Athens, 04-29-2022 Prot. No.: 977 DECISION 24/2022 (Department) The Personal Data Protection Authority met as a Department via video conference on Wednesday 04-21-2021 at 10:30 a.m. at the invitation of its President, in order to examine the case referred to in the present history. The Deputy President, Georgios Batzalexis, obstructing the President of the Authority, Constantinos Menoudakos, the regular member of the Authority, Konstantinos Lambrinoudakis, and the alternate member of the Authority, Grigorios Tsolias, were present, as a rapporteur, in place of the regular member, Charalambos Anthopoulos, who, although summoned legally in writing, did not attend due to disability. Present without the right to vote were Stefania Plota, special scientist-lawyer, as assistant rapporteur, who left after the discussion of the case and before the conference and decision-making, and Irini Papageorgopoulou, employee of the Authority's administrative affairs department, as secretary. The Authority took into account the following: With no. prot. C/EIS/6429/22-09-2020 and C/EIS/7111/16-10-2020 her complaints to the Authority, A (hereinafter "complainant"), an employee of the Secretariat of the office ... which is under the Fire Administration of Prefecture X Services (hereinafter "DI.P.Y.N.") denounces the DI.P.Y.N. X, which at the time when the complaint was submitted was represented by the Governor, B (hereinafter "former Governor"), on the one hand with the first complaint for violation of provisions of the Authority's competence, regarding control of her computer during her work in the above service and on the other hand with the second complaint for failure to satisfy the right of access. 1-3 Kifissias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 In particular, the complainant states in the first complaint under consideration that on ... she was given a verbal order to work in a different office computer from the one he used every day to cover official needs in a different place from the one he worked on every day. On that day, a check was carried out, as stated in the complaint, by the former Governor, on the official computer operated by the complainant, during which she was not present and had not received any verbal or written information about its action and whether it concerned all of the service's computers. Then, on ... the complainant received the no. ... call of the Governor DI.P.Y.N. X in an apology, where it is stated that in a check of the website visit history of the official computer that she operates, she was found to have visited social networking and entertainment websites many times during her working hours, documenting disciplinary offences, with which the complainant became aware of the check that she had carried out on the service computer it handles. On ..., the complainant submitted the no. ... Apologetic Memorandum to the Commander, following which he received from ... Excerpt of Daily Order regarding the imposition of disciplinary punishment. The Authority, in the context of examination of the above complaint, sent to the DIPYN, under no. prot. C/EX/6429-1/07-10-2020 document to provide opinions, where in no. prot.

C/EIS/6905/09-10-2020 her response to the Authority stated, among other things, that because on ... there was a need to process a fire safety case, the Governor went to the complainant's office to use the protocol application to search for a pending case on the computer of the Fire Department and found that the computer was open in standby and power saving mode and immediately with the first movement of the cursor personal social networking pages and entertainment pages appeared on the screen, in a large number of concurrently open tabs and performed a history search to ascertain since when the pages are open. It was also mentioned that the computer in question is not personal but intended to serve official needs, with programs and applications that are necessary for the affairs of the Office. Finally, the Commander requested that the Authority inform him whether access to an official computer by a Head or Commander of a Service constitutes a breach of personal data and whether an employee's permission is required for the Commander of a service to use any of the computers belonging to it. 2 Then, the Authority with no. prot. C/EX/6429-2/18-12-2020 document, forwarded to DI.P.Y.N. for her information under no. prot. C/EIS/7099/15-10-2020 Memorandum of the complainant, which the complainant submitted to the Authority voluntarily, and invited it to answer a series of questions and in particular the following: a) when and what measures has the agency taken to its compliance with personal data protection legislation and to provide all of the documents in question, such as policies and procedures, b) to provide the Personal Data Protection Policy applicable to the service, mainly in relation to the use of electronic media by employees, indicating the date on which the employees became aware of its content, as well as any other relevant document, c) to document the Governor's claims for the actions he took on ..., presenting the evidence at his disposal, in particular to clarify and document if the search was only done in the browser history of the websites/social media or in any other files, such as locally stored files and/or on the internal disk of the complainant's computer, providing relevant supporting documents/records of said actions that can be extracted for the specific computer (e.g. logs), d) if a Data Protection Officer (DPO) has been appointed for the service. In the above questions, the DI.P.Y.N. replied with the no. prot. C/EIS/41/04-01-2021 document, without providing any of the above requested documents, stating that the staff consisting of two employees has a shared computer, on which all work is done and on which there is direct accessibility by employees without passwords, because there are no personal data files, employees are aware of the provisions concerning personal data, but without any proof being provided, and finally, that there has not been the slightest problem in this matter and that there is no Data Protection Officer. It was also reported that on ... after the Commander together with the Chief of Fire Safety determined that the use of the computer in question is mostly for personal matters, they shut it down, with no other action being taken other

than searching the internet history and without recording and data extraction. With reference to the second complaint under consideration, the complainant states that she requested on … copies of extracts of the Daily Order dated … and … concerning the imposition of disciplinary penalties and bearing her signature on the date 3 of their receipt by her. In the opinions presented by DI.P.Y.N. it was mentioned that "she (the complainant) states in the complaint against me that the requested documents have been served on her and bear her signature with the date of receipt by her ... . Therefore, there was no reason to re-grant Copies of Agenda Excerpts." The complainant, in the Memorandum that she voluntarily presented to the Authority regarding the views of the Administration, stated that "the copies that have been served to me do not have my signature and the date of receipt" and that she had not received any positive or negative written response to her request for the granting them. In view of the above, the Authority with no. prot. G/EX/664/17-02-2021, G/EX/665/17-02-2021, C/EX/666/17-02-2021 and C/EX/667/17-02-2021 calls called for hearing i. the complainant, A, ii. the Administration of Fire Services X (DI.P.Y.N.), iii. the Regional Fire Administration Ψ (PE.PY.D.), as the directly hierarchically superior Authority of the DI.P.Y.N., and iv. the Headquarters of the Fire Brigade (hereinafter "Headquarters" or "APS"), as the highest staff Service of the Fire Brigade, to attend the meeting of the Department of the Authority on 02-24-2021, in order to discuss the complaints under consideration and to present the their opinions. During the meeting in question, the complainant and among the complainants the new Governor of DIPYN were present. X, C, and the new Commander of PE.PY.D., D. Also present at the meeting was E, Data Protection Officer (DPO) of the Fire Brigade Headquarters, who appeared without having to provide clarifications following questions from Principle. At the beginning of the procedure, the respondents were asked by the Authority about which services have the status of data controller and none of them reserved to answer in a memorandum. Those present, after expressing their opinions orally, submitted to the Authority within the set deadline, on the one hand, the complainant under no. prot. G/EIS/1463/02-03-2021 memorandum and on the other hand the complained DI.P.Y.N. under no. prot. C/EIS/1573/05-03-2021 memorandum. The complainant during the above hearing and also with her memorandum pointed out, among other things, regarding the first complaint that she had not been informed by the service nor had he signed any policy document for the protection of the personal data of the employees that may be applied or the Regulation on the Use of Electronic Media, that the processing of personal data takes place without compliance with the legislation on personal data and without 4 compliance measures having been taken, as well as that she does not know what was seen on her computer during the audit. The Commander of PE.PY.D. during the above hearing he argued that in the context of their work there is no

concept of "my computer", as it belongs to the Service and is accessed by the Commander and the employees and therefore, there is no question of processing personal data and it cannot be requested permission to check the computer, as well as that there is no reason to refer to personal data since the issue concerns websites and social media visited by the complainant. He also stated that no GDPR compliance actions have been taken at the Services level, however, a responsible employee has been designated in the protocol and only those related to the subject have access. The Governor of DI.P.Y.N. during the above hearing, he informed the Authority that B, with whom the correspondence with the Authority had been exchanged, was a former Commander of the Service, as he has retired and in the Memorandum submitted by DIPYN. it was mentioned that in the context of the implementation of the GDPR and Law 4624/2019, the Service collects personal data of employees in order to compile the corresponding individual file of each individual employee and is in the process of being converted into electronic individual booklets, while "in any case where there is an issue of access to documents containing personal data (simple and/or sensitive) the Service addresses hierarchically to the Legal Support Directorate of the Fire Brigade Headquarters (A.P.S.), in order to ensure ad hoc compliance with the above special provisions, as well as with the provisions in art. 5 of Law 2690/99." He also stated that the Service is in the process of preparing a Civil Protection Policy, which also depends on the process of issuing the regulatory acts regarding electronic individual passbooks and "does not have computers with unique users, but only shared ones, the use of which is intended exclusively in the conduct and processing of official duties. Any use that deviates from these duties is not permitted. The control of the execution of the duties of the employees is left to the Commander of the Service (art. 19 of the decree 210/92). 3. Regarding A's complaints, we inform you that a Sworn Administrative Examination is underway. 4. Our Service has not appointed a separate Data Protection Officer, in the absence of an employee with the status of a legal officer, but addresses for an opinion on a case-by-case basis the Data Protection Officer of the APS, E. 5 It is pointed out that no answers were provided with the Memorandum presented by DI.P.Y.N. to the following questions raised during the hearing: a. if there are files with personal data on the computer that was checked, b. how do websites stay open for days without a password protecting the computer, and c. what are the personal data security measures taken by the Service. The Authority, after examining the elements of the file, the hearing procedure and after hearing the rapporteur and the assistant rapporteur, who withdrew after the discussion of the case and before the conference and decision-making, after a thorough discussion, CONSIDERED THE LAW 1. 2. It follows from the provisions of Articles 51 and 55 of the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR") and Article 9 of Law 4624/2019 (Government Gazette A´ 137) that

the Authority has the authority to supervise the implementation of the provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. In order for personal data to be lawfully processed, i.e. processed in accordance with the requirements of the GDPR, the conditions for applying and observing the principles of article 5 paragraph 1 GDPR1 must be met cumulatively. The existence of a legal basis (art. 6 GDPR) does not exempt the data controller from the obligation to comply with the principles (art. 5 para. 1 GDPR) regarding legitimacy, necessity and transparency2. In the event that any of the principles provided for in article 5 para. 1 of the GDPR is violated, the processing in question is considered illegal (subject to the provisions of the GDPR) and the examination of the conditions for the application of the other provisions and the legal bases of the article is omitted 6 GDPR. Thus, according to 1See Decision of the Court of Justice of the European Union (CJEU) of 16-01-2019 in case C496/2017 Deutsche Post AG v. Hauptzollamt Köln "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. CJEU decisions C-465/00, C-138/01, C-139/01, C-131 /12)". 2 Relatedly see L. Mitrou, the general regulation of personal data protection [new law-new obligations-new rights], published by Sakkoula, 2017 pp. 58 and 69-70. 6 3. 4. violation of the principles of Article 5 of the GDPR, unlawful processing of personal data is not cured by the existence of any lawful purpose and legal basis. In addition, the CJEU3 considered as a condition for the legitimate and legal processing of personal data the information of the subject of the data prior to the processing thereof. Furthermore, the controller, in the context of observing the principle of legitimate or fair processing of personal data, must inform the data subject that it is going to process his data in a legal and transparent manner4 and be in a position per at any time to prove his compliance with these principles5. The processing of personal data in a transparent manner is a manifestation of the principle of legitimate processing and is linked to the principle of accountability6, giving the subjects the right to exercise control over their data by holding the controllers accountable7. The collection and processing of personal data should not take place secretly or by concealing it from the data subject, as well as by concealing all necessary information, unless provided for by law, in compliance with the conditions of Article 8 ECHR, such as it is interpreted with the decisions of the ECtHR and always in the light of the principle of proportionality8. Pursuant to Article 4 para. 7 of the GDPR, the data controller determines the purposes and manner of data processing. The subjective field of application, in relation to the public sector, of the concept of controller, which is an

autonomous concept of Union law, and, in particular, in relation to the content of the terms public authority and public service, is related to the administrative organization of national legal orders. Fundamental to the determination of the controller is the functional criterion. In other words, a data controller is the one who determines the purpose and/or the essential, at least, elements of the processing method. The 3See his decision of 01-10-2015 in the context of case C-201/14 (Smaranda Bara). 4 See CJEU C-496/17 and CJEU C-201/14 of 01-10-2015 paras. 31-35 and especially 34. 5 Principle of accountability according to art. 5 para. 2 in combination with articles 24 para. 1 and 32 GDPR. 6 See APD decisions 26/2019, pp. 15-17, 43/2019, p. 14. 7 See Guidelines OE 29, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, pp. 4 and 5. 8 See Decision APD 43/2019, sc. 5. 7 5. 6. 7. defining the objectives and the manner is equivalent to defining, respectively, the "why" and the "how" of certain processing activities9. In the public administration, the said criterion is in principle concluded with the powers conferred by law on a specific authority, agency or legal entity under public law, which, moreover, should in practice be exercised by this entity. A structural element of the concept of the controller is the influence he exercises by virtue of exercising decision-making power, a competence that may be defined by law or may come from the analysis of the factual elements or circumstances concerning the case, while it is pointed out that it is a functional concept, which is intended to allocate powers where the factual influence lies. And according to the ESPD Guidelines 07/2020 "in most cases, the "determining body" can be easily and clearly defined by reference to certain legal and/or factual circumstances from which the "influence" can be inferred. unless other elementssuggest the opposite." According to the no. 115/2011 Directive of the Authority on the processing of personal data in employment relations, as follows from the principle of purpose, the collection and processing of personal data of employees is permitted exclusively for purposes directly related to the employment relationship and as long as it is necessary for the fulfillment of the obligations of both parties based on this relationship, whether they arise from the law or from the contract10. 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 data11, nor does it entail an exception from the relevant protection12, even when the data controller 9 See on the meaning of the controller and processor, Opinion 1/2010 of the O.E. of Article 29, as well as paragraphs 22 – 24 of the GDPR guidelines 07/2020 on the concepts of controller and processor in the GDPR. 10 Authority Directive 115/2011, p. 10, available on its website. 11 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. 12 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. 8 8. 9. 10. acts in the context of the exercise of his public duties13, while the protection of "private life" does not exclude professional life and is not limited to life within the place of residence. Therefore, to not accept that the processing of information related to professional life or taking place through information systems (e.g. computers) belonging to the employer constitute personal data would have the consequence of not respecting the principles and the protection guarantees and especially the control exercised by the control authority14. Employees have a reasonable expectation of privacy in the workplace, which is not abrogated by the fact that they use equipment, communication devices or any other professional facilities and infrastructure (eg electronic communications network, Wi-Fi, corporate electronic mailing addresses, etc.) of the employer15. The fact that the employer-public body may be the owner of the electronic means of communication (e.g. computers) does not lead to the deprivation of the employees' right to the protection of personal data, the right to the protection of the confidentiality of communications and relevant location data16. Access by the employer to personal data stored on the employee's computer constitutes processing of personal data17. The above applies in case of access to personal data contained in any storage medium or electronic communications system18, as well as in the history of website visits19. The employer in any case, in accordance with the principles of transparency and legality, should communicate and apply policies for the acceptable use of electronic media used by employees, which will describe the permitted use of the organization's networks and equipment 13 General Court of Justice T-496/13 McCullough decision of 11-6-2015 on the inclusion of the names of the data subjects in the meeting minutes regardless of the fact that they exercise public authority para. 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. 14 See CJEU C-434/16 decision Peter Nowak v Ireland Data Protection Commissioner of 20-12-2017, para. 49. 15 see APD decisions 43/2019, 34/2018, 61/2004. 16 See OE29 Opinion 2/17, p. 22. 17 See Decisions APD 34/2018 and 61/2004. 18 See Decisions APD 43/2019, request. 9 and 44/2019, application no. 22. 19 See ECtHR Mr. Barbulescu of Romania of 05-09-2017, sc. 72. 9 and the processing carried out in detail20, as well as the employer's ability to access the electronic media used by the employees21. The employer processes the personal data of the employees in principle based on their contractual relationship and exercising his managerial right for the orderly operation of the organization is entitled to exercise control over the electronic means of communication that he provides to the employees for their work, as long as the relevant processing, respecting the principle of proportionality, is

necessary for the satisfaction of the legal interest it pursues and on the condition that this obviously outweighs the rights and interests of the employee, without affecting his fundamental freedoms according to art. 6 par. 1 sec. to the GDPR and after the latter has been informed even about the possibility of a related control22. In this case, the fair and necessary balance should be achieved between the purposes of achieving the legitimate interests pursued by the data controller on the one hand23 and the respect of the reasonable and legitimate expectations of employees for the protection of personal data in the workplace, from the other. Regarding the right of access, taking into account articles 12 and 15 of the GDPR in conjunction with recital 63 of the GDPR, article 33 of Law 4624/2019 which introduces, by virtue of article 23 of the GDPR, restrictions on the right of access and as always the Authority accepts, the data subject has the right to know whether personal data concerning him or her are being processed, as well as to be aware of them, without the need to invoke a legitimate interest24 and every data subject should have the right of access to personal data collected and concerning him and to be able to exercise this right easily and at reasonable regular intervals, in order to be aware of and verify the legality of the processing. The data controller, in any case, has an obligation to respond, even if negatively, to a relevant 11. 20 OE article 29, Opinion 2/2017 regarding the processing of data at work, par. 3.1.2, 4, 5.3. 21 See for minimum fair use policy content OE29 Working paper on the surveillance of electronic communications in the workplace WP55 of 29.5.2002 and Authority Decision 34/2018. 22 See in detail Authority Decision 34/2018 and 43/2019. 23 See OE29, Opinion 2/2017 on the processing of data at work, p. 4. 24 See in particular, Decisions of the Authority 32/2019, 144/2017 195/2014 193/2014 and 75/2011 10 12. 13. 14. request of the subject25, while the non-response is an independent violation of the GDPR. Finally, regarding the Data Protection Officer (hereinafter DPO), in accordance with articles 37 of the GDPR and 6 of Law 4624/2019, it is recognized as a key component of the new data governance system and the conditions for the definition, position and his duties. According to the aforementioned provisions of the GDPR and Law 4624/2019, it is possible to define a DPO for several public authorities or bodies, but in this case, the data controller or the processor must26 ensure that the only data protection officer , assisted by a team if required, can effectively perform all his duties for all public authorities and public bodies to which he has been appointed27. In the first complaint under consideration, from the data in the file and from the hearing procedure, the following emerged: The public services - authorities summoned to the hearing (public bodies according to art. 4 section a' cond. 2 section a' Law 4624/2019) in the context of their hierarchical structure, they were unaware and had not determined internally, in the context of the required factual analysis according to the above, who or which had the status of data controller, even at the time of the hearing

before the Authority. Therefore, any kind of processing of personal data took place without determining the purpose and manner of processing of personal data by a specific public authority or service pursuant to art. 4 par. 7 GDPR. As a consequence of the lack of internal determination among most public services-authorities regarding the status of the data controller, there was on the one hand the complete absence of taking measures to comply with the requirements of the GDPR and Law 4624/2019 through the application of the appropriate technical and organizational measures ' No. 5 para. 1 cond. 24 par. 1,2 and 32 par. 1, 2 GDPR (ref. s. 78 GDPR), on the other hand, the inability of each data subject (such as the complainant in this case) to be informed about the organization 25 See SC Decision 2627/2019, Authority Decision 43/2019, request. 20. 26 See Guidelines "on data protection officers" issued by the Working Group of article 29 27 WP 243 rev. 01 of 13.12.2016, as last revised and approved on 05.04.2017, p.14, available on the website https://edpb.europa.eu 11 who has the role of controller for the exercise of his rights and by extension for the possibility of ensuring fair and transparent processing (art. 60 GDPR), as well as to verify the legality of the processing (art. 63 GDPR). The complete lack of compliance with the requirements of the GDPR and Law 4624/2019, including the absence of the application of personal data protection policies, beyond what was established by the Authority in the context of the present procedure, as will be demonstrated in detail below, was additionally confirmed by: the under no. prot. G/EIS/6905/09-10-2020 response of the DI.P.Y.N. through its former Commander to the Authority, with which he submitted a request for information on whether it is a breach of personal data to access an official computer by a Head or Commander of a Service and whether an employee's permission is required for the Commander of a service to use any of the computers that belong to it, a fact which proves the complete absence of knowledge and application of the provisions of the GDPR and Law 4624/2019, the failure to send any data protection policy and any document or any other type of proof of compliance with the requirements of the GDPR and Law 4624/2019 in response to No. prot. C/EX/6429-2/18-12-2020 document - request for production of the Authority, the non-production of any proof that the employees are aware of the provisions concerning personal data if the DIPYN . with the no. prot. C/EIS/41/04-01-2021 her document invoked the relevant information of the employees, the admission with the no. prot. C/EIS/41/04-01-2021 document of the DI.P.Y.N. that there is no Data Protection Officer, the oral position and admission of the Commander of the PE.PY.D during the hearing before the Authority that at the level of services no actions have been taken to comply with the GDPR, the hearing memorandum of the DI.P.YN . in which "[…] our Service is in the process of drafting a Civil Protection Policy for the fuller information of employees" and therefore the processing of personal data takes place without taking technical and

organizational compliance measures, - - - - - - 12 - - - 15. the admission of DI.P.Y.N. with the no. prot. C/EIS/41/04-01-2021 its document, according to which "the staff in question has a shared computer [...] without passwords...", the hearing memorandum of the DI.P.YN. in which "[…] 4. Our Service has not appointed a separate Data Protection Officer, in the absence of an employee in the capacity of a legal officer, but addresses for an opinion on a case-by-case basis the Data Protection Officer of the APS...", but without providing any proof that has at any time appealed to the DPA of the APS for an opinion, but did not previously present this claim during the hearing before the Authority in the presence of the DPA of the APS, when the Authority would have requested relevant clarifications from the DPA of the APS, the complete absence of answers to the with hearing a memorandum regarding the questions raised by the Authority during the hearing and in particular "a. if there are files with personal data on the computer that was checked, b. how do websites stay open for days without a password protecting the computer, and c. what are the personal data security measures taken by the Service". The Headquarters of the Fire Brigade is the highest staff service of the Fire Brigade, whose competence as a central service extends throughout the Territory and to which the decentralized services with local competence are subordinated in order of hierarchy, i.e. the Regional Fire Administration Ψ (PE.PY .D.) and the reported Administration of Fire Services of Prefecture X (DI.P.Y.N.) 28. Also, "the operation of the offices and the general conduct of the service in them is the responsibility of the Commander, in accordance with the legislation which applies and the relevant orders of the Fire Brigade Headquarters"29. The Headquarters as a public body, which in the context of its powers and duties acts as a data controller, as it determines the purpose and/or the essential elements, at least, of the method of data processing that it should apply, as well as the services and units that fall under it, processes personal data of the employees working in it, of 28 Law 3511/2006 Reorganization of the Fire Brigade, upgrading its mission and other provisions (Government Gazette 258/A/27-11-2006), as amended 29 art. 19 P.D. 210/1992 Codification of provisions of Presidential Decrees of the Internal Service Regulation of the Fire Brigade. (Official Gazette 99/16-06-1992). 13 16. 17. of the suppliers who are citizens/natural persons, as well as any cooperating with him, must comply with the personal data protection framework, as long as the legal bases provided for in Article 6 GDPR exist, and the processing principles of article 5 of the GDPR, taking into account that a sufficient period of time has now passed since the entry into force of the GDPR and Law 4624/2019. The Headquarters as the controller, within the framework of the principle of accountability, is obliged to design, implement and take the necessary technical and organizational measures, including the design and implementation of the necessary policies and procedures according to art. 24 par. 1, 2 cond. 32 par. 1, 2 GDPR30

in order for the processing of the data to be in accordance with the relevant legislative provisions and to be able to demonstrate compliance with them. Furthermore, because in the public administration the hierarchy is a way of its internal organization that aims to ensure the uninterrupted continuity of its work31 and the coherence of the rules applied between the units and services that fall under the higher body of the organization and because the operational criterion is concluded in principle with the powers granted by law to a specific authority, service or legal entity under public law, which, in addition, should in practice be exercised by this body, the Authority finds that the Headquarters of the Fire Brigade should , as the staff authority of the House and acting as data controller to have taken all the necessary actions to comply with the legislative framework for the protection of personal data, by drawing up policies and procedures, including the Regulation on the Proper Use of Electronic Media, which should have been implemented by the services and the units that fall under them and administratively in this and in this case and the DI.P.Y.N. For this reason, although the Headquarters has already appointed a Data Protection Officer, to whom the D.I.P.Y.N. could be addressed for advice and opinion on a case-by-case basis, as stated in the Memorandum submitted by DIPYN. after the hearing, although no evidence emerged from personal data protection of the 30 See and request. 78, 82, 83, 87 GDPR and Decision APD 44/2019 sc. 16 for appropriate accountability measures. 31 X. Akrivopoulou, X. Anthopoulos, Introduction to Administrative Law, Hellenic Academic Electronic Publications, 2015, Chapter 3, p. 77. 14 that the DI.P.Y.N. had requested the assistance of the Ministry of Foreign Affairs. On the contrary, it is pointed out that, although the Memorandum after the hearing was submitted to the Authority by the D.I.P.Y.N. considering that it has the role of controller, however, the Authority finds that the Headquarters, based on the administrative and operational criteria, becomes the controller of the personal data processed by the existing services and units of the Fire Brigade, and not the DI .P.Y.N. Regarding the specific complaint, it was established that the complainant was the "main operator", as stated by the former Director of the DIPYN, of a specific computer, as she spent most of her working time on it . Even in case of use of the computer by herself for personal (non-business) reasons such as e.g. sending from her e-mail personal correspondence or browsing websites for her personal information, this is processing of personal data. In addition, the fact that the complaint concerns personal data generated by the use of electronic means of communication and therefore touches on the right to privacy of personal data in the field of electronic communications and therefore concerns the core of the relevant individual right, makes it incontrovertible that it takes place processing of personal data, as well as that there is an obligation of the public body to protect them. From the memoranda submitted to the Authority and from the hearing process, it appears that the

DIPYN, as subordinate to the Headquarters, did not apply any kind of technical and organizational measures to comply with the requirements of GDPR and Law 4624/2019, did not apply personal data protection policies, nor implemented an internal Regulation for the proper use and operation of IT and communications equipment and networks by employees, from the content of which it would appear on the one hand that the use of computers for personal purposes was prohibited, on the other hand, the possibility and the possible control of these, the conditions, terms, procedure, scope and guarantees of carrying out the control. The important and crucial thing in the complaint under consideration is that the data controller had not designed and therefore neither implemented any policy and/or procedure regarding the processing of personnel data 15 18. 19. character of the employees, nor Regulation of the Proper Use of Electronic Media32 , so that the employees have been regulated and informed about the context in which the processing of personal data will take place both by the management/employer and by the employee33. In view of the Authority's finding that the Head Office is the controller, even if it is considered that the D.I.P.Y.N. developed relevant allegations at the hearing but also in the presented memoranda, even on behalf of the Headquarters, they are rejected. In particular, with regard to the claims that "[…] the computer in question is not personal but to serve official needs, with programs and applications that are necessary for the affairs of the Office, [...] there is accessibility for other employees as well, and for the for this reason, there is no question of personal data processing and permission cannot be requested to check the computer", and "our Service does not have computers with unique users, but only shared ones, the use of which is intended exclusively for conducting and processing the official duties. Any use that deviates from these duties is not permitted. The control of the execution of the duties of the employees is left to the Commander of the Service (art. 19 of the decree 210/92)" and "[…] there is no reason to refer to personal data since the issue concerns websites and social media that visited the complainant", since, according to the Authority's jurisprudence34 and what has been mentioned above in paragraphs 7-9, it constitutes processing of personal data and the GDPR and Law 4624/2019 apply in a case where an employee processes data using electronic equipment , communications network and any other professional facilities and infrastructure owned by the employer and the legitimate expectation of protection of the employee's private life is not removed, because he is at the place of work and processes personal data for non-official employer - controller wishes to prohibit the use of any kind of electronic means of communication for personal reasons (e.g. e-mail personal computer, network (professional) If the reasons. 32 See Authority Decision 34/2018 p. 12 ff. 33 See Authority Decision 34/2018, p. 15 ff. 34 See Authority Decisions 34/2018, 43/2019, 26/2019. 16 of communication, e-mail, internet

access, etc.), must have previously informed the employee-data subject of its relevant policy. In addition, it should be noted that in addition to the above-mentioned provision of no. 210/92 P.D., in which it is provided that "the operation of the offices and the general conduct of the service in them is the responsibility of the Commander, in accordance with the legislation and the relevant orders of the Headquarters of the Fire Brigade", and the provisions of Law 3528/200735 invoked by DI.P.Y.N. in the summons to the employee's apology, where even they do not provide what is the correct or illegal use of the electronic media for which the complainant here is accused as an employee, the employees of DI.P.Y.N. they have not been informed by an internal document about the correct use of the electronic means of the service and the processing of personal data in general. In this case, the Headquarters, as the controller, did not prepare and implement relevant policies, nor did it inform the employees that the use of the electronic means of communication available for the provision of the work due may be prohibited. Furthermore, it should be pointed out that the Headquarters as controller is burdened with the obligation to take the appropriate organizational and technical measures in order to ensure the appropriate level of data security against risks, in accordance with the security principle of article 5 par. 1 sec. f', 24 par. 1, 2 and article 32 par. 1, 2 GDPR. A breach of personal data means a breach of security that leads to the accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed. As long as the personal data of either the employee himself or other natural persons are processed on the computer used by an employee, the controller must have taken the appropriate technical and organizational security measures, such as at least the provision and application of codes 20. 35 art. 107 § 1, Chapter A', Section A', of Part E' "DISCIPLINARY LAW" of Law 3528/2007, disciplinary offenses are: k) the refusal or failure to perform a service, kc) wear and tear due to unusual use, abandonment or the illegal use of a thing, which belongs to the service, and k) the negligence or incomplete fulfillment of the official duty. 17 access/security to the computers corresponding to each operator, which will be private and not shared, while the relevant security measures should be included respectively in a Security Policy. In this case, it appears from the information in the file that this particular computer does not have a password/security and the service files can be accessed by anyone who seeks it. Furthermore, from the documents in the file itself, it appears that the appropriate technical and organizational security measures have not been taken to authenticate and identify the authorized access of each authorized user of the computer, while anyone could have access to the included personal data third. It happens that the claim of DIPYN is rejected. which was mentioned under no. prot. C/EIS/41/04-01-2021 its document, according to which "the staff in question has a shared computer [...] without passwords,

because there are no personal data files", in principle because it relies on incorrect condition. From the information in the file and the hearing, it emerged that processing of personal data takes place using the computer in question and the application complies with the GDPR and Law 4624/2019, regardless of the fact that the computer belongs to the data controller and that it is carried out processing of personal data to achieve the purposes of the public body, as mentioned above. In addition, because the data controller, although burdened with the obligation of accountability according to art. 5 para. 2 GDPR to prove his compliance with the processing principles of Article 5 para. 1 GDPR, he did not provide any answers, nor any evidence to the individual questions submitted during the hearing regarding i. if there are personal data files on the computer in question, ii. how do websites stay open for days without a password protecting the computer, and iii. what are the personal data security measures taken by the Service. From the elements of the file, the hearing process and the memoranda of the parties, it emerged that the former Governor of DIPYN. carried out a check of the website visit history of the official computer operated by the complainant in the Department … and from which (check) it was established that she had visited social networking and entertainment websites on … and during working hours. 18 21. The above finding is included on the one hand as a disciplinary offense attribution in no. ... call of the Governor DI.P.Y.N. X in apology of the complainant here. On the other hand, in no. prot. G/EIS/6905/09-10-2020 response of the DI.P.Y.N. to the Authority, it is understood that the former Governor conducted a history search, in order to ascertain when the pages have been open. Therefore, the belatedly submitted claim in which the former Governor of DI.P.Y.N. he did not check and search the history of visits to the websites, but opening the computer he found, without checking, a large number of tabs opened at the same time, it is rejected. Therefore, it emerged that the former Governor of DIPYN. acting within the administrative structure as part of the controller, audited the accesses of the last operator of the shared and password-free computer to the visit history of the websites and so in the control of personal data during the use of electronic means of communication without having previously informed any of the users of the shared computer both about the control and whether the use of the official computer, means and communication network is permitted or prohibited, without relevant personal data protection policies, security policy and Regulation for the correct use and operation of IT and communications equipment and network by employees have been drawn up and implemented. It did not appear that the complainant was the employee who last used the particular shared computer in turn, given that access to it was allowed to every employee of the service and indeed without having previously been assigned a different password for each person. Therefore, from the above data, on the one hand, it emerged that a history check of visits to social networking websites by a

user - employee of the service took place, on the other hand, it did not emerge that the check related to the processing of the complainant's personal data. In view of the above, with regard to the first complaint, from the entire file and the hearing process, it appears that the Headquarters of the Fire Brigade is responsible for processing the data processed through the shared computer operated by the employees of the departments/units under in this for the 19 achievement of processing purposes linked to the mission of the Fire Brigade. This processing is automated and includes personal data of both employees and citizens and is carried out on the one hand for the former in the context of the employment relationship and on the other hand for citizens to fulfill the duty of the data controller in the public interest. It appears, however, that the processing in question is not in accordance with the legislation on the protection of personal data, in particular with the GDPR and Law 4624/2019, as the appropriate technical and organizational measures have not been taken to implement the framework in question , according to art. 5, 24 par. 1, 2 of the GDPR, and to ensure the appropriate level of security against risks, according to art. 32 par. 1, 2 of the GDPR. The complete lack of policies and procedures, including security policies and Regulations for the proper use and operation of IT and communications equipment and network by employees makes any processing of personal data that takes place through the computer contrary to Articles 5, 24 para. 1, 2, 32 para. 1, 2 GDPR, violating the principles of legality and transparency according to art. 5 par. 1 sec. a' GDPR, as well as security in accordance with paragraph f of the same provision due to a lack of security policies combined with the principle of accountability according to art. 5 par. 2 GDPR. With reference to the fact that it has been appointed by the Headquarters of the Fire Brigade, which acts as a data controller according to the above, one (1) Data Protection Officer (DPO) for all services and responsibilities of the Headquarters and its supervised services and units, without exception, the Authority finds that yes according to art. 37 par. 3 GDPR cond. 6 par. 2 of Law 4624/2019 if the controller is a public authority or public body, it is possible to designate a single DPO, but its organizational structure and size are taken into account. In this case, it emerged that the controller did not ensure that the sole DPO is sufficient and has the ability to participate properly and in a timely manner pursuant to art. 38 par. 1 GDPR cond. 7 par. 1 of Law 4624/2019 in all matters related to the protection of personal data in order to exercise the rights under Art. 39 par. 1 GDPR cond. 8 Law 4624/2019 its duties, including that which concerns the monitoring of compliance with the GDPR and Law 4624/2019 20 22. 23. 24. including accountability and relevant (internal) controls pursuant to . 39 par. 1 sec. 2nd GDPR comp. 8 par. 1 sec. second law 4624/2019. Therefore, the Authority finds that the data controller does not correctly apply the obligations arising from the provisions of art. 38 par. 1 GDPR cond., 7 par. 1 Law 4624/2019 in relation to

the duties of the DPA pursuant to art. 39 par. 1 sec. 2nd GDPR comp. 8 par. 1 sec. second law 4624/2019. With reference to the second complaint, the complainant exercised her right to information and access to the D.I.P.Y.N. on ..., to which no response was received. After forwarding the said complaint to the DI.P.Y.N. by the Authority for the provision of opinions by the complainant, the said service with the G/EIS/8012/23-11-2020 electronic message replied for the first time and only to the Authority (not to the complainant) that it considered that there was no reason to new granting of copies of Excerpts of the Agenda, as they had already been served on the complainant. The public body as data controller and the services acting on its behalf, have an obligation to respond with reasons to the subject's access request, even negatively, in a case where, in the opinion of the data controller, there is no legitimate reason to satisfy the request. If the data controller does not act on the data subject's request, he shall inform the data subject within one month of receipt of the request of the reasons for not acting and of the possibility of filing a complaint with a supervisory authority and taking legal action (Article 12 par. 4 GDPR). It is pointed out that the data controller, even when he does not keep a file with the subject's data, is not released for this reason from his obligation to respond even negatively to a relevant request for information and access36. The controller's failure to respond to the subject's request for access and information about his personal data constitutes an independent violation of the GDPR and Law 4624/2019, as the subject in the present case did not receive a response, which was only given to the Authority following the submitted complaint. In continuation of what has been mentioned in relation to the first complaint, it should be pointed out the fact that the complainant did not even receive a negative response from the service, as a result of the lack of internal compliance procedures with 36 See Decisions SC 2627/2017 and APD 43/2019. 21 the personal data protection framework and specifically with the satisfaction of the subjects' rights. Therefore, the Authority considers that the data controller as a public body has violated articles 15 par. 3 in combination with article 12 of the GDPR and with article 33 par. 2 of Law 4624/2019 for not satisfying the right of access of the subject. According to the GDPR (ref. sc. 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 a minor offence, or if the fine that might be imposed 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 and Law 4624/2019 as stated above, taking into account recital 148 of the GDPR and in addition, in addition to the above, in particular: The Guidelines for the implementation and determination of administrative of fines for the purposes of

Regulation 2016/679 issued on 03-10-

2017 by the Article 29 Working Group (WP 253) and having duly taken into account the provisions of articles 58 par. 2 and 83 GDPR to the extent that they apply in this particular case and of article 39 par. 2 of Law 4624/2019 and in particular which of the prescribed criteria pertain to the specific case examined by the Authority: A. Regarding the case of processing personal data of an employee in violation of the principles of legality, transparency and security pursuant to art. 5 par. 1 sec. a' and f', 24 par. 1. 2 and art. 32 par. 1, 2 of the GDPR combined with the principle of accountability according to art. 5 par. 2 GDPR and B. Regarding the improper implementation of the obligations of the data controller arising from the provisions of art. 38 par. 1 GDPR cond. 7 par. 1 Law 4624/2019 in relation to the duties of the Ministry of Foreign Affairs according to art. 39 par. 1 sec. 2nd GDPR comp. 8 par. 1 sec. second law 4624/2019 22 25. the Authority after taking into account a) the nature, gravity and duration of the breach, the extent or purpose of the relevant processing, as well as the number of personal data subjects affected by the breach and the degree of damage suffered by them and specifically : i. the fact that the Headquarters of the Fire Brigade violated the provisions of article 5 par. 1 sec. a' and f' of the GDPR principles of legality, transparency, security and accountability, i.e. violated fundamental principles of the GDPR for the protection of personal data. ii. the fact that, although article 39 par.1 applies to administrative sanctions of the public entity, the violation of the above principles is subject to the provisions of article 83 par. 5 sec. a' GDPR in the highest prescribed category of the GDPR administrative fine classification system, if it is deemed necessary to impose them. iii. the fact that the violation of the principles of article 5 par. 1 sec. a', f' 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. iv. the fact that the violation of the principles of article 5 par. 1 sec. a', f' and par. 2, 24 par. 1, 2, 32 par. 1 and 2 of the GDPR concerned personal data generated by the use of electronic means of communication and thus concerns the right to the privacy of personal data in the field of electronic communications and therefore concerns the core of the relevant individual right. v. the fact that the violation of the principles of article 5 par. 1 sec. a', f' and par. 2, 24 par. 1, 2, 32 par. 1 and 2 of the GDPR in addition to the complainant concerned also every user of the shared computer in question, so that it is not an isolated or opportunistic violation of burden of a specific employee but for a violation that has a systemic (structural) nature, as it concerns compliance with the framework for the protection of personal data processing and the complete lack of policies and procedures of the data controller. vi. the fact that three (3) years have already passed since the GDPR came into force and the data controller has not taken due care to comply with its provisions. 23 b) any actions taken by the controller to

mitigate the damage suffered by the data subjects It has not been established that the controller has taken actions to mitigate the damage suffered by the complainant. c) with regard to any relevant previous violations of the data controller, it follows from a relevant check that no administrative sanction has been imposed by the Authority to date. d) 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. e) the way in which the Authority was informed of the violation, in particular if and to what extent the data controller notified the violation In this case, the Authority was informed of the finally established violations following a complaint by an employee/data subject. f) any other aggravating or mitigating factor resulting from the circumstances of the specific case The fact that, while the DPO is a basic accountability tool, the data controller did not use it in order to achieve the required compliance with the requirements of the GDPR and Law 4624 /2019. C. Regarding the case of violation of articles 12 and 15 GDPR, as well as article 33 par. 2 of Law 4624/2019 in relation to the violation of the right of access, the Authority after taking into account a) the nature, gravity , the duration of the breach, the extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage suffered by them, specifically: i. the fact that the company violated the right of access and information of one (1) data subject regarding his access to personal data by granting a copy thereof which is also due to the absence of policies and procedures to satisfy the rights of personal data subjects. ii. the fact that, although article 39 par. 1 applies to the administrative sanctions of the public body, it follows from the provisions of article 83 par. 5 para. b GDPR that the violation of the rights of the subjects falls under the higher 24 prescribed category of the system gradation of administrative fines of the GDPR, if it is deemed necessary to impose them. iii. the fact that, from the elements brought to the attention of the Authority, no material damage occurred to the data subject-complainant from the non-satisfaction of her right, nor did the complainant claim any relevant damage. iv. the fact that in the response provided by the complained service to the Authority with G/EIS/8012/23-11-2020 electronic message it stated that it considered that there was no reason to re-grant copies of Excerpts of the Agenda, as they had already been served to the complainant. From this response to the Authority, it appears that the complained-about service was not properly aware of its obligation to respond even negatively to the complainant. In view of the above, the non-response to the subject was the result of the controller not providing orders, policies and procedures to the services and/or units acting on his behalf and on his behalf. b) any actions taken by the controller to mitigate the damage suffered by the data subjects No actions were found to comply with GDPR requirements. c) with regard to any relevant previous violations of the data controller, it follows from a

relevant check that no administrative sanction has been imposed by the Authority to date. d) 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. e) the way in which the Authority was informed of the violation, in particular if and to what extent the data controller notified the violation In this case, the Authority was informed of the finally established violations following a complaint by the subject. f) any other aggravating or mitigating factor resulting from the circumstances of the specific case The fact that, while the DPO is a key accountability tool, the data controller did not utilize it in order to achieve the required compliance. 25 THE AUTHORITY Having taken into account the above Because it decided pursuant to article 58 para. 2 GDPR and 15 para. 4 Law 4624/2019 to exercise its corrective powers in cases A, B and C for which a violation of the GDPR was found and of Law 4624/2019. Because pursuant to the provision of article 58 par. 2 sec. 4th GDPR cond. 15 par. 4 sec. b. Law 4624/2019, the Authority decided to instruct the Headquarters of the Fire Brigade as controller to comply with the provisions of the GDPR and Law 4624/2019 for cases A and B by taking all appropriate technical and organizational measures including the preparation and implementation of policies and procedures so that all the services and/or units supervised by it comply accordingly, within the framework of the principle of accountability in order to make the processing operations that take place via the computer comply with the provisions of the GDPR and of Law 4624/2019. Because the above order should be executed within two (2) months from the receipt of this, informing the Authority accordingly. Because the Authority considers that in all cases A, B and C, based on the circumstances established, it should apply the provision of article 58 par. 2 sec. i GDPR cond. 15 par. 6 of Law 4624/2019 to impose an effective, proportionate and dissuasive administrative fine according to Article 39 par. 1 of Law 4624/2019, both to restore compliance and to punish this illegal behavior37. Because with regard to all cases A, B and C for the violations found by the Authority of the provisions of articles 5, 12, 15, 32, 38, 39 of the GDPR and 33 par. 2 of Law 4624/2019 it is provided by the article 39 par. 1 of Law 4624/2019 imposition of an administrative fine up to EUR 10,000,000.00. 37 See OE 29, Guidelines and the application and determination of administrative fines for the purposes of regulation 2016/679 WP253, p. 6. 26 FOR THESE REASONS THE AUTHORITY A. Orders the Headquarters of the Fire Brigade, as, within two (2) months from the receipt of this notice, informing the Authority: i. comply with all the provisions of the GDPR and Law 4624/2019 by taking all necessary and appropriate technical and organizational measures including the preparation and implementation of policies and procedures, so that all the services and/or units supervised by it comply accordingly, in within the framework of the principle of accountability, in order to make the processing operations that take

place via the computer in accordance with the provisions of the GDPR and Law 4624.2019, within the framework of the principle of accountability in accordance with what is contained in the explanatory statement hereof, ii. take the appropriate measures, in order to restore the correct application of his obligations as data controller arising from the provisions of article 38 par. 1 GDPR cond. 7 par. 1 of Law 4624/2019 in relation to the duties of the Ministry of Foreign Affairs according to article 39 par. 1 sec. 2nd GDPR comp. 8 par. 1 sec. second law 4624/2019, iii. instruct the Administration of Fire Services of Prefecture X to provide a reasoned response to the complainant's access request in accordance with article 15 par. 3 of the GDPR. B. Imposes the following effective, proportionate and dissuasive administrative monetary fines on the Headquarters of the Fire Brigade thatappropriate to the specific cases, according to the special circumstances

of these, which are as follows:

1. regarding case A', for the violation of article 5 par. 1 sec. a',

f', 2 (comp. 24 par. 1, 2), as well as of article 32 par. 1 and 2 of the GDPR, the

administrative fine of twenty-five (25) thousand (25,000.00) euros.

2. regarding case B', for the violation of his obligations as

data controller resulting from the provisions of article 38 par. 1

GDPR cond. 7 par. 1 of Law 4624/2019 in relation to the duties of the Ministry of Foreign Affairs according to Article 39

par. 1 sec. 2nd GDPR comp. 8 par. 1 sec. b' n. 4624/2019, the administrative money

a fine of five thousand (5,000.00) euros.

27

3. regarding case C', for the violation of article 15 par. 3 in

combination with article 12 of the GDPR, as well as article 33 par. 2 of n.

4624/2019, the administrative fine of five thousand (5,000.00)

euro.

The Deputy President

George Batzalexis

The Secretary

Irini Papageorgopoulou