Athens, 20-12-2022 Prot. No.: 3371 DECISION 68/2022 (Department) The Personal Data Protection Authority met at the invitation of its President in a teleconference meeting on Wednesday 27-

07-2022 and time 10:30, in order to examine the case mentioned in the history of this present. The Deputy President of the Authority, Georgios Batzalexis, obstructing the President of the Authority, Constantinos Menoudakos, the alternate members of the Authority, Demosthenes Vougioukas and Maria Psalla, appeared, in place of the regular members, Constantinos Lambrinoudakis and Grigorio Tsolias, who, although legally summoned in writing, did not attend due to disability, and Christos Papatheodorou as rapporteur. Present without the right to vote were Stefania Plota, specialist legal scientist, as assistant rapporteur 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/2640/19-04-2021 complaint to the Authority the Association of Employees of the Athens Psychiatric Hospital (hereinafter "complainant Association" or "Association"), complains i. the Athens Psychiatric Hospital (hereinafter "Hospital" or "PSNA"), ii. the company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. (hereinafter "Company"), and iii. doctor A (hereinafter "complained Doctor" or "Occupational Doctor") "for illegal processing and use of sensitive personal data of the working members of the Association". Specifically, according to the complaint, PSNA entered into a contract on 12-28-2020 1-3 Kifissias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 and for one year with the company PRO.EX.OE for the provision of an Occupational Doctor by the company in PSNA who was doctor A. In March 2021, employees of the Hospital made complaints to the Association, as from a check they carried out on their personal record in EOPYY, they appear themselves to have received visits worth ten (10) euros from the EOPYY and to have made them to the doctor, on specific dates, which never took place, according to the complaint. The Association immediately informed its members and then it emerged that dozens of employees, researching their records in the EOPYY, found similar visits to the doctor in question, worth ten (10) euros each, to be recorded. The complainant Association presented the signed contracts and indicatively some certificates from the EOPYY concerning employees of the Hospital, in which the visits in question are recorded and claims that the Hospital violated articles 6, 22 par. 3, 26 par. 2 and 3, 45, 46, 62 and 63 of Law 4624/2019, resulting in the illegal processing of employees' data, as well as that without their consent he provided sensitive personal data to a third private company, he did not take all the necessary measures with controls and investigations to protect them and did not notify the employees, nor their trade union, of the data breach. Also, the Association claims that serious responsibilities arise from the contracting Company because it violated the provisions of Law 4624/2019

and the contract which led to the illegal processing and use of the employees' personal data and finally, the doctor is responsible for the illegal processing of sensitive data of the employees, as well as for the use of the data for selfish purposes beyond the framework of Law 4624/2019 and the purpose for which it was granted. The Authority, in the context of examining the above complaint, sent the documents for providing opinions with no. prot. C/EXE/1786/27-07-2021 to the first two defendants and with no. prot. C/EXE/1834/06-08-2021 to the complained doctor. The Hospital replied with the no. prot. C/EIS/5383/23-08-2021 document, stating that the doctor has been allocated as an Occupational Physician at the Hospital by the 2nd Company with relevant contracts and had called it with the no. first ... document to provide explanations for the doctor's illegal behavior, failure to observe and maintain the confidentiality of information in violation of the above agreements and the Appendix entitled "Protection of personal data". Also, the Hospital reports that with the no. 6/25-02-2021 His decision approved the non-acceptance of the provision of the Company's services, until he responds fully and thoroughly to what is stated in the document in question for explanation and then with the no. 21/16-06-2021 Decision of the Board of the Hospital the Company was declared bankrupt. Finally, the Hospital reported that on the matter in question it made a report to Mr. Athens Malpractice Prosecutor, the EOPYY regarding the doctor's actions, notification of a personal data breach incident to the Authority and informed the Ministry of Health and the Health Expenditure Control Service of Social Agencies Insurance. The company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. forwarded to the Authority under no. prot. C/EIS/4989/28-07-2021 letter of the contact details of Doctor A "with every reservation", due to the interruption of the Company's cooperation with the doctor and subsequently with the No. prot. C/EIS/5684/09-09-2021 electronic message, the company submitted to the Authority a memorandum with its views and the documents attached to it, in which it states that contracts have been concluded between the Company and the Hospital with the object of disposal an Occupational Doctor to provide services in accordance with the provisions of the Code of Laws for the health and safety of workers (hereafter K.N.Y.A.E.) and then the company contracted with the doctor with the Independent Provision contracts Services and Partner Confidentiality. In execution of the above agreements, together with the Hospital, they assigned the said duties to the doctor in writing, signing the relevant document tripartitely, and with the approval of the Hospital, the doctor was hired as the processor for all the withdrawals from the Company services and not for part of them. The Company reports that the Hospital had issued a certificate of good cooperation with the Company regarding the execution of the contract regarding the services of the Occupational Physician for the period 3 from 05-13-2019 to 05-12-2020, the responsibilities and the duties of the Occupational

Physician are provided for in the K.NY.A.E., as well as what emerges from the contract for the Provision of Independent Services that the doctor in question was not under the orders and instructions of the Company during the performance of his duties , while in article 3 par.1 of Law 3418/2005 (Medical Code of Ethics) it is defined that "Each doctor enjoys, in the exercise of the medical profession, scientific freedom and freedom of conscience, and provides his medical services with respect for human dignity." Also, the Company claims that from the confidentiality agreement it follows that the doctor undertook not to use any confidential information for his own benefit or on behalf of a third party and has sole responsibility for the safe management (storage, processing) of the information he receives from the Company or its customer and the processing of the above information carried out by the partner will be exclusively in accordance with the requirements of the Company and will satisfy the requirements of the applicable legislation on personal data. The Company reports that, by virtue of the letter dated 02-15-2021, it was informed by the Hospital that for several of its employees it was found that billed visits by the Occupational Physician appear in the EOPPY system, but without these having taken place and it was asked to meet at the Hospital which terms of the contracts provide for the Occupational Physician to charge visits to the EOPYY without the physical presence of the employees and their consent. As soon as the company became aware, it took the decision to terminate cooperation with the said Doctor for the specific institution, asked him for a written explanation for his illegal behavior reported by the Hospital and decided to conduct an investigation into any other similar actions by him and notified her said decisions at the Hospital, replacing the doctor with another person. On 03-22-2021 the Company responded to the Hospital that the doctor, since he committed the alleged acts, did not act as an agent of the Company and that his conduct was not causally related to the duties he had undertaken, while at the same time sending the Hospital the relevant form for the replacement of the complained doctor by another doctor and invited him to sign it, 4 in order to continue the implementation of the cooperation between them. Subsequently, the Company proceeded to terminate the contract with the complained doctor and to file a Summons-Summon Report against him to the Athens District Attorney for committing the offenses of fraud, forgery and illegal use of personal data and filing a complaint with the Athens Medical Association .The Company also reports that the AMKA of the employees of the Hospital was not part of the medical files of the employees that were kept in the context of the provision of Doctor services of Work and the doctor in question did not gain access to the workers' health insurance from the employees' personal medical files (A.I.F.), which he kept in the context of his duties as a Work Doctor, but possibly from other personal files kept at the Hospital data and outside his competences. The appointed Occupational Physician did not act as an employee of the

Company and the Company is not responsible for having assisted him, since the illegal and culpable behavior of the employee is due to completely personal reasons of the perpetrator, unrelated to the service assigned to him and that the Occupational Physician as towards the processing of the data shows such great autonomy that it makes him the controller, determining the purpose and the way of processing the data and is an ad hoc controller with regard to the medical data he keeps on file and with regard to the medical data he processes in the context of his duties. In the complaint of the Employees' Association, it is stated that serious responsibilities of the Company arise, however, the Company claims that it did not violate the provisions of Law 4624/2019 because a. the hiring of the Doctor as the processor was done with the approval of the PNSA, b. the confidentiality agreement provided for the above for the correct processing of data and information by the doctor, c. the physician's obligation to observe and implement the legislation on personal data is also provided for in article 18 par. 3 of Law 3850/2010 ("The occupational physician has an obligation to observe medical and business confidentiality"), d. by law only the doctor can have access to the personal data of the employees in the capacity of the processor, e. by law the Company does not have access to the personal data, f. access to AMKA 5 obtained from other files, acting in excess of the agreed terms in the contractual relationship with the Company. The complained doctor with no. C/EIS/5383/23-08-2021 document provided written explanations to the Authority, in which it denies what the Employees' Association complains about and furthermore maintains that the non-reporting of specific incidents of employees, as well as the complete lack of substantial justification for those reported by the Association, demonstrate the complete vagueness of the report/complaint, since at no point in the report are any facts presented by employees, which took place and from which it can be concluded that the doctor made illegal use of the employees' personal data, but neither issuing false certificates of medical visits. The doctor claims that he never unlawfully processed the personal data of the employees and any form of processing he carried out, limitedly included the collection, storage and general management of the personal data of the employees that the Hospital itself had provided him, in order to fulfill the purpose of his contract with the company, as well as that any processing of personal data was carried out in accordance with the express instructions and orders of the Hospital and in a completely legal and compatible manner with the purpose of their initial collection, in accordance with the principle of purpose limitation (art. 5 par. 1 f. b GDPR), in order to carry out a specialized medical diagnosis and to assess the employees' ability to work, by virtue of the above contract (article 22 of Law 4624/2019), while he proceeded, in some cases, in the processing of personal data of the employees of the Hospital in order to cross-check and complete their personal data through the Individual Health File (AHY) kept for its employees in the

information system of the EOPYY, in order to be able to to issue the appropriate employee attendance certificates, which they themselves had requested. He also mentions that the details of the employees had been made available to the Doctor from the Hospital for use in cross-referencing the EOPYY employee record and he did not obtain them illegally and without the consent of the 6 employees and while he had access to their personal information, therefore also in the "locked" file kept in the EOPYY record (where the patient's consent is explicitly requested by the system), he never used this file, nor prescribed drugs or paraclinical tests, nor disseminated or transferred data to third parties, which proves the lack of malice, the legality of his intentions and actions, while employee health records are kept in a locked cabinet within the Hospital, as stipulated by law. Finally, among the remaining duties of the Doctor at the Hospital was to be responsible for monitoring the workers and issuing certificates of fitness for work, where due to the conditions and the measures that have been implemented and are being followed to prevent and protect against the COVID-19 virus , the examination of the majority of employees was carried out remotely and the processing of the data was carried out during the evening hours and not during his working hours at the Hospital for the most part, in collaboration with the data provided to him by the Hospital's ENL, with which he had close cooperation for the implementation of the health protocols and instructions of the NHS, while the personal information of the employees was used only to access the Individual Health File for the purpose of issuing certificates, pointing out that every Doctor is bound by the Code of Medical Ethics to ensure medical confidentiality and to protect the details of his patients and to avoid creating doubts about his personal ethics and the prestige of his medical profession, the EOPYY has already initiated the control of visit registrations, as well as for the return of the amount charged per visit . Subsequently, the Authority called under no. prot. G/EX/875/07-04-2022, G/EX/876/07-04-2022, G/EX/874/07-04-2022 and G/EX/873/07-04-2022 documents the complainant Association of Employees of the Athens Psychiatric Hospital and the complainants i. Athens Psychiatric Hospital, ii. company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & SIA OE., and iii. doctor A, respectively, as they are legally represented, to appear at the meeting of the Department of the Authority on 13-04-2022, in order to discuss the complaint in question. At this meeting 7, the postponement requests submitted by the complaining Association and the complaining doctor were discussed, which were accepted by the Department of the Authority. Subsequently, the Authority called again with the under no. C/EX/1051/04-05-2022, C/EX/1052/04-05-2022, C/EX/1053/04-05-2022 and C/EX/1054/04-05-2022 documents as above involved parties respectively, as legally represented, to appear at the meeting of the Department of the Authority on 11-05-2022 in order to discuss the complaint in question. The said meeting was attended by the President B and the General

Secretary C of the complainant PSNA Workers' Association after the attorney of Anestis Prousanidis (...), the legal advisor of PSNA Dimitrios Polemis and the Director of the Administrative and Financial Service of PSNA D, the legal representatives of the company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. E and F and the legal advisor of the company Polychronis Karsambas, and the attorney of the accused doctor A, Efstathios Mardakioupis (...). During this meeting, those present developed their opinions and subsequently submitted to the Authority the complainant under no. prot. G/EIS/7485/27-05-
2022 memorandum, the complained Hospital under no. original G/EIS/7577/31-05-
2022 memorandum and the complained Doctor under no. prot. G/EIS/7589/31-05-
2022. It is noted that the complained company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. did not submit a memorandum after the case was discussed. In the memorandum submitted by the complainant, the Association states that during the discussion of the case, the complainants denied that they are responsible for the illegal processing of the personal data of hundreds of employees and confirms the validity of its complaints, pointing out that the employees of PSNA and members of their trade union organization constitute data subjects, the n.p.d.d. PSNA is the recipient of the employees' data and must define the YPD, the n.p.i.d. PROE.EX.O.E. is executing the processing of the data of the employees of the PSNA, in accordance with the contracts drawn up between the hospital and the sponsoring Company, and doctor A, appointed by the Company1 as a subcontractor by order and by authorization 1 According to par. 1.4. of the Annex for the protection of Personal Data with no. 47.20/28.12.2020 of contract 8 of the contractor Company assumed the duties of performing the data processing of the employees of PSNA. With reference to the PSNA, the complainant Association states that the document submitted to the Authority does not answer the complaints, namely that it handed over a large amount of data, some sensitive, to a third private company without the consent of the subjects, through which process was the handing over of the data to the Company, which was recorded which data and of which subjects it was transferred, how the DPO of PSNA checked and ensured that the processing is done in a lawful manner and even when the problem with the data breach was identified why PSNA did not, as it should have, informed the subjects to know what happened and to take measures to protect them. Regarding the Company, the complainant Association states that it is trying to disclaim its responsibilities by claiming (the Company) that the Occupational Doctor was operating completely freely and there is no additional relationship between the Company and the Occupational Doctor and all responsibility lies solely with him, while the Company is certified for the

provision of an Occupational Doctor and for the provision of advice on health and safety issues and received the total amount of the budgeted expenditure from PSNA. Therefore, the legal relationship is between PSNA and the Company on the basis of which the Company is allowed to appoint a subcontractor and perform on its behalf obligations that fall on it. The relationship between the Company and the subcontracted Occupational Physician is a relationship of attachment and entails legal consequences, and the scientific freedom and freedom of conscience of the Doctor does not imply the cancellation of the attachment relationship. Medical confidentiality should not be confused with the personal data that the Company had knowledge of and it is inappropriate that the Company did not gain access to AMKA. In conclusion, the Company bears heavy responsibilities for the violation of the employees' data, itself as the processor, as it did not comply with its obligations according to the law, but also as an additional company that bears the responsibilities that fall on the subcontractor Occupational Doctor which itself defined. As for the subcontracted doctor, as alleged by the Association, the complainant Association stated that the Doctor was the only one who had a financial benefit through the appearance of hundreds of non-existent medical visits on his person 9 by PSNA employees, illegally using their AMKA, the illegality the extension to the criminal branch is also obvious. As the processor, he, at the behest and authorization of the Company, violated the law and the obligations set by the Company. Finally, the Association submits four hundred and thirty-three (433) EOPYY benefit certificates of PSNA employees, in which they are said to have made medical visits to the complained Occupational Doctor. Specifically, three hundred and seventy-three (373) certifications concern the year 2019, twenty-three (23) certifications in 2020, ten (10) certifications in 2021, twenty-six (26) certifications in the years 2019 and 2021 and one (1) certification in the years 2019, 2020 and 2021. The complained PSNA with the post-hearing memorandum it submitted states that between the Hospital and the Company the contracts numbered 125.18 and 47.20 were concluded, pursuant to which, the Company assigned to the PSNA "Doctor A as an Occupational Physician in within the framework of the provisions of Law 3850/2010, as these provisions replaced the provisions of the previous Law 1568/1985 "On the Health and Safety of Workers", the application of which had already been extended to the State, the legal entities under Public Law and the Organizations of Local Government, pursuant to the provisions of article 39 of Law 1836/1989". In particular, in contract 47.20 it is provided that "the Occupational Doctor carries out a medical examination of the employees related to their job position, after their recruitment or change of job position, as well as a periodic medical examination at the discretion of the labor inspector following a request from the E.Y.A.E., when this is not defined by law..." and that "For each employee, the company's occupational physician keeps a

relevant medical file". Also, in the Appendix of the Agreement under the title Protection of Personal Data, it is provided that "PROEX O.E. is obliged to process the personal data of P.N.A. only in the context of the execution of this contract for its specific purposes". During the execution of the Agreement, it was established, as reported by the PSNA, that a large number of employees of the Hospital were appearing as doctors in the EOPYY information system, without these having been carried out either in their physical presence, nor with their consent and without yet having 10 visits are charged to the complainant, the exact number of employees for whom it is alleged that the doctor charged them with unfulfilled visits and non-existent prescriptions, a total of 229 Responsible Statements for visits or prescriptions registered in the Health Insurance File of the EOPYY have been filed in the protocol of the PSNA said doctor. Regarding the damage caused to EOPYY, PSNA cannot have a safe order of its magnitude, as it does not have at its disposal the necessary data and documents, which are at the disposal of the EOPYY service. Also, the PSNA reports that the DPO of the PSNA, as soon as it was informed of the data breach in question, completed and sent the Authority's relevant form to the Authority, informed the Ministry of Health and its DPO and the employees of the PSNA about the breach of their data and repeats the further actions he took, as he had set them out in under no. prot. G/EIS/5383/23-08-2021 document. Finally, in order to refute the objection raised by participants in the discussion of the case before the Authority, that, before granting the Occupational Physician the A.M.K.A. of each employee, that their consent had been given, the PSNA maintains that "in the field of providing health services, legal bases (as special) for the processing of patient data, but not only those: a. the provision of medical services according to art. 9 par. 2 item the GDPR is based in particular on legal regulations for the provision of health care services by public bodies and services by private sector bodies and b. the fulfillment of the public interest in the field of public GDPR, and not the consent of the subject (especially the patient). Based on the above, if e.g. the data subject is asked to sign upon receipt of a personal form, his signature means that he is "aware" of the information required by law and not that he consents to the processing of data... The processing of personal data is necessary for the execution of projects of public interest or a project carried out by a public authority or assigned by it to the controller to whom the data is disclosed. This is exactly what happened in the present case of PSNA, where the notification of the A.M.K.A. of the PSNA employees to the Occupational Physician, was an absolutely necessary and imperative action, as this was the only way the medical file of each of them could be legally compiled and, by extension, the implementation of the contract with the contracting company could be made possible". In support of the above, the PSNA states that the 4th Department of the Council of Ministers with no. 517 and 518/2018 of its decisions, points out that

the processing of personal data carried out through AMKA is a legal and legitimate action for the protection of personal data, as it aims to serve clear and legitimate constitutional purposes of public interest, which tend to fulfill the obligation to provide health services directly provided by article 21 par. 3 of the Constitution, while it aims to avoid over-prescription and to easily monitor pharmaceutical costs. The complained Occupational Doctor A in no. first C/EIS/7589/31-05-2022 his memorandum states that he denies the accusation of illegal processing of the data of the working members of the Association during the exercise of his duties, as every processing he carried out, limitedly included the collection, storage and in general management of the personal data of the employees that the Hospital itself had provided to him, in order to fulfill the purpose of his contract with the Company and all data processing was carried out in accordance with the express instructions and orders of the Hospital and in a completely legal and compatible manner the purpose of their initial collection, in accordance with the fundamental principle of purpose limitation (article 5 par. 1 f. b' of the GDPR), in order to carry out a specialized medical diagnosis and assess the employees' ability to work, under of the relevant contract (article 22 of Law 4624/2019), and adds that "specifically, in some cases, personal data of Hospital employees were processed in order to cross-check and complete their personal data through the Individual Health File (APHY) that is maintained for the employees of the Hospital in the EOPYY information system, so that I can then issue the appropriate attendance certificates for the employees, which they themselves had requested. He emphasized that the details of the employees had been made available to me by the Hospital, specifically via electronic mail from the Personnel Department of the P.S.NA, for use in cross-referencing the EOPYY employee record and I did not obtain them. illegally and without the consent of the workers. Besides, while I had access to their personal information, therefore also to the "locked" file kept in the EOPYY record (where the patient's consent is explicitly required by the system), I never used this file, nor prescribed drugs or paraclinic examinations, nor their medical history, nor dissemination or transfer of data to third parties, which proves the lack of malice, as well as the legality of my intentions and actions." Finally, he states that the content of the report is completely vague and no specific incidents are listed that prove the illegality of his actions, while the details of the employees, specifically the structure, surname, first name, patronymic, AMKA, branch and the specialty had been made available to the doctor by the Hospital, specifically through electronic mail from the Personnel Department of the P.N.A. and any processing of personal data of the employees of PSNA was done for the purpose of cross-checking and completing their personal data through the Personal Health File (PIF) kept for the employees of the Hospital. Also, this processing was limited in scope, limited to opening the EOPYY information system, checking the

employee's details and completing the patient's individual file, while the above processing did not cause any harm to the hospital's employees, stating that "in accordance with 4624 / 2019 article 22. By way of derogation from article 9 paragraph 1 of the GDPR the processing of special categories of personal data within the meaning of article 9 paragraph 1 of the GDPR by public and private bodies is permitted, for reasons of preventive medicine, for the assessment of the capacity to employee's work and for medical diagnosis". The Authority, after examining the elements of the file, after hearing the rapporteur and the clarifications from the assistant rapporteur, who was present without the right to vote, after a thorough discussion 13 DECIDED IN ACCORDANCE WITH THE LAW 1. Because, from the provisions of articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) and Article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, this law and other regulations concern the protection of the individual from the processing of personal data. In particular, the Authority undertakes the reported illegal processing of personal data of the employees of the Hospital during the performance of medical procedures on behalf of the complained Occupational Doctor by virtue of the Hospital's contract with the Company and with the complained doctor in the context of ex officio competence, in accordance with the provisions of provisions of articles 57 par. 1 item a and h GDPR and 13 par. 1 item n. Law 4624/2019, as personal data of employees of the Hospital were processed, as the complained doctor himself agrees with the under no. original G/EIS/7589/31-05-
2022 of his memorandum, given that, in addition to and regardless of any legal representation of the members of the complainant Association - employees of PSNA pursuant to article 80 of the GDPR, the complained processing of the transmission of the AMKA of the employees of the Hospital to the complained doctor appointed by the Company and the performance of medical procedures by the doctor, without the consent of the employees of the Hospital, constitutes processing of personal data, subject to the regulatory scope of articles 2 par. 1 of the GDPR and 2 of law 4624/2019. In fact, the aforementioned ex officio competence of the Authority is justified independently of the investigation into the commission of any criminal offenses by the accused. 2. Because Article 5 of the GDPR defines the processing principles that govern the processing of personal data. Specifically, it is defined in paragraph 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity, transparency"), b) are collected for specified, explicit and legitimate purposes and are not 14 further processed in a manner incompatible with these purposes (…), c) are appropriate, relevant and limited to what is necessary for the purposes for which they are

processed ("data minimization") f) are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality")" . 3. Because, according to the provisions of article 5 paragraph 2 of the GDPR, the data controller bears the responsibility and must be able to prove his compliance with the principles of processing established in paragraph 1 of article 5. As the Authority has judged, with the GDPR a new compliance model was adopted, the central point 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 the data to be in accordance with the relevant legislative provisions. In addition, the controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 4. Because the concept of the controller plays a decisive role in the application of the personal data protection rules, the proof of compliance with them (principle of accountability, Article 5 para. 2 GDPR) and the assignment of responsibilities in the event of their violation. According to the provisions of art. 4 pc. 7 of the GDPR as data controller means "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of processing personal data (…)". Furthermore, according to Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Party to determine the controller 15, according to the aforementioned definition, three main elements a) the personal aspect ("the natural or legal person, public authority, agency or other body"), b) the possibility of multiple control ("who, alone or jointly with others") and c) the basic elements to distinguish the controller from other actors ("determine the purposes and manner of personal data processing"). Finally, the processor is defined as "the natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller" (Article 4 para. 8 GDPR). 5. Because, according to the "Guidelines 07/2020 of the European Data Protection Board on the concepts of controller and processor in the GDPR", it is pointed out that: "In principle, any processing of personal data carried out by employees in area of an organization's activities may be considered to be carried out under the control of that organization. In exceptional circumstances, however, an employee may decide to use personal data for the same purposes and, therefore, unlawfully exceed the powers assigned to him (e.g. to establish his own company or for a similar purpose). . Consequently, as a controller the organization has a duty to ensure that appropriate technical and organizational measures are implemented, including training and information of employees, which will ensure compliance with GDPR, no. 24 par. 1»2. Furthermore, it is clarified in CG 07/2020 that "While the terms "personal

data", "data subject", "controller" and "processor" are defined in the regulation, the concept "persons who, under the direct supervision of the controller or processor, are authorized to process the personal data" is not defined. (…) In 2 Sk. 19 CG 07/2020 available at the link: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_en.pdf 16 measure that the employee processes personal data for the same purpose or purposes, different from those of his employer, will be considered responsible for processing and will bear all the legal consequences and responsibilities associated with the processing of personal data (…) Accordingly, a third party refers to anyone who, in this case, is not a data subject, controller, processor or employee. For example, the controller may employ processors and to instruct him to transmit personal data to a third party. The third party will now be considered a controller as an independent entity with respect to the processing it carries out for the same purposes." 3 In relation to the processor, the same Guidelines specify that "The broad concept of "persons authorized to process the data" includes employees and temporarily employed staff. In general, the processor should only make personal data available to employees who actually need it to perform the tasks for which the processor was engaged by the controller." 4 6. Because the controller must implement appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR, in accordance with Article 24 GDPR and only use processors who provide sufficient assurances for the implementation of the prescribed measures, which must process the data based on recorded instructions of the data controller, in accordance with Article 28 para. 1 GDPR. In addition, in accordance with the provisions of article 28 par. 4, the sub-executor, who may be hired by the executor, shall be subject to the same obligations regarding the protection of data provided for in the contract between the controller and the processor. Finally, in case the 3 Sk. 88-89 CG 07/2020. 4 Sk. 123 CG 07/2020. 17 processor determines the purposes and means of the processing in violation of the GDPR, the processor is considered responsible for the specific processing in accordance with article 28 paragraph 10 GDPR. 7. Because, in article 2 of Law 3850/2010 "Sanction of the Code of Laws for the health and safety of workers" (Government Gazette A 84) (hereinafter "Code of Laws") it is defined that: "1. The provisions of the code apply, unless otherwise specified, to all businesses, holdings and operations in the private and public sector. (...) 8. in companies that employ 50 or more workers, the employer has the obligation to use the services of a safety technician and an occupational doctor, in accordance with chapter B' of this document. Next, in article 20 the obligations of the safety technician and the occupational doctor are determined and in articles 31 and 42 the obligations of employers regarding the health and safety of

employees. 8. In no. 18 of the Code of Laws describes the responsibilities of the Occupational Physician for the supervision of the health of employees, as follows? "1. The occupational doctor carries out a medical examination of the workers in relation to their job, after their recruitment or change of job, as well as a periodic medical examination at the discretion of the labor inspector at the request of the workers' health and safety committee, when this is not defined by law. He takes care of carrying out medical examinations and measurements of factors of the working environment in application of the regulations that apply at any time. He assesses the suitability of employees for the specific work, evaluates and registers the results of the examinations, issues a certificate of the above assessments and communicates it to the employer.[…] 2. The occupational physician supervises the implementation of measures to protect the health of employees and prevent accidents.[…] 3. The occupational doctor has an obligation to observe medical and operational confidentiality. 4. The occupational doctor announces through the company to the labor inspection diseases of the employees due to work. 5. The doctor must be informed by the employer and the employees about any factor in the workplace that has an impact on health. 6. The supervision of the workers' health cannot entail a financial burden for them and must be done during their working hours. 8. The occupational doctor, in the context of his obligations and the obligations of the employer, in accordance with the written special provisions, if the company does not have the appropriate infrastructure, has an obligation to refer the employees for specific additional medical examinations.[…] Then the an occupational physician receives knowledge and evaluates the results of the above tests.[…] 9. For each employee, the occupational physician of the company keeps a relevant medical file. In addition, an individual occupational risk book is established and included in the medical file, where the results of the medical and laboratory tests are recorded, every time an employee undergoes the corresponding tests.[…] 10. It is prohibited to write and edit the individual occupational risk book of the employee, elements or data other than the results of the medical and laboratory tests to which he is submitted each time, in accordance with the provision of paragraph 9. Additional medical data may be collected, with the care of the employee himself in order to be the subject of processing, only if this is absolutely necessary: a) to assess his suitability for a specific position or job, b) to fulfill the employer's obligations for the health and safety of employees and c) to establish the employee's rights and provide corresponding social benefits. 11. Those who record or collect or process information or data in violation of paragraph 10 are punished with the administrative and criminal sanctions provided for in the provisions of articles 21 and 22 of Law 2472/1997 "Protection of the individual from the processing of personal data" (Official Gazette 50/A') respectively. Article 23 of Law 2472/1997 applies in the event of property

or moral damage." Therefore, taking into account the above-mentioned provisions of this law, it follows that the Hospital, as n.p.d.d. had the obligation to appoint an Occupational Physician and the complained Occupational Physician has the statutory 19 responsibilities for supervising the health of the Hospital's employees. 9. Because article 1 of Law 3418/2005 regarding the Code of Medical Ethics stipulates, among other things, that: "1. A medical procedure is one whose purpose is the prevention, diagnosis, treatment and restoration of human health by any scientific method.[…] 3. The concept of a medical procedure also includes the prescription, the order to carry out all kinds of paraclinical examinations, the issuance of medical certificates and certificates and the general advisory support of the patient. (…)". Furthermore, according to article 14 par. 1 of Law 2348/2005, the employee's medical file kept by the Occupational Physician can be kept either manually or electronically. 10. Because, with regard to the complained processing of the entry of the employees' data in their electronic files in the EOPYY, the complainant Association provided copies of four hundred and thirty-three (433) EOPYY benefit certificates from the year 2019 to 2021, printed from the electronic address " www.eopyy.gov.gr" from the electronic file of the employees of PSNA, in which it is recorded that each of the insured/employees, with their name and AMKA registered, on a specific date had visited the complained-about Doctor with the specialty "...", at a cost of ten (10) euros per visit, without the knowledge of each employee. According to what he mentioned in the under no. prot. C/EIS/7589/31-05-2022 his memorandum the complained doctor, he himself had access to the personal information of the employees and to the "locked" folder in the EOPYY tab, which he could open, check the data of the employee and to complete the individual file of the patient. The Authority finds, in this case, that since the visits in question have been registered in the name of the specific doctor using the latter's codes, it is reasonable to conclude that the complained doctor had gained access to the electronic medical file of the EOPYY of each employee and had also registered the in the matter of visits and had processed the personal data 20 of a nature concerning the health of the employees of the PSNA, without it appearing that the consent of the subjects had been obtained, especially since the subjects themselves expressly denied before the Authority through the complaining Association that made registered visits. The claim of the complained doctor that the system explicitly requires the consent of the patient for any medical procedure and therefore proves that the employees of the Hospital consented to the performance of medical procedures, is rejected as unfounded and the performance does not in itself constitute proof that the required consent had been obtained, as the doctor himself selects the field in the EOPYY electronic file, where the subject is asked to give his consent5. Therefore, the Authority finds that the complained doctor processed personal data of a special category of employees, whose details appear in the certificates

provided, without a legal reason, i.e. in violation of the principle of legality according to article 5 par. 1 of the GDPR. 11. Because, regarding the distribution of roles between the parties involved, namely the Hospital, the contracting Company and the Occupational Physician, it appears that the Hospital is the controller of the personal data of its employees. Furthermore, the complained Company, which by virtue of under no. 125.18 and 47.20 of Contracts with the purpose of providing an Occupational Doctor for the Hospital, became the processing operator, according to article 4 par. 8 GDPR, as it undertook, by order of PSNA, to determine individual elements of the processing method. Finally, the Occupational Physician (contracting party) undertook, on the one hand, as the processor to execute individual conditions of the contract from 01-06-2019 with the contractor Company, and on the other hand, as the processor (Occupational Physician) based on the provisions of Law 3850/2010 to processes the special category personal data of the organization's employees. However, regarding the processing of employee data in 5 See relevant decision of the Authority 138/2013, in particular s. 7. 21 which was carried out on the basis of what was said in paragraphs 5 and 6, from the data of the file it appears that the Occupational Doctor acted in excess of the limits of the contract from 07-12-2019 with the Company and became the controller himself (no. 28 par. 10 GDPR). 12. Because, as far as the accused Hospital is concerned, taking into account all the elements of the case file, the hearing process and the submitted memoranda, it appears that the Hospital forwarded details of the employees to the Occupational Doctor and specifically, as the accused doctor mentioned, the structure , the last name, first name, patronymic, AMKA, branch and specialty of each employee. On this fact, the Hospital claimed that the notification of the AMKA was an absolutely necessary action, as this was the only way the medical file of each employee could be legally compiled. It is noted that the AMKA, in accordance with the Authority's jurisprudence6, does not by itself reveal the slightest sensitive personal data of each interested subject, but only in cases where the last 4 digits of the AMKA are registered together with other data, which reveal a specific health status of the patient, constitute a special category of personal health-related data. Therefore, the Hospital transmitted to the Occupational Physician simple personal data of its employees in accordance with the legal obligation to protect its employees in its workplace, in accordance with the provisions of no. 6 par. 2 items 3 GDPR and the individual provisions of Law 3850/2010, without, however, showing that the Hospital informed its employees that the complained-about doctor became the recipient of the data in violation of the provisions of Article 13 par. 1 item. e' of the GDPR. 13. Furthermore, from all the elements of the file, it appears that the Hospital, as a data controller, did not implement policies and procedures for the processing of employee data in accordance with 6 See Decision 56/2010 of the Authority 22

article 24 par. 1 GDPR. In particular, in the 28-12-2020 Contract 47.20 that has been concluded between the Hospital and the contractor Company, the "Annex: Protection of Personal Data" has been incorporated, in which the obligations of the parties are recorded in general, no specific technical and organizational measures are foreseen, such as the specifications of the electronic application, which the Occupational Physician uses when processing the patient's medical file, or whether and how it is permitted to extract data from the terminals that may be used by the contracting company or the Occupational Physician. Instead, the Hospital issued letter no. first ... certificate of good cooperation in response to a relevant application of the contractor company, in which it confirms that "regarding the execution of the signed Contract ... concerning the services of the Occupational Physician, in accordance with the technical specifications, as defined in Law 3850/2010 and for the time period from 13-05-2019 to 12-05-2020, the conditions were well respected", without resulting in any substantial evaluation and assessment of the work provided in accordance with the law of the complained Doctor, even though it is proven that there were registered visits in the electronic employee file of the Hospital by the complained Occupational Physician. This fact proves the lack of measures by the Hospital as the controller to carry out periodic checks for the protection of the special category of data of the employees, in accordance with the provisions of the provision 32 par. 1 item. d' GDPR. It is pointed out that the assignment by the Hospital to the company and, by extension, to the Occupational Physician of specific processing operations, does not constitute a reason for exemption from the obligations that he bears in his capacity as the data controller for the observance of the appropriate technical and organizational measures according to application of articles 24 and 32 GDPR to ensure the principle of article 5 par. 1 item. f), on the contrary, it increases its responsibility for the control of the processor, pursuant to article 28 par. 1 of the GDPR. Also, although the Hospital owed according to article 13 par. 1 item. e' of the GDPR to inform the employees of the Hospital, as subjects, about the processing to which the 23 personal data concerning them are submitted by the Hospital in general and especially by the Occupational Physician, from the entire file there is no relevant information employees. Finally, with regard to the claim of the complaining Association for the non-appointment of a Data Protection Officer by the Hospital, from the files and registers kept by the Authority, it appears that the PSHNA has complied with the obligation to appoint a Data Protection Officer, in accordance with the provisions of article 37 GDPR and 6 of Law 4624/2019. 14. Because, finally, PSNA as data controller submitted to the Authority under no. prot. C/EIS/1201/18-02-2021 (as well as the under no. prot. C/EIS/3136/12-05-2021 supplementary data) notification of a personal data breach incident and with the subject incident of the "use of data

outside the context of a contract" for the breach of confidentiality, complying with the requirement of article 33 GDPR. 15. In view of the above, the Authority finds that the Hospital has not provided the employees with the required information on the processing of personal data, in violation of Article 13 par. 1 item. e of the GDPR, and has not implemented the appropriate technical and organizational measures to ensure that the processing of employee data is carried out in accordance with the GDPR, in violation of Articles 24 para. 1 and 32 para. 1 item. d of the GDPR and there is reason to exercise the right according to article 58 par. 2 item. i' corrective power of imposing a fine. 16. Because, secondly, with regard to the complained company, taking into account all the elements of the case file, the hearing procedure and the submitted memoranda, it appears that the contractor, as the processor, company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & SIA OE, has contracted, as mentioned above, with the Hospital for the appointment of the Occupational Physician and bears the obligations provided for in article 28 of the GDPR regarding both the responsibility it undertakes to the person in charge of the recorded orders that he has received from him in the context of the above contract, as well as with the assignment of the same responsibilities and obligations in processing, i.e. the Hospital application for 24 whoever hires to carry out specific processing activities, i.e. the Occupational Physician, pursuant to 28 para. 4 GDPR on behalf of the data controller. In the 12-07-2019 contract, it does not appear that the processing company had incorporated provisions regarding the processing of the subjects' personal data, whose data would be processed by the Occupational Physician, nor did it take specific technical and organizational measures, to ensure that the processing of the data by the performing Occupational Physician would be carried out in accordance with the GDPR. Therefore, the Authority finds that the company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. has violated article 28 par. 4 of the GDPR and there is a reason to exercise the right according to article 58 par. 2 item. i' corrective power of imposing an administrative fine. 17. Because, thirdly, with regard to the complained doctor, taking into account what is contained in the immediately preceding considerations of this present and in particular paragraph 10, all the elements of the case file, the hearing procedure and the submitted memoranda, it appears that they have been registered in the electronic file of EOPYY visits by employees of the Hospital in the name of the complained Occupational Physician with his specialty, during the three years of his cooperation with thecontracting company and the Hospital, i.e. from the year 2019 until the year 2021, for visits to him by employees of the Hospital, without their knowledge

and accordingly no information was submitted to the Authority by the complainant

Occupational Physician capable of refuting his individual claims

Association. The Occupational Doctor as a sub-processor on behalf of

of PSNA and within the framework of the Hospital's contract with

complained company appears to have acted in excess of

responsibilities assigned to him by the controller and

he himself became a data controller in accordance with the provisions of the article

28 par. 10 GDPR. The registration of employee visits to

their electronic file constitutes health data processing, i.e

special category data, for the processing of which the

25

consent of the subjects, as provided for in article 9 par. 2 item. a

of the GDPR, which in the complaint in question does not appear to have been received from

the subjects7. Therefore, the Authority finds that the complained doctor

processed employee health data, in the electronic file

whose visits to the doctor in question were registered without their knowledge,

in violation of the principle of legality, as provided for in article 5 par.

1 pc. a' of the GDPR, acting in accordance with article 28 par. 10 as

data controller in excess of his powers based on

assignment contract and there is reason to exercise the right under article 58 par. 2

item i' corrective power of imposing an administrative fine.

18. Furthermore, the Authority took into account the criteria for measuring the fines which

defined in article 83 par. 2 of the GDPR, the Guidelines "for

implementation and determination of administrative fines for its purposes

Regulation 2016/679»8 of the Working Group of article 29 and

Guidelines 04/2022 of the European Protection Council

Data9, as well as the actual data of the case under consideration

and especially:

i.

ii.

The fact that the complained Hospital has not received the

appropriate technical and organizational measures to ensure the

application of the GDPR by the appointed Occupational Physician, although

it is a n.p.d.d., which processes a large number

personal data of its employees (no. 83 par.

2 pcs. d').

The fact that the complained company has not received the appropriate

technical and organizational measures to ensure its implementation

GDPR by the Occupational Physician (no. 83 par. 2 item d')

7 See Decision of the Authority no. 138/2013, s. 7

8 WP 253 from 03.10.2017 available at the link https://www.dpa.gr/sites/default/files/2019-

12/wp253_en.pdf

9 Guidelines 04/2022 on the calculation of administrative fines under the GDPR from 12.05.2022 under

public consultation, available at https://edpb.europa.eu/system/files/2022-

05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

iii.

iv.

The fact that the violation committed by the Occupational Physician

affected a large number of data subjects (no. 83 par. 2 item

a') and concerned health data, i.e. of a special category (no. 83

par. 2 item g').

The fact that the Occupational Physician due to his profession has

increased responsibility towards society as a functionary and

must, among other things, avoid any act or omission, h

which may damage his honor and dignity and to

shake the public's faith in the medical profession, as well as that

earned a financial benefit (no. 83 par. 2 letter k').

Based on the above, the Authority unanimously decides that they should be imposed on

defendants, in the capacity of the first and the third of these

controllers, and the company as the processor, the

administrative sanctions referred to in the ordinance, which are considered proportionate

with the gravity of the violations.

FOR THOSE REASONS

THE BEGINNING

A. Finds that the complained Psychiatric Hospital of Athens, as

data controller violated articles 13 par. 1 item e' and 24 par. 1 GDPR

and imposes on the Hospital according to article 58 par. 2 item. i GDPR the administrative

a fine of eight thousand (8,000.00) euros.

B. Finds that the complained company PRO.EX. O.E. - G. Psathas - K. Chrysou &

SIA O.E., as the operator of the processing, violated Article 28 para. 4 GDPR and

imposes on the company PRO.EX. O.E. - G. PSATHAS - K. CHRYSOU & CO. OE. per article

58 par. 2 item i GDPR, the administrative fine of six thousand

(6,000.00) euros.

C. Finds that the accused doctor A, acting in violation of

of his responsibilities, as a data controller, violated article 5 par. 1 item

a' GDPR and imposes on doctor A according to article 58 par. 2 item. i GDPR, the administrative

a fine of ten thousand (10,000.00) euros.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou

28