. 5 para. 1 GDPR, not even those provided as "basic" according to Opinion 3/2010 of OE 29 (para. 44, ibid.) the fact that the violation of the above principles took place in the context of personal data processing in computing infrastructure (hardware and software) which is used to serve a large number of electronic communications of data subjects the fact that the violation of the above principles took place during the processing of personal data of subjects in the field of labor relations where it is characterized by an imbalance of power between employer and workers. 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 para. 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. the fact that the principle of safe processing of personal data was previously violated no. 5 par. 1 sec. in the GDPR for the possibility and ultimately achieving access, copying, transmission and in general processing of personal data of data subjects that were connected to third companies, outside of the AMRNI Group the fact that the violation of the above principles is subject to the provisions of the article 83 par. 5 sec. a GDPR in cases of administrative fines up to EUR 20,000,000 or, in the case of businesses, up to 4% of the total global annual turnover of the previous financial year, whichever is higher, i.e. in the highest prescribed category of the administrative classification system fines, the imposition of which is reserved respectively, in application of the principle of proportionality, in the case of the most serious violations of the GDPR. Therefore, already from the regulations of the GDPR it follows that the violation of the principles provided by article 5 paragraph 1 and paragraph 2 GDPR is treated as more serious than the violations provided for by article 83 paragraph 4 GDPR. 48 x. the fact of causing damage to the right to protect the personal data of the subjects from the violation of the aforementioned principles and in particular, firstly, the processing of personal data in violation of the GDPR, secondly, the subsequent processing of personal data in violation of the GDPR in more stages (initial retention and processing, access and control, copying, transmission) and thirdly, the complete deprivation of the rights and exercise of control over the personal data of the data subjects (cf. Ref. 75 GDPR and OE 29 for the administrative fines, ibid., p. 11). xi. The fact that, from the information brought to the Authority's attention, no material damage to the data subjects has occurred at this stage, nor has a relevant material damage been invoked xii. the fact that the violation of the principles of article 5 par. 1 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. xiii. The fact that the violation of the principles of article 5 par. 1 and par. 2 concerned any subject whose personal data was processed in the context of the service of his electronic communications by computing infrastructure (hardware and software) so that it is not an individual or opportunistic violation but a violation that has a systemic (structural) nature. b) the fraud or negligence that caused the violation From the hearing before the Authority and the memoranda of the data controller, it appears that the company was completely unaware of its obligations to comply with the requirements of the GDPR, moreover, it showed no willingness to comply, as will be demonstrated below. Therefore, the identified violations were the result of a lack of complete knowledge and application of the provisions of the GDPR in the

context of the organization of internal compliance despite the fact that the data controller could and should, in particular due to the obligation of accountability, comply with the provisions of the GDPR, violating thus the duty of care required by law. c) any actions taken by the controller to mitigate the damage suffered by the data subjects, The controller did not take any action to repair or mitigate the damage suffered by the data subjects, nor did it inform them, even after the illegal processing of their personal data. It should be noted at this point that the data controller invoked the exception of article 14 par. 5 sec. b GDPR so as not to harm the achievement of the purposes of the processing, i.e. the invoked internal control. Regardless of the validity or otherwise of this claim, even after the completion of the cited internal audit, at no time did the controller 49 inform the data subjects of the subsequent or further processing, i.e. the copying and transmission of their data to Manchester, United Kingdom , in particular of natural persons connected to third parties outside the AMPNI Group, so that they have not been informed about it until now. It is recalled that according to what was accepted herewith, the violation of the principles of article 5 par. 1 GDPR took place at the expense of every subject whose data was illegally processed and not only the natural persons who complained. d) the degree of responsibility of the data controller, taking into account the technical and organizational measures he applies pursuant to articles 25 and 32, The data controller did not take into account technical and organizational measures, nor did he carry out the necessary evaluations in order to draw appropriate conclusions (see under No. 28 of the present petition). e) regarding 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) regarding the degree of cooperation with the Authority to remedy the violation and limit the possible adverse effects of, the Authority recognizes as a mitigating circumstance the controller's admission of the illegal copying and sending to Manchester, United Kingdom "[...] any e-mails of natural persons who did not have and/or do not have any employment or service relationship services or any other relationship with companies of the AMPNI group, which AMPNI would be available to separate and provide evidence about it" (Supplementary Memorandum AMPNI-ABS of 05-4-2019 pp. 8 and 12 APDPX C/EIS/ 2616/05-4-2019 end page, point 4) as well as the expression of his intention, according to the above, to separate or delete (see Supplementary Memorandum AMPNI- ABS of 19-12-2018 p. 23), although he did not express the same intention for the personal data of the other data subjects. g) the categories of personal data affected by the violation, namely that it is not personal data of Articles 9 and 10 GDPR, according to the information brought to the attention of the Authority. h) the way in which the supervisory authority was informed of the breach, in particular whether and to what extent the data controller or the processor notified the breach, In this case, the

Authority was informed of the finally established breaches primarily through the Data Breach Notification which submitted by the ABS company as a result of which it carried out an ex officio audit. The data controller did not inform the Authority, nor did he himself proceed with a Data Breach Notification i) any other aggravating or mitigating factor resulting from the circumstances of the specific case, such as the financial benefits obtained or losses avoided, directly or indirectly, by violation 50 The Authority, in addition to the above, recognizes as an additional mitigating factor that from the data brought to its attention to date and on the basis of which it established the violation of the GDPR, the data controller did not obtain a financial benefit, nor did it cause material damage to the subjects of data. The Authority recognizes as an aggravating factor the fact that the data controller has not demonstrated to date any intention to comply with the requirements of the GDPR, nor has it informed the Authority of its inclusion in an internal compliance program in order to make any processing of personal data lawful No. 5 para. 1 and 6 para. 1 GDPR carried out on its computing infrastructure (hardware and software of "original servers"). The data controller in a series of documents to the Authority, especially after the hearing, focused all his efforts on highlighting the importance for him of the use of the content of the copied servers (“back up” servers according to him) for the purposes of the internal control of the AMPNI Group and consequently for the presentation of relevant data to the US Securities and Exchange Commission and the competent US judicial authorities, even requesting that the Authority not impose the sanction of the destruction of the content of the copied servers, at the time when the Authority had prohibited the processing and use of the content of the copied servers, but not at that time the "original servers". THE AUTHORITY Having taken into account the above Because it decided the no. 58 par. 2 GDPR exercising its corrective powers in this particular case by imposing corrective measures Because pursuant to the provision of article 58 par. 2 sec. d GDPR, the Authority decided to instruct the company "AEGEAN MARINE PETROLEUM NETWORK INC (AMPNI)" as data controller to make the processing of personal data included in the used computing infrastructure (hardware and software) compliant with the provisions of the GDPR "master servers" DANAOS, AMPFS1, AMPFS2), as well as to the new master server copy archive system sent to Manchester, UK. Because in particular the company should take all the necessary internal compliance and accountability measures to the principles of article 5 par. 1 and par. 2 in conjunction with article 6 par. 1 GDPR. Because the above order should be executed within three (3) months from the receipt of this, informing the Authority. Because the above corrective measure is not sufficient by itself to restore compliance with the violated provisions of the GDPR in accordance with what was accepted with 51 no. 31 recital of the present and in addition, at the moment when the company, despite its essentially

admitting at least part of the violation of the GDPR, showed complete indifference to compliance with the provisions of articles 5 and 6, paragraph 1 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 administrative fine under no. 83 GDPR, both to restore compliance and to punish this illegal behavior40. Because the violation of the provisions of articles 5 and 6 of the GDPR established by the Authority is subject to the provisions of article 83 par. 5 sec. a GDPR in cases of administrative fines up to EUR 20,000,000 or, in the case of businesses, up to 4% of the total global annual turnover of the previous financial year, whichever is higher. Because the Authority took into account, on the one hand, that the company AMRNI has filed for bankruptcy in the USA, on the other hand, that according to the report submitted by the company in 2017 to the US Securities and Exchange Commission. (SEC) its total revenue for the year 2016 was 4,076,219,000.00 US dollars. (see p. 157 at attachment no. prot. C/EIS/7306/10-09-2018 document41).Because with the issuance of this document, no. 19 par. 7a Law 2472/1997 the validity of

Temporary Orders of the President of the Authority No. 2/2018 and 3/2018 and are in force

now the events accepted in the operative part of the present

FOR THOSE REASONS

THE BEGINNING

A.

It instructs the company "AEGEAN MARINE PETROLEUM NETWORK INC."

(AMPNI)"" as within three (3) months from the receipt of this, informing

the begining :

40 See OE 29, Guidelines and the application and determination of administrative fines for the

purposes of Regulation 2016/679 WP253, p. 6

41 Also available at www.aegeanmarine.gcs-web.com/static-files/ebca7627-4368-4e6c-9a75-45862ad60cac

i.

to make the processing operations in accordance with the provisions of the GDPR

personal data included both in the used

computing infrastructure (hardware and software of "prototype servers" DANAOS,

AMPFS1, AMPFS2), as well as in the new file system by copying it

original server shipped to Manchester, UK,

ii.

to take all necessary measures of internal compliance and accountability to

principles of article 5 paragraph 1 and paragraph 2 in combination with article 6 paragraph 1 GDPR.

B.

It imposes on the company "AEGEAN MARINE PETROLEUM NETWORK INC

(AMPNI)' the effective, proportionate and dissuasive administrative fine

which is appropriate in the specific case according to its special circumstances,

in the amount of one hundred and fifty thousand (150,000.00) euros.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou