Athens, 20-07-2020 AP: C/EX/5078/20-07-2020 GREEK REPUBLIC PERSONAL DATA PROTECTION AUTHORITY Tel. Address: KIFISIAS 1-3 115 23 ATHENS TEL.: FAX: 210-6475600 210-6475628 DATE 20/2020 The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting at its headquarters on Tuesday 03.03.2020 at 09:00, postponed from 25.02.2020, in order to examine the case referred to in the history of the present. The President of the Authority, Konstantinos Menudakos and the regular members of the Authority Spyridon Vlachopoulos, Charalambos Anthopoulos, Konstantinos Lambrinoudakis and Eleni Martsoukou were present. Grigorios Tsolias, alternate member of the Authority, also attended the meeting, by order of the President, as rapporteur. Present, without the right to vote, were Chariklia Latsiu, legal auditor - lawyer, as assistant rapporteur and Georgia Palaiologou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With the complaint from ... (and with no. prot. APDPX C/EIS/4278/18.06.2019) A complains of a violation of the legislation on personal data, as upon entering the portal of 401 General Military Hospital of Athens (hereinafter "401 2 GSNA") she was asked to show the identity of a family member e.a. military, her police ID card was withheld until she left the Hospital premises and, finally, her police identity card details were recorded without her consent in a daily card. The Authority, during the examination of the above complaint, with the under no. prot. APDPH G/EX/4278-1/01.07.2019, G/EX/4178-2/17.07.2019 and G/EX/2478-3/27.09.2019 documents, delimiting its competence, underlined that it has the authority to charged with the processing of personal data, i.e. the details of the police identification, which - according to the complaint - are registered by the Hospital in a daily report, as part of the filing system, and invited the 401 GSNA to provide specific explanations. In response to the above documents of the Authority, the 401 GSNA with the under nos. prot. ..., ... and ... documents (under no. prot. APDPCH G/EIS/4880/11.07.2019, G/EIS/6099/09.09.2019, G/EIS/7034/16.10.2019, respectively), clarified , among other things, that upon entering the Hospital, based on military legislation, the following information is entered in a daily card: 1) name, 2) identification number, 3) office or place of visit, 4) purpose of visit and 5) time of entry – exit, which are kept for a decade. In addition, according to the claims of 401 GSNA, the above information constitutes simple personal data and does not fall into any special category, given that the status of the visit is not noted, i.e. if it is a patient and the related health problem, and only what is recorded, what is expressly required and is absolutely necessary according to the provisions contained in relevant regulations - orders for the security of military installations. Furthermore, the 401 GSNA citing Article 10 of Law 4624/2019 argues that: "(...) we believe that you do not have jurisdiction over issues related to national security. In addition, you are informed that the 401 GSNA is an

Organizational Formation of the GES, subject to an Administrative Management relationship and as a consequence of this it is obliged to comply with the provisions contained in the military regulations. As a result, it is established that the Military Regulation (…) and the related classified orders (…) which determine how the control for entry and exit to military installations is carried out, constitute the legal basis for the processing of personal data". Finally, regarding compliance with the obligation to appoint a Data Protection Officer (hereinafter DPO), 401 GNSA notes: "as it appears from the (…) relevant, a Data Protection Officer 3 office was established at the General Staff of National Defense and is responsible for protection issues of personal data both in the General Staffs and in the Units - Services under them, therefore also in the 401 GSNA". Subsequently, the Authority with sub. No. prot. G/EX/4278-6/07.11.2019 (in continuation of document G/EX/4278-4/01.11.2019) and G/EX/4278-7/07.11.2019 (in continuation of G/EX/ 4278-5/01.11.2019 document) documents invited 401 GSNA, as legally represented, and A, respectively, to be presented at a meeting of the Plenary of the Authority on Friday 15.11.2019 at 11:00 in order to discuss the aforementioned complaint A. At the meeting of the Authority on 15.11.2019, 401 GSNA was present, through B, ..., while A with the applications from ... and ... (under no. prot. C/EIS/7710/08.11.2019 and C/ IIS/7750/11.11.2019, respectively, documents) submitted a postponement request. Following this, the Authority set a new date for discussing the case on 03.12.2019 at 10:30, which it announced to the representatives of 401 GSNA who were present during this meeting on 15.11.2019, while A was informed with the no. . prot. APDPH C/EX/4278-8/15.11.2019 document. At the meeting of the Authority on 03.12.2019, the 401 GSNA was present, through Major General Konstantinos Karliautis, Commander, C, Director of ... Office and B, ... and the complainant A. This meeting was also attended by D..., Data Protection Officer of the General Staff National Defense. At the end of the meeting, those present requested and received a deadline for the submission of a memorandum document, on the one hand 401 GSNA until 08.01.2020 and on the other hand A (who asked to receive a copy of the 401 GSNA memorandum before submitting hers) until 15.01.2020. 401 GSNA submitted a timely memorandum to the Authority under no. prot. ... (and with no. prot. APDPH C/EIS/92/08.01.2020) his document, whereas, on the contrary, A did not request within the set deadline to receive a copy of the relevant memorandum of the 401 GSNA, nor submitted within the deadline a relevant memorandum. 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 and left after the discussion of the case and before the conference and decision-making, following a thorough discussion , CONSIDERED IN ACCORDANCE WITH THE LAW 1. Because, from the provisions of articles 51 and 55 of General Data

Protection Regulation 4 2016/679 (hereinafter "GDPR") and article 9 of Law 4624/2019 (Government Gazette A' 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. In order, however, for the Authority to receive A's complaint against 401 GSNA, pursuant to articles 57 par. 1 item. f GDPR and 13 para. 1 item g´ Law 4624/2019, and to exercise respectively the powers granted to it by the provisions of Articles 58 of the GDPR and 15 of Law 4624/2019, the claim of 401 GSNA must first be examined, which, citing Article 10 par. 5 of Law 4624/2019, argues that the Authority does not have the authority to examine the above complaint because it refers to issues related to the national security of the country. 2. According to Recital 16 of the GDPR, this Regulation does not apply to matters of protection of fundamental rights and freedoms or to the free movement of personal data related to activities outside the scope of EU law, such as activities related to national security. And in the provisions of article 2, concerning its essential scope, it is provided that the GDPR does not apply "in the context of an activity which does not fall within the scope of Union law" (par. 2 item a') and "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including the protection and prevention against risks that threaten public security" (par. 2 item d'). Furthermore, Article 23 of the GDPR provides for the possibility of establishing through a legislative measure restrictions on the rights, obligations and rights of Articles 12 – 22 and Articles 34 and 5, when these restrictions respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society to ensure, inter alia, the security of the state (item a), public safety (item c) and the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection against threats to public security and their prevention (item d´). Finally, in article 45 par. 2 GDPR regarding transfers of personal data to a third country or international organization it is defined that when assessing the adequacy of the level of protection, the Commission takes into account, in particular, the followingelements: "the rule of law, respect for human rights and the 5 fundamental freedoms, relevant legislation, both general and sectoral, inter alia regarding public safety, defence, national security and criminal law and access of public authorities to personal data, as well as the application of this legislation (…)" (item a'). From the above provisions, it follows that the concept of national security is found in article 45 of the GDPR, which concerns transfers based on an adequacy decision (and in requests s. 16 - scope and 104 - transfers), while mainly reference is made to the concept of public security (articles 2, 23 and 45 and request. s. 19, 50, 73, 104) and security of the state (article 23). Law 4624/2019, defining

the competence of the Authority, provides in article 10 paragraph 5: "The Authority is not competent to control acts of processing of personal data carried out by the judicial and prosecutorial authorities in the context of the judicial function and the judicial duties, as well as acts of processing classified personal data carried out for the activities related to national security". According to the explanatory statement of the law, Article 10 defines the competence of the Authority in compliance with Article 55 GDPR. Article 55 GDPR provides for a limitation, only with regard to processing operations carried out by courts within the framework of their jurisdiction (paragraph 3), i.e. with regard to the first case provided for in paragraph 5 of article 10. It is also worth noting that, according to the same explanatory report, with paragraph 4 of article 10, the Authority exercises the corresponding supervisory powers provided for by special provisions of international and EU law and concerning the processing of personal data1. As such are understood, according to the explanatory statement, among others, the provisions regulating the Schengen Information System, the Europol Information System, the Eurodac Information System and the Convention on the use of IT in the customs sector. From the systematic interpretation of the provisions of paragraphs 4 and 5 of Law 4624/2019, it follows that the legislator does not generally exclude national security issues from the competence of the Authority, as where international and interstate conventions expressly provide for competence of the Authority, the latter retains the relevant authority. 3. Following this, taking into account the aforementioned recital 16 1 Article 10 paragraph 4 states: "In cases where international or transnational agreements or European Union law or national legislation provide for independent control or supervision, the Authority exercises the respective responsibilities and powers". 6 of GDPR 2016/679, the Authority considers that a relative limitation of the exercise of its powers through the implementing law for reasons of national security does not, in principle, contradict the GDPR. Furthermore, from the wording of the aforementioned provision of paragraph 5 of article 10 of Law 4624/2019, it follows that the Authority does not have the authority to control the processing operations carried out for activities related to national security if the following two conditions are met cumulatively: a) it is for classified personal data processing operations, and more correctly, information registered in filing systems that have been competently classified and which constitute personal data and b) these are personal data processing operations carried out for activities related to national security. From the documents in the file, the hearing and the hearing memorandum of the 401 GSNA, it did not appear that the daily report, as part of the filing system as well as the personal data recorded in the above daily report and which are collected from the subjects upon entry in 401 GSNA, (i.e. name, ID number, office or place of visit, purpose of visit and entry-exit time), have been duly classified as classified documents and information in accordance with the

National Security Regulation (NSR)/ 2018/GEETHA/E'KL/E3 ratified by the Decision of the Minister of National Defense f.120/01/510313/S.94/01-01-18/GEETHA/E'KL/E3 (Government Gazette B'683/27 -02-2018). Therefore, the Authority considers that in this case it was not proven that the first condition for the application of article 10 par. 5 of Law 4624/2019 is met and therefore it is competent to exercise its powers, the relevant allegation-objection of 401 GSNA being rejected as unfounded . However, even if the first condition were met, it would have to be proven, further, that the second condition for the application of article 10 par. 5 of Law 4624/2019 is also met, namely that the said processing of classified information attributed to a natural person (data of a personal nature) is carried out for activities related to national security. "National security" is a vague legal concept, which must, based on the facts of each case, be interpreted, determined and 7 documented ad hoc2 by the data controller. Therefore, the vague and general invocation of the assistance of national security is not sufficient to exclude the Authority from exercising its powers, but documentation is required in this particular case that the processing is carried out for an activity concerning the national security of Greece, unless it is obvious the assistance of this concept (e.g. purely military installations with war material, not accessible to the public). The Authority, in fact, with the Opinion under no. 01/20203 decided with reference to the provision of article 10 par. 5 of law 4624/2019 that: "Due to the generality of the provision, in which the operations of processing classified personal data carried out for the activities concerning national security, difficulties arise in the characterization of these acts. In view of this, it is appropriate to add the following provision to par. 5: "The authorities that process classified personal data in the context of national security activities, inform and cooperate with the Authority for compliance with the legislation on personal data protection and in particular the receipt and the observance of the necessary general safety measures". According to article 1 of Law 2292/1995 "Organization and Operation of the Ministry of National Defence, command and control of the armed forces and other provisions" (Government Gazette A' 35/15-02-1995), which defines the mission of the Armed Forces , "National Defense includes all the functions and activities developed by the State, with the aim of protecting territorial integrity, national independence and sovereignty and the security of citizens against any external attack or threat, as well as supporting the national interests". Besides, in the documents sent to the Authority by the 401 GSNA during the pre-trial of this case, reference is made to the military legislation, which contains the principles and the organization of military security, which include the establishment of a specific procedure for entering military installations, as a security measure of the of military units (APDPH no. prot. 7034/16-10-2019). In addition, 401 GSNA supported with the hearing memorandum 2 For the concept of national security, see regarding Gr. Tsolia, Special Criminal

Laws, Privacy of Electronic Communications, vol. II, p. 13 ff., 2nd ed. (June 2013), Sakkoulas publications, with the references there to the relevant bibliography and the reservations regarding the possibility of an abusive appeal and invoking national security as a reason for lifting the confidentiality of communications, a reason for limiting the right to information according to art. 5A par. 1 S. and reason for suspension of constitutional provisions no. 48S. 3 Available on the Authority's website. 8 of (APDPH no. prot. 92/08-01-2020) that: "[…] the freedom that belongs to the bodies responsible for the national security of the country, to proceed with the establishment of specific security measures without the mediation or control by above Authorities is lawful, in accordance and harmonized with the new provision of Law 4624/2019, which came to guarantee this very independence and the initiative of action in terms of managing security issues and in this case also the entry into military installations...para. 5 of article 10 of law 4624/2019 (…) From the language of the above provision in conjunction with the case under consideration (that is, the recording of personal data upon entry into a military installation) it follows that the determination of the level of security measures and consequently, the withholding of the identity and the recording of the details of allvisitors of 401/GSNA cannot be subject to the control of the Authority. It should be noted that the provision in question is consistent and follows the spirit of EU Regulation 2016/679 which in paragraph 1b of article 23 gives the national legislator a wide margin of action regarding the limitation of the rights of the data subject as a necessary and proportionate measure for ensuring the national defense of the country. From the above it follows that the 401 GSNA did not invoke facts, nor did it present relevant evidence from which it can be seen that the recording in the daily report of the personal data of the subjects entering its hospital facilities for the provision of health services constitutes, in accordance with Article 10 par. 5 of Law 4624/2019 "activity concerning national security", and he argued that the measures taken concern the military security of the facilities citing the relevant legislation which, however, does not mention national security. In particular, in Ministerial Decision no. Y4a/137327 of the Ministers of National Defense and Health-Social Solidarity (Government Gazette B´ 1757/09.11.2010) regarding the "Framework of cooperation of the Hospitals and Health Centers of the National Health Service with the Military Hospitals and the Health Services of the Armed Forces" provides for the possibility to the citizens of the country to enter for the provision of health services 4 in the military hospitals of Athens and 4 "3... All citizens gain access to the Military Hospitals of Athens and Thessaloniki ... in order to serve the health needs of the population of the country.... patients who are transported through EKAB are served during working hours... Citizens have the right of access to the laboratories as well as to the special clinics of the above Military Hospitals... with the possibility of carrying out specialized tests

for each citizen or through a referral from NHS Hospitals where he is hospitalized the patient either by direct appointment. In order to better serve the citizens, an indicative table of special examinations that can be carried out in 9 Thessalonikis, including the 401 GSNA, is posted on the internet, as well as the possibility of transferring patients to these hospitals through EKAB or direct telephone appointments, without specifying that the citizens are bound by any kind of secrecy or confidentiality of classified information in order not to disclose to any third party the fact of their entry and stay for the purposes of hospitalization or accompanying or visiting patients, as otherwise provided in other cases (cf. article 35 of Law 3978/2011 Official Gazette A' 137/16-6-2011 "Contracts for Defense and Security Procurement Projects" which incorporated article 22 of Directive 2009/81/EC). The importance for the examined issue of the lack of obligation to maintain confidentiality or secrecy for reasons of national security by those entering the hospitals, subjects of personal data, is also confirmed by position 401 GSNA (APDPX no. prot. 7034/16-10-2019) that in accordance with the National Security Regulation, among other things, the degree of security attributed to certain information and which is proportional to the risk posed to national security by its disclosure to unauthorized persons is provided for. The claim of 401 GSNA during the hearing that it alone, without the mediation or control of the Authority, has the absolute freedom to choose and establish the security measures and also to determine the level of these in relation to those entering its facilities , although valid, is not crucial for the question of the Authority's audit competence or not being examined in this case. The Authority does not have any kind of authority over the physical security measures of 401 GSNA, which the latter chooses and applies, however, to the extent that a processing is not carried out for an activity concerning national security, it competently exercises its control authority to judge the legality of processing and further relevant issues e.g. if the data controller has taken the necessary technical and organizational security measures in accordance with articles 5 par. 1, 24 and 32 GDPR. For the above reasons, the Authority considers that none of the conditions of the provisions of article 10 par. 5 of Law 4624/2019 are met and, therefore, the request-objection regarding the Authority's incompetence to deal with A's complaint against the 401 GSNA for reasons of national security. 4. Because Article 5 GDPR defines the processing principles that govern the processing of personal data. Specifically, it is defined in the paragraph in the said Hospitals as well as the contact numbers for the respective laboratories". 10 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity, transparency"), b) are collected for specified, explicit and legitimate purposes and are not 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 ("minimization of 5. Because, article 6 par. 1 GDPR provides, among other things, that: "Processing is lawful only if and as long as at least one of the following conditions applies: a) the data subject has consented to the processing of his personal data for one or more specific purposes, (…) e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of public authority delegated to the official right of processing". Article 9 para. 1 GDPR introduces, in principle, a ban on the processing of information that falls under special categories of personal data, i.e. personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership organization, as well as genetic data, biometric data for the purpose of indisputable identification of a person, data concerning health or data concerning a natural person's sexual life or sexual orientation. Subsequently, paragraph 2 of the same article states that: "Paragraph 1 shall not apply in the following cases: a) the data subject has provided express consent to the processing of such personal data for one or more specific purposes, unless the law of the Union or a Member State provides that the prohibition referred to in paragraph 1 cannot be lifted by the data subject (…) g) the processing is necessary for reasons of substantial public interest, based on the law of the Union or a Member State, which is proportionate to the objective pursued, respects the essence of the right to data protection and provides for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject (…)". 6. Because, in the case under consideration, from the data in the case file, it appears that 401 GSNA collects and keeps for a decade in a daily report the 11 name, ID number, office or place of visit, purpose of visit and time of entry - exit of incoming persons, patients of the Hospital or visitors of the patients. The Authority judges, in this case, taking into account the provision of article 4 par. 155 and recital 35 GDPR6, that the collection and retention of information related to the purpose of a natural person's visit, insofar as it concerns a patient of the Hospital, constitutes information that falls under the special category of personal data, as it is combined with the relevant file of the provision of health services of 401 GSNA may immediately disclose information regarding the health status of the specific natural person. The Authority further considers that the processing of the above information is legal, in accordance with the provisions of articles 5 and 6 par. 1 item. e', as well as 9 par. 2 item. g' GDPR, even in so far as they concern visiting patients and the patients themselves, respectively, insofar as the essential or essential public interest may consist in the protection, under military regulations, of military installations. Following the above, the Authority deems A's complaint against 401 GSNA as unfounded. 7. Because the GDPR recognizes the data protection officer (hereinafter DPO) as a key component of the new data governance system and establishes the conditions for his definition, position and duties. In particular, with regard to

the DPO definition, Article 37 para. 1 GDPR provides that "The data controller and

the processor appoints a controller in any case in which:

a) the processing is carried out by a public authority or body, except courts that

act within their jurisdiction, b) its core activities

controller or processor constitute processing operations,

which due to their nature, scope and/or purposes, require regularity

and systematic monitoring of data subjects on a large scale, or c)

5 Specifically defined as health data are personal data related to

the physical or mental health of a natural person, including the provision of services

health care, and which disclose information about his health status

(Article 4 item 15 GDPR).

6 According to Recital 35 of GDPR 2016/679, health data means, among

others, and the information about the natural person collected when registering for them

health services and their provision, such as a number, symbol or identifier

attributed to a natural person in order to fully identify him for health purposes.

the main activities of the controller or processor

constitute large-scale processing of special categories of personnel data

character according to article 9 and data concerning criminal convictions and offences

referred to in article 10". Furthermore, paragraph 3 of article 37 GDPR provides

that “If the controller or processor is a public authority or

public body, only one data protection officer can be appointed for

several such authorities or several such bodies, taking into account their organizational

their structure and size".

8. Since, from the records kept by the Authority under the GDPR and Law 4624/2019,

it appears that the General Staff of National Defense proceeded with the under no. first

C/EIS/8303/29.11.2019 (replacing it with under no. prot. C/EIS/3837/29.05.2019

of application) application in the announcement to the Authority of the contact details of the Ministry of Foreign Affairs which

defined, in accordance with the aforementioned provisions of article 37 of the GDPR and to

Article 6 of Law 4624/2019. Further, from the evidence in the case file,

it follows that 401 GSNA citing the possibility provided by the provisions of

of articles 37 par. 3 of the GDPR and 6 par. 2 of Law 4624/2019 claims that it has complied with

the fulfillment of the DPO definition, as the DPO (and/or the DPO office) of the General

of the National Defense Staff, according to his claims, has jurisdiction over issues

protection of personal data both at the General Staff and at

Units - Services belonging to them, therefore also in 401 GSNA.

According to the aforementioned provisions of the GDPR and Law 4624/2019, the

possibility of defining a DPO for more public authorities or bodies, in

but this case, in accordance with the guidelines "regarding the

data protection officers" issued by the working group of article 29, o

controller or processor, must ensure that one

only data protection officer, assisted by a team if necessary

required, he can effectively perform all his duties for all

public authorities and public bodies, to which it has been appointed7.

The Authority considers, in this case, that the designation of a single DPO and/or DPO office in

General Staff of National Defense for all services and responsibilities of all kinds

of the General Staff of National Defense and its supervised bodies, is not enough

for the effective performance of his duties and in terms of 401 GSNA, for the

7 WP 243 rev. 01 from 13.12.2016, as last revised and approved on 05.04.2017, p.14,

available at https://edpb.europa.eu

which requires the definition of the DPO independently, given that it is a public body,

whose main activity is the systematic monitoring of natural persons in

large scale (providing health services to patients) and involves processing

of special categories of personal data on a large scale (data

patient health). Following these, the Authority considers that in this particular case

it is appropriate to exercise the corrective power according to article 58 par. 2 item. 4 GDPR with

the imposition as an appropriate corrective measure of the imposition of 401 GSNA

obligation to appoint a Data Protection Officer.

The beginning

FOR THOSE REASONS

a) rejects as unfounded the claim-objection of the 401 General Military

of Athens Hospital that pursuant to article 10 par. 5 last subsection of Law 4624/2019 the Authority

does not have jurisdiction to deal with A's complaint against him as far as

processing of personal data carried out for the activities

relating to national security,

b) rejects A's complaint against the 401st General Military as unfounded

Athens Hospital and considers that the specific processing is legal, according to

with the provisions of articles 5, 6 par. 1 item e' and 9 par. 2 item. g' GDPR 2016/679 and

c) calls, pursuant to article 58 par. 2 item. d' GDPR 2016/679, 401 General

Athens Military Hospital to arrange for the appointment of a Protection Officer

Given in a way that meets the requirements of GDPR 2016/679 and

of Law 4624/2019, according to what is mentioned in the reasoning herein.

The president

The Secretary

Konstantinos Menudakos

Paleologo Georgia