Athens, 29-12-2021 Prot. No.: 3027 DECISION 54/2021 The Personal Data Protection Authority convened at the invitation of its President in a teleconference meeting on Tuesday 23.11.2021 at 12:00, adjourned from the meeting of 16.11.2021, 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, were present, as rapporteur, Konstantinos Lambrinoudakis and Charalambos Anthopoulos. Present, without the right to vote, were Chariklia Latsiu, legal auditor - lawyer, as assistant rapporteur and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With the complaint from ... (and with No. prot. APD C/EIS/1921/18.03.2021) A informs the Authority that he submitted to the D.O.Y. X, where he works, from ... and with no. first ... application, in order to obtain a special leave of absence, which he accompanied, among other things, with the medical opinion of doctor B from ..., which certifies that he additionally suffers from ... . In the framework of the supporting documents that he submitted to his Service for the above purpose, A complains that: "(...) on ... I received knowledge that it was notified on ... to the Employees' Association at D.O.Y. Φ by order of the Head of the D.O.Y. X, the dated ... medical opinion of Doctor B, by virtue of which it is confirmed that I suffer from ..., without any prior information from me and obtaining my necessary consent and with the purported purpose of preventing me from possible future blood donation". Furthermore, 1-3 Kifissias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 A requests the Authority, through the power of attorney of Nopis Tintzoglidou, to instruct the Head of D.O.Y. X "to stop the illegal transmission of my principal's data to third parties, in accordance with the relevant legislation". From the accompanying information submitted to the Authority by complainant A, it appears that on ... he submitted a request to the Independent Data Protection Officer Support Department of A.A.D.E. requesting to be informed about: a) which documents, containing his special category personal data, have been communicated by his service to third parties, b) the recipients, to whom they were communicated, c) the time and manner of their communication and d) the legitimate reason for their notification. In response to the above request, A received the no. first ... response from D.O.Y. X, following previous correspondence with the Independent Support Department of the Ministry of Internal Affairs of the A.A.D.E., in which the following is included: "(...) Because you are an employee, a servant in the D.O.Y. X, to which you have applied for and received from time to time a blood donation permit (last certificate ... with A.P. ... of the Employees' Association of D.O.Y. F). Because, in the medical opinions, which you yourself presented to our Service for the granting of a special purpose permit in the context of measures to deal with the spread of the COVID-19 pandemic, it is stated that you are a person belonging to a

high-risk group, in need, according to the opinions, mandatory stay at home, leave, which was granted to you. Because, within the time frame of the covid-19 pandemic and after you had already submitted the medical opinions of doctor C from ... (date of submission) and ... to our Service, that you suffer from a serious health problem and while you were on sick group leave due to of a serious health problem, you have applied through our Service to the Human Resources Management Division (Department B) of the General Directorate of Human Resources and Organization of A.A.D..E. on ... through your application with number ... your secondment to the D.O.Y. Ψ for the months of … year …, an application in which the recommendation of our Head of Service had been worded as follows: "the employee is on sick group leave (…) and does not produce work in our service, therefore as long as his health is not threatened 2 we have no objection to his application." Subsequently, and while you continued to be on a special purpose leave, you presented to our Service the certificate from ... DYPE ... PEDY Health Unit Y and the certificate from doctor B. Because, given the obvious contradiction arising from your above-mentioned applications (on the one hand, a serious health problem and therefore the granting of a special purpose permit as a person belonging to a vulnerable group, on the other hand, at the same time, an application for a three-month secondment to a tourist island area with high traffic both from abroad and internally, but also your application for a permit due to donating blood as a result certificates of the Employees' Association D.O.Y. F), and mainly due to the fact that our Service had learned from there that you suffer from serious illnesses, as you yourself had informed us, and at the same time you are a blood donor at the blood bank of the Employees' Association in D.O.Y. Already active, as can be seen from your aforementioned applications for blood donation permits. For these reasons, we deemed it imperative, primarily for reasons of public health protection, i.e. an indefinite number of patients who may need and receive the transfused blood, but also you who provide the blood without possibly having previously informed the blood donation center about the state of health, such as informing the blood donor of the existence of the above medical events, so that the appropriateness of the transfused blood can be medically investigated and, depending on the results, the blood donation for you as a blood donor can be allowed or excluded. We sent the from ... certificate of doctor B, necessary for assessment in our judgment for the above reasons, through ... with the numbered ... document of our Service to the above blood donation organization with the subject "BLOOD DONATION", as competent for carrying out the process of donating blood, maintaining the register of blood donors and the aforementioned purposes having indeed taken into account and absolutely respecting both the relevant legislation (…) which provide for the cases of deviation from art. 9 par. 1 as above European GDPR for the processing of the special categories of personal data, as well as the laws

of the transfused blood for the security 3 interests of you as the subject of the special categories of personal data (…)". The Authority, during the examination of the case, called with reference no. prot. C/EXE/962/31.03.2021 document of the Authority the D.O.Y. X to provide explanations on the complaints. In response to the Authority's above document, the Authority was submitted under no. first ... from ... (and with no. prot. APD C/EIS/2602/15.04.2021) response of the Independent Support Department of the Data Protection Officer of AADE, which includes, among others, the no. first ... response from D.O.Y. X to the Independent Support Department of the Ministry of Foreign Affairs of AADE. In under no. first ... response from D.O.Y. X entitled "Proposal of response to the Authority's document" the Head of D.O.Y. X informs that he forwarded to the Employees' Association Φ the under no. first ... document, with the following content: "We inform you, according to the attached documents, that employee A has presented to our service a certificate that he suffers from ... . We ask for your own actions', further forwarding to the said Association the disputed by ... medical opinion presented by the complainant A to the service. Moreover, refuting the claim of the complainant that he had no intention of donating blood again after the diagnosis of his condition, he argues that: "(…) however his attitude in relation to his condition and its consequences does not appear sufficiently responsible and this is proven from the mentioned events, as within the time frame of the covid-19 pandemic and after the applicant employee had already submitted the medical opinion of the doctor from ... and ... he (...) requested (...) his secondment to the D.O.Y. Ψ for the months of ... year ..., an application which was not accepted. Consequently, his non-inclusion among blood donors in the interim may be the result of either the disputed document of the D.O.Y. X, or of the fact that the complainant is on special purpose leave anyway for the entire interim period (…). While in order to verify this claim, it must be known when this diagnosis occurred. However, it should be noted that already from ... he had presented a certificate with ... and his last blood donation was just one month and five days ago, namely on ... (...)". Afterwards, the Head of D.O.Y. X invokes, among other things, the provisions of article 24 4 par. 1 item a' and b' of Law 4624/2019, informs that the blood donation is carried out during working hours with the organization and supervision of the Association of Employees at the D.O.Y. Φ and concludes: "(...) based on the specific behavior of the employee, my responsibility as head of the Service of which the complainant is an employee and my responsibility towards society as a whole from my actions or omissions in this capacity, I deemed it appropriate to inform the top body of blood donation (…) as responsible for carrying out the blood donation process, keeping the register of blood donors and for his actions for the safety of the blood being transfused (…)".Finally, he argues that the transmission of the medical opinion in question does not indicate that the complainant was a

hostile person, nor that he had a friendly or other social relationship with him. The Independent Support Department of the Ministry of Internal Affairs of AADE, with the no. prot. ... from his ... document, asserts among other things: "When our service was informed (...) about the complainant's case, it dealt with what was mentioned in the document of the D.O.Y. X facts as an incident of personal data breach and with the e-mail from ... requested to be informed by the Association of Employees in D.O.Y. Φ regarding whether the employee's personal data was further forwarded, but to date we have not received a response from the Association (...). In parallel with the above actions, our department (…) made a reasoned recommendation to the Commander of the AADE: 1. The non-disclosure of the incident to the Protection Authority pursuant to Article 33 of the GDPR, as there were no indications of possible harm or damage to the data subject from the incident, despite the involvement of special class personal data in it. And this is because knowledge of the employee's personal data was obtained by a clearly defined and limited circle of persons (employees of the Employees' Association at D.O.Y. F), the majority of whom are civil servants bound by an obligation of confidentiality (Article 26 of the Civil Servant Code), the disclosed health data (information that the employee suffers from ...) were not capable of discriminating against the data subject but 5 and because any further transmission of the data to the blood donation center collaborating with the club does not entail adverse consequences for the data subject data, on the one hand because the blood donation center probably already has the data in question from the employee (data subject) himself, who is obliged to disclose it to him in the context of obtaining the donor's medical history (see article 5 in conjunction with ANNEX II , PART B paragraph 2 of PD 138/2005) on the one hand because the employees of the blood donation center let them be bound by medical confidentiality. 2. Non-notification of the incident to the data subject according to Article 34 GDPR, because the complainant was informed about the processing of health data by the D.O.Y. X, under no. first ... her document. The above recommendation of our service was approved by the Governor of AADE and the case was placed in the file of cases of incidents and potential incidents of personal data breach (article 33 par. 5 GDPR)". Subsequently, the Authority called under no. prot. APD C/EXE/1384/07.06.2021 document D.O.Y. X as provides additional clarification. Due to the non-response of D.O.Y. X in the above document, the Authority came back with the newest under no. prot. APD C/EXE/1804/09.07.2021 document. Following these, the D.O.Y. X with the no. prot. ... (and with no. prot. APD G/EIS/5105/02.08.2021) document replied that "(...) according to DIDAD/F.69/126/16316/20.9.2020 circular of the Ministry of Interior (...) the groups of increased risk were redefined and the conditions for granting a special permit in absence to groups of increased risk were defined. According to the above, in order for the employees to be included in groups of increased risk in

order to be entitled to a special permit of increased risk, they should henceforth be subject to at least two of the cases listed in the DIDAD by presenting respectively medical opinions from the attending physician of the relevant specialty or from a physician of the relevant health structure specialty (public or private). Finally, it is clarified that the mentioned medical opinion of doctor B was forwarded through ... to the Association of Workers at D.O.Y. Φ with our document no. ..., on the subject "BLOOD DONATION", as the body responsible for carrying out the blood donation, and the document submitted (initially by email and then as an original) is located and kept in the archives of our Service". 6 In addition, the Authority with no. prot. C/EXE/1386/07.06.2021 document invited the Workers' Association to the D.O.Y. Φ as it provides specific clarifications. Due to the non-response of the above Employees' Association to the Authority's document, the Authority came back with the newest under no. prot. APD C/EXE/1803/09.07.2021 document. In response to the above, the Employees' Association with no. prot. ... (and with no. prot. APD C/EIS/5018/30.07.2021) memorandum, informs, among other things, the Authority that: "(...) D) In the above context, and especially for employee A, the Our association was never requested either by him or by the D.O.Y. X the sending of any medical certificates and attestations in the form of supporting documents for the above employee's participation in blood donation. And this, because we are not a competent body to examine and approve the participation of employees in the blood donation program, actions and control that belong exclusively to the competent health personnel of the [hospital]. E) The disputed medical certificate concerning A was sent to us via ..., without a previous request on our part, and without prior notification from the competent department of the D.O.Y. X. For our part, we immediately notified the beneficiary and the data subject, A, and did not proceed with any processing of the disputed health data. G) It is necessary to point out that the health data in question was sent to us without our knowledge, without our involvement, or our intervention in any kind of automated or non-automated personal data file. And this is proven by the way it was sent to us, that is, through ...". In addition, he informs the Authority that "the disputed medical certificate was not processed by our Association or the Blood Bank... In particular, it was not transmitted to third parties and was not disclosed to third parties." Finally, the Employees' Association emphasizes with the above document, that it does not keep or process any personal data of the members who participate in the blood donation, and the latter is carried out exclusively at ... Hospital ..., under the supervision and responsibility of the medical and nursing staff, and in accordance with the procedure established by the National Blood Donation Center. Therefore, according to the above answer, the Employees' Association is not responsible for processing 7 the blood donations of its members, and it takes on an exclusively organizational and coordinating role. and C/EXE/2371/19.10.2021 C/EXE/2261/08.10.2021

C/EXE/2372/19.10.2021, Subsequently, the Authority with under no. prot. C/EXE/2262/08.10.2021, C/EXE/2263/08.10.2021, C/EXE/2259/08.10.2021 documents called the D.O.Y. X, the AADE with the indication that the Independent Protection Department of the Data Protection Officer, the Association of Employees in D.O.Y. Φ and A, respectively, as presented at a meeting of the Authority's Plenary on Tuesday 19.10.2021 in order to discuss the aforementioned complaint. At this meeting, the Authority adjourned the examination of the case. Subsequently, the Authority with no. prot. G/EXE/2373/19.10.2021, and G/EXE/2374/19.10.2021 documents called the D.O.Y. X, the AADE with the indication that the Independent Protection Department of the Data Protection Officer, the Association of Employees in D.O.Y. F and A, respectively, as presented at a meeting of the Plenary of the Authority on a new date for discussion of the case, on Tuesday 26.10.2021. This meeting was attended by D, Head of D.O.Y. X, E and F, General Director […] of AADE, respectively, Z, Deputy Head […] of AADE, H, President of the Workers' Association in D.O.Y. F, as well as Ioannis Karouzos (AM DSA ...) and Marianna Katsiadas (AM DSA ...), attorneys-at-law of the above Association and A after the attorney Nopis Tintzoglidou (AM DSA ...). During this meeting, those present, after developing their views, were given a deadline of 01.11.2021 to submit written memoranda. Following this, the Head of D.O.Y. X with the no. ... (and with prot. no. C/EIS/7055/01.11.2021) document and the Independent Support Department of the Ministry of Internal Affairs of AADE with the no. ... (and with no. prot. APD C/EIS/7045/01.11.2021) document, submitted their relevant memoranda on time. 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 , 8 CONSIDERED ACCORDING TO 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 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 particular, from the provisions of articles 57 par.1 item. f of the GDPR and 13 par. 1 item g΄ of Law 4624/2019 it follows that the Authority has the authority to deal with the complaint of A against D, Head of D.O.Y X, since the transmission of the disputed medical opinion of doctor B by D.O. Y.X to the Employees' Association Φ through ... constitutes automated processing of personal data, subject to the regulatory scope of the articles 2 para. 1 of the GDPR and 2 of Law 4624/2019. Besides, the disputed opinion submitted to his service by the complainant A was included in the filing system of the personal register, with classification criteria no. first ..., the name of the complaining

employee and the subject of his request (special leave of absence). 2. Because, under no. No. D.ORG.A 1125859 EX2020 (Government Gazette B´ 4738/26.10.2020) Organization of the Independent Public Revenue Authority (hereinafter AADE) provides in article 1: "1. The Independent Public Revenue Authority (A.A.D.E), hereinafter Authority or A.A.D.E, which was established with the provisions of paragraph 1 of article 1 of Chapter A` of Part One Law 4389/2016 "Emergency Provisions for the Implementation of the Agreement on Fiscal Goals and Structural Reforms and Other Provisions" (A' 94), based in Athens, is an Independent Administrative Authority without legal personality. 2. Mission of A.A.D.E. is the determination, certification and collection of tax, customs and other public revenues, which are related to the scope of its competences. 3. A.A.D.E. enjoys operational independence, administrative and financial autonomy and is not subject to control or supervision by government bodies, state bodies or other administrative authorities, 9 except to parliamentary control, in accordance with the provisions of the Rules of Procedure of the Parliament and with the procedure defined in the provisions of Article 4 of Law 4389/2016.(...)". Furthermore, from article 48 of the Organization of AADE it follows that D.O.Y. X is a regional service of the AADE that organically falls under the General Directorate of Tax Administration and does not have an independent legal personality. It follows from the above that the Authority, within the framework of the powers granted to it by the GDPR and Law 4624/2019, has the authority to deal with A's complaint against D.O.Y. X, which organically and/or functionally falls under the A.A.D.E. position to prove its compliance with the processing principles established in paragraph 1 of article 5. As the Authority1 has judged, a new model of compliance was adopted with the GDPR, the central point of which is the principle of accountability in the context of which the controller processor is obliged to design, 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 data 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, according to the provisions of article 4 par. 7 GDPR as a 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 (…)". And according to Opinion 1/2010 on the concepts of "controller" and "processor" of the Article 29 Working Group for the definition of the controller, according to the aforementioned definition, three main elements are taken into account: 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") 1 See Authority decision 26/2019, paragraph 8, available on its website. 10 and c) the basic characteristics to distinguish the controller from other actors ("determine the purposes and manner of personal

data processing")2. It is pointed out that the concept of the data 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 attribution of responsibilities in the event of their violation 3. Further, it is explained in the above-mentioned Opinion 1/2010 regarding the first element - as stated in the immediately preceding paragraph: "In the strategic perspective of the distribution of responsibilities, and in order to provide the persons to whom the data refer a more stable and reliable reference entity for the exercise of the rights under the Directive, it is preferable to consider the company or body as controller rather than a specific person within the company or body. The company or body will ultimately be held responsible for the processing of the data and for the obligations arising from data protection legislation, unless there is clear evidence that a natural person is responsible. In general, it should be assumed that the company or public body is responsible for the processing activities that take place in the context of their activities and risks. Sometimes, companies and public bodies appoint a specific person responsible for carrying out the processing tasks. However, even where a specific natural person is appointed to ensure compliance with data protection principles or to process personal data, that natural person will not be the controller, but will act for account of the legal entity (company or public body), which will remain liable in the event of a violation of the principles in its capacity as responsible WP 2 from http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm 3 See regarding Opinion 3/2010 on the principle of accountability of the Article 29 Working Group, wp 173 of 13.07.2010. 16.02.2010, website available at 169 11 processing (…) However, in the strategic perspective of the distribution of responsibilities, it is preferable to consider the company or body responsible for processing rather than a specific person within the company or body. The company or body will ultimately be held responsible for data processing and obligations under data protection law, unless there is clear evidence that a natural person is responsible, for example where a natural person who works for a company or a public body uses data for his own purposes, outside of the company's activities." 4. In addition, it is clarified in the aforementioned Opinion 1/2010 of the Article 29 Working Group: "(...) It does not matter if the decision to process data is "lawful", in the sense that the entity that took the relevant decision was legitimized to do something such or that the controller was appointed formally, according to a specific procedure. The question of the lawfulness of the processing of personal data will matter at a different stage and will be assessed in the light of other articles (in particular, Articles 6-8) of the Directive. In other words, it is important to ensure that, even in those cases where data processing is unlawful, a controller can easily be identified and held responsible for the processing (…). Special analysis is required in cases where a natural person acting in the context of a legal entity uses data

for its own purposes outside the scope and potential control of the legal entity's activities. In this case, the natural person involved will be the designated controller and will be responsible for the specific use of the personal data. The original controller may nevertheless retain some responsibility in the event that the new processing took place due to a lack of appropriate security measures (…) If a natural person working for a company or a public body uses data for his of the objectives, apart from the activities 4See WP 169 from 16.02.2010, p. 21 ff., p. 42 ff. 12 of the company, the person in question is considered de facto responsible for processing and bears responsibility in this capacity"5. Finally, the Article 29 Working Group in Opinion 1/2010 has accepted that "access to data does not in itself imply control, while on the other hand, that access to data is not an essential condition for the designation of the controller"6. Subsequently, the European Data Protection Board (EDPB), now interpreting the GDPR, accepted with Guidelines 07/2020 that the ability to access the filing system, nor certainly the "possession" of the filing system or the supervision in this, it is enough to determine the purpose of processing even in "foreign" files7. 5. Because, article 4 of P. Legislative Decree 178/2004 (Government Gazette A΄154) entitled "Maintenance and updating of personnel register data" provides, among other things: update of all the elements that make up thepersonal register, as well as for the transmission of these details, when this is required by special provisions of law, after having previously informed the employee, taking all the necessary measures to ensure the confidentiality of this content. Depending on the needs of the service, the head of the personnel service can designate for the performance of the above duties employees who serve in the organic unit, in which he heads or in the units subordinate to it. (…) .4. In addition to what is defined in the previous paragraphs 2 and 3 and without prejudice to the provisions of paragraph 5 of article 23 of the Public Status Code 5 WP 169 from 16.02.2010, page 13 ff. 21-22. 6 p. 26, Opinion 1/2010, WP 169. 7 (…) It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller" (p. 3), "42. It is not necessary that the controller actually has access to the data that is being processed. Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data" (p. 16). 13 Civil Administrative Officers and Employees of the N.P.D.D. sanctioned by Law 2683/1999, the knowledge and access of any third party to the content of the data in the personal register is excluded. (…) 5. The details of the personal register are registered and subject to processing electronically. During the registration and processing, all necessary measures are taken to exclude: (a) the access of any third

party to them, in accordance with and as defined in the previous paragraph 4 of this article and (b) the alteration, destruction, loss of the data kept electronics. 6. The maintenance and processing of the data of the employee's personal register, as well as the obligations of those responsible for its maintenance, are additionally governed by the current provisions on the processing of personal data". 6. Taking into account the information contained in the immediately preceding considerations herein, all the elements of the case file, the hearing procedure and the submitted memoranda, the Authority considers in this case that the data controller, according to article 4 par. 7 GDPR, the alleged processing of the transmission of the disputed medical opinion by ... is the AADE, as the purpose and method of the collection, transmission and in general processing of the employees' personal register while ensuring an appropriate level of security against risks is determined by the last. In this case, the claim of AADE, the Autonomous Support Department of the Ministry of Internal Affairs of AADE and D.O.Y. is rejected. X that due to the fact that the Head of D.O.Y. was responsible for maintaining the personal register of the complaining employee. X therefore becomes a data controller, according to article 4 par. 7 GDPR, of the reported processing. And this, because based on what was discussed in the immediately preceding considerations, on the one hand, the element of access/physical authority of the Head of the D.O.Y. X in the information entered in the personal register of the complaining employee does not constitute an essential condition for the assignment to him of the role of data controller. On the other hand, because, assuming the claim that the Head of 14 D.O.Y. X, regarding the alleged processing of the transmission of the disputed medical opinion, acted voluntarily, the adoption of appropriate organizational and technical security measures of the employees' personal register is determined by the AADE. This is implicitly agreed by the Independent Support Department of the Ministry of Internal Affairs and Communications of the AADE, as well as with the document No. ... (which is forwarded to the Authority with its document No. ...) - and at a time subsequent to the reported transmission of disputed medical certificate and in any case before the response of the D.O.Y. X in satisfaction of the complainant's request - provided internally to the services of the AADE Organization "instructions regarding the processing of health data of AADE employees in the context of granting licenses for health reasons". Furthermore, it did not appear that the Head of D.O.Y X when transmitting the disputed medical opinion, even if it is accepted that he acted voluntarily, and beyond the appropriate organizational and technical security measures taken or should have been taken by AADE, as a data controller, for the processing of data of the complaining employee from the personnel file of the registry, he acted for his own goals, outside the scope of potential control of AADE's activities. Furthermore, from the records kept by the Authority regarding the independent obligation of the data

controller pursuant to par. 7 of article 37 GDPR to notify the Authority of the contact details of the data controller it must appoint, it appears that a data protection officer has been notified to the Authority for AADE, as controller and not for D.O.Y. X independently, as controller. 7. 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 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 illegal processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality')'. 8. Because, as the Authority has judged8, taking into account the decisions of the Court of Justice of the European Union (CJEU)9 and the Council of State10, in order for personal data to be lawfully processed, i.e. processing in accordance with the requirements of the GDPR, it should to cumulatively meet the conditions of application and observance of the principles of article 5 par. 1 GDPR. The existence of a legal basis (Articles 6 and 9 GDPR) does not exempt the data controller from the obligation to comply with the principles (Article 5 para. 1 GDPR) regarding legality, necessity and proportionality and the principle of minimization11. 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 applying the legal bases of articles 6 and 9 of the GDPR is omitted , for the processing, respectively, of simple and special category personal data. Consequently, the illegal collection and processing of personal data in violation of the principles of Article 5 GDPR is not cured by the existence of a legitimate purpose and legal basis12. 9. Because, according to the provisions of Law 3402/2005, the competent authority for the coordination, control, recommendation for licensing and supervision of the individual blood donation services is the National Blood Donation Center, while the 8 See in particular, decision 44/2019 of the Authority, s. 17, available on its website. 9 See CJEU decision of 16-01-2019 in case C-496/2017 Deutsche Post AG v. Hauptzollamt Köln, sc. 57. 10 See decision StE517/2018, sc. 12. 11 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 12 See in particular decision 38/2004 of the Authority, available on its website. 16 exclusive competence and responsibility for the collection, disposal and management of blood, based on internationally accepted

principles, belongs to the Ministry of Health and is exercised through the E.KE.A. and Blood Donation Units (articles 1 and 4). Furthermore, it is provided in article 10 of the above law: "(...) B. The Hospital Blood Donation Services (N.Y.A.) are hospital units that cooperate with the Blood Center, with which they are interconnected, supervised and controlled by the E .KE.A., regarding the blood donation process and blood management in general and they have the following responsibilities (...) 6. They carry out blood draws in accordance with the international rules and instructions of the E.KE.A. both in the hospital and in the district, with mobile blood collection units. 7. Provide prescribed information to prospective blood donors and assess their eligibility. (…) 11. Maintain traffic records and conduct incompatibility investigation. (…) 18. They implement a system identification of each blood donation and each unit of blood and components, which allows identification of the donor, as well as the transfusion and the related recipient.(…) 19. They have a procedure that allows the effective and verifiable withdrawal from the distribution of blood or its components associated with serious and adverse events and reactions'. 10. Pursuant to the above, in the considered complaint, the test of the suitability of the complainant's blood donor is judged by the medical and nursing staff of [...] Hospital ..., which manages the Blood Bank ... of the Employees' Association of the D.O.Y. F, in the context and under the conditions of the E.KE.A., in accordance with and under no. first ... (and with no. first APD G/EIS/5018.30.07.2021) response of the Employees' Association to the DO.Y. F to the Authority. It is noted, moreover, that the Authority, under the existing institutional framework for data protection (law 2472/1997 and Directive 95/46), examining the relevant notice of record keeping of the National Register of Voluntary Blood Donors, decided with the license no. 1598/2015 that the Ministry of Health and the E.K.E. are jointly responsible for the processing of the National Register of Voluntary Blood Donors, and the processing is carried out by the company National Research and Technology Network (EDET S.A.) and the country's Hospitals, the competent services of which 17 are connected to the central information system of the National Registry of Voluntary Blood Donors. 11. Taking into account the above, it follows from all the elements of the case file that the complained processing of the transmission of the disputed by … medical opinion of doctor B, which the complainant presented to his service for the purpose of granting the requested special license absence, in the Employees' Association Φ it was done in violation of the provision of article 5 par. 1 item. a' of the GDPR. Specifically, the claim of the D.O.Y. X in no. ... response to the Independent Support Department of the Ministry of Foreign Affairs - claim, which is repeated in no. ... response from the D.O.Y. X to the complainant, in satisfaction of the request he addressed to the Independent Support Department of the Public Health Service of the AADE - that, i.e. the transmission of the disputed medical opinion was imperative "for reasons of

protecting public health, i.e. an indefinite number of patients who may need and they will receive the transfused blood, but also of the employee himself who provides the blood without possibly having previously informed the blood donation center about the state of health, as we inform the body of the blood donation about the existence of the above medical events, so that it can be medically investigated the suitability of the transfused blood and to allow or exclude, depending on the results, the blood donation for the specific blood donor (…)" is rejected as unfounded. And this, because the legal recipient of the disputed medical opinion cannot be the Association of Workers in the Public Health Organizations. Φ, as according to the aforementioned provisions of Law 3402/2005, the competent authority for the control of blood donation is the E.K.E.A., while the control of the suitability of the blood of the complaining blood donor is carried out by the medical and nursing staff of […] Hospital ..., which manages the Blood Bank ... of the above Employees' Association. Furthermore, the Authority considers that the alleged processing of the transmission of the disputed medical opinion was done in violation of the principle of data minimization (Article 5 para. 1 letter c GDPR), as even if the claim that the transmission was made for reasons protection of 18 public health, it was sufficient to transmit it and not to list the condition (...) of the complainant in no. first ... transmission document of the D.O.Y. X to the Association of Workers in D.O.Y. F. Furthermore, the Authority considers that since the transmission of the disputed medical opinion was carried out in violation of the principles of article 5 par. 1 item. a' and c' GDPR, there is no need to examine any legal bases according to articles 9 GDPR, 22 and 24 of Law 4624/2019, as on the one hand the existence of any legal bases does not exempt the data controller from observing and applying the general principles of data processing of article 5 par. 1 of the GDPR as discussed above, on the one hand, the granting of blood donation permits, as well as sick leaves, and the process of checking the fulfillment of the conditions for their granting are specifically regulated by the provisions of Law 3528/2007 (in particular, articles 50 and 54 ff.). 12. The Authority, in relation to the established violation of the principles of article 5 par. 1 item. a' and c' of the GDPR for the alleged processing of the transmission of the disputed medical opinion of the complainant to the Association of Employees at D.O.Y. F, considers that there is a case to exercise its corrective powers under article 58, paragraph 2 of the GDPR. In particular, the Authority after taking into account the claim put forward in the hearing process by the Association of Workers in D.O.Y. F, that the transmitted by D.O.Y. X medical opinion concerning A, was delivered by the Association to the complainant, and therefore, is not kept in its records, it considers that it must send an order, according to article 58 par. 2 item. d' GDPR, to AADE as data controller, to delete from its files the no. ... document, with which the medical opinion in question was illegally transmitted and in which the

condition of the complaining employee is stated. Furthermore, the Authority considers that the imposition of the above corrective measure is not sufficient to restore compliance with the above general principles of the GDPR that have been violated and that it should, based on the circumstances established, be imposed, pursuant to the provision of the article 58 par. 2 sec. i GDPR, and an effective, proportionate and dissuasive administrative fine according to article 83 GDPR in accordance with the Guidelines "for the application and determination of administrative fines for the purposes of the 19 regulation 2016/679" of the working group of article 29. When evaluating the data, in order to choose the appropriate corrective measure to restore compliance, as well as to punish the illegal behavior, the Authority considers that the specific violation related to the processing of a special category of personal data (health data, article 83 par. 2 item g) and that it constitutes an individual case (article 83 par. 2 item a) 13. Since, article 5 par. 1 item f GDPR provides that personal data: "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"). Furthermore, Article 32 GDPR regarding the security of processing provides: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, as the case may be: (…) b) the ability to ensure the confidentiality, integrity, availability and reliability of the systems and processing services on an ongoing basis (…). 2. When assessing the appropriate level of security, particular account shall be taken of the risks deriving from the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, transmitted, stored or otherwise processed. (…) 4. The controller and the processor take measures to ensure that any natural person acting under the supervision of the controller or the processor who has personal data who has access to personal data processes it only on the instructions of the controller, unless required to do so by Union or Member State law'. It follows from the above that the GDPR must ensure, by using appropriate technical and organizational measures, that personal data are processed in a way that guarantees the appropriate security of personal data, including their protection from illegal processing . Consequently, a key feature of any data security policy is to provide the ability, when possible, to prevent a breach and, should it hopefully occur, to respond in time. 14. Because, in this case, the observance of the appropriate technical and organizational measures, in the context of an

appropriate security policy regarding the observance of the personal register of employees by AADE, as the controller, would provide for: a) the prohibition of the transmission of health data of the complainant employee to a non-legal recipient, i.e. toAssociation of Employees at D.O.Y. F, taking into account, in any case, the above-mentioned provision of article 4, paragraph 2 of Presidential Decree 178/2004, which requires prior notification of the employee concerned, b) ensuring the confidentiality of the content of the personal register and c) the possible legal transmission of health data with a classified document and in an encrypted file, and by taking these measures the alleged violation could possibly be prevented. As a consequence of the above, at the level of security policy and to the extent that the complained processing was carried out, i.e. the opinion in question was sent, AADE, as the controller, had to, with a timely reaction to limit the violation, delete from its files the ' No. first ... transmission document of D.O.Y. X which was not classified and the complaint's employee's illness was stated in its body. 15. Because, subsequently, in accordance with the provisions of article 4 par. 12 GDPR defines a personal data breach as "the breach of security that leads to the accidental or unlawful destruction, loss, 21 alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". This definition is explained in terms of "unauthorized or illegal processing" in the Guidelines of article 29 regarding the notification of personal data breaches pursuant to Regulation 2016/679 as follows: "(...) Finally, unauthorized or illegal processing it may include the disclosure of personal data to (or access by) recipients who are not authorized to receive the data (or have access to it) or any other form of processing that violates the GDPR" (p. 7)13. 16. Because, in the considered complaint, the transmission of the disputed medical opinion constitutes an illegal disclosure of personal data or, otherwise, based on the principles of information security in accordance with Opinion 3/20214 of the OE of article 29 regarding the notification of a breach of personal data14 and the Article 29 OE Guidelines on the notification of personal data breaches under Regulation 2016/679, breach of privacy. 17. Because, Article 33 para. 1 GDPR provides: "In the event of a breach of personal data, the data controller shall immediately and, if possible, within 72 hours of becoming aware of the breach of personal data notify the supervisory authority competent in accordance with Article 55, unless the breach of personal data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay.' 13 WP250rev.01 from 03.10.2017, as As finally revised and issued on February 6 http://ec.europa.eu/justice/data- protection/index_el.htm, p 7. 14 Opinion 03/2014 on the notification personal data breach http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf,. available online 2018,

location 22 The importance of being able to detect a breach in order to assess the risk to persons and then to notify it, if required, is highlighted in recital 87 GDPR: "It should be ascertained whether they have put in place all appropriate technological protection measures and organizational measures for the immediate detection of any breach of personal data and the immediate notification of the supervisory authority and the data subject. It should be established that the notification was made without undue delay, taking into account in particular the nature and seriousness of the personal data breach, as well as its consequences and adverse results for the data subject. This notification may lead to intervention by the supervisory authority, in accordance with its duties and powers defined in this regulation"15. from 18. Since recital 75 GDPR clarifies that the risk to the rights and freedoms of natural persons may consist of: "physical, material or non-material damage, in particular when the processing may lead to discrimination, abuse or interception identity, economic loss, damage to reputation, loss of confidentiality of personal data protected by pseudonymisation, or any other significant economic or social disadvantage; when data subjects could be deprived of their rights and freedoms or prevented from exercising control on their personal data; when personal data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership are processed and genetic data is processed, data that professional secrecy, unlawful removal 15 Worth noting that recently those from 14.01.2021 (under public consultation) Guidelines 1/2021 on examples regarding the notification of incidents of breach of the EPR underlines the factor of human error in incidents of breach and the need to ensure appropriate safeguards to prevent human errors. See Guidelines 01/2021 on Examples regarding Data Breach Notification, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotifica tionexamples_v1_en.pdf, p. 19. 23 relate to health or data relating to sex life or criminal convictions and offenses or related security measures; when personal aspects are assessed, in particular when an analysis or prediction of aspects relating to work performance, financial situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; when personal data of vulnerable natural persons, in particular children, are processed; or when the processing involves a large amount of personal data and affects large number of data subjects". Accordingly, Recital 85 GDPR explains the physical, material or non-physical damage to natural persons as a result of the breach as follows: "loss of control over their personal data or the limitation of their rights, discrimination, misuse or interception of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or other significant economic or social disadvantage for the natural person concerned". identity, economic unlawful loss, removal Finally, it is clarified that OE 29 in

the above-mentioned CG regarding the notification of personal data breaches pursuant to Regulation 2016/679 recommends that when assessing the risk to persons as a result of a breach, the data controller should consider the specific circumstances of the breach, taking into account the following criteria: 1) type of breach, 2) nature, sensitivity and volume of data, 3) ease of identification of the persons, 4) seriousness of the consequences for the persons, 5) special characteristics of the person , 6) special characteristics of the controller and 7) number of affected persons16, while also referring to the relevant ENISA Recommendations a methodology for assessing the seriousness of personal data breaches17. 16 p. 27 seq. WP250rev.01 from 03.10.2017. 17 Available on the website https://www.enisa.europa.eu/publications/dbn-severity 24 19. Because, in this case, the illegal transmission of the disputed medical opinion of the complainant A to the Association of Workers in the D.O.Y. Φ was likely to lead to a risk to the rights and freedoms of the complainant, as a) it led to the disclosure of health status protected by professional confidentiality (medical confidentiality), b) it was processing of personal data relating to health, c) it constituted processing of a vulnerable person, belonging – even potentially – to the groups at increased risk of contracting the coronavirus COVID-19, d) the work status/suitability of the specific employee was carried out, e) it entailed the risk of discrimination of the specific employee against the rest of his colleagues and possibly members of the Workers' Union in question, as well as voluntary blood donors. Following the above, the Authority considers that the alleged illegal processing constitutes a data breach that should have been notified to the Authority, according to Article 33, paragraph 1 GDPR. assessment framework in the of the personal data bound Besides, the Authority considers that the data cited by the Independent Support Department of the Ministry of Internal Affairs of the AADE, in reference no. first ... from ... his document to the Authority for the non-disclosure of the incident to the Authority according to Article 33 of the GDPR, namely that: a) the employee's knowledge was received by a clearly defined and limited group of persons (employees of the said Employees' Association), b) the majority of whom are civil servants 26 of the Civil Servant Code), c) the health data disclosed (information that the employee suffers from ...) was not capable of discriminating against the data subject, d) but also because any further transmission of the data to the blood donation center cooperating with the association does not entail adverse consequences for the data subject, on the one hand because the blood donation center probably already has the data in question from the employee himself, on the other hand because the employees of the blood donation center are bound by medical confidentiality , do not justify the failure to notify the Authority of the incident in accordance with article 33 of the GDPR, in view of the obligation of privacy (Article 25 of the risk of harm from the incident, as described in the aforementioned recitals 75 and 85 of

the GDPR, in accordance with the aforementioned Opinion 3/2014 of Article 29 regarding the notification of a personal data breach, as well as the Guidelines of Article 29 regarding the notification of personal data breaches under Regulation 2016/679. Furthermore, and for the above reasons, the decision of the AADE to archive the incident in question was incorrect. 20. Because Article 34 GDPR provides in paragraph 1: "When the breach of personal data may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data subject of the breach of personal data data (…) 3. The communication to the data subject referred to in paragraph 1 is not required, if any of the following conditions are met: a) the data controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to those affected by the breach of personal data, in particular measures that make the personal data unintelligible to those not authorized to access it, such as encryption, b) the controller has subsequently taken measures that ensure that it is no longer likely to occur as referred to in paragraph 1 high risk to the rights and freedoms of data subjects, c) requires disproportionate efforts. In this case, a public announcement is made instead or there is a similar measure by which the data subjects are informed in an equally effective way (…)". In addition, OE 29 of article 29 in the Guidelines on the notification of personal data breaches under Regulation 2016/679, taking into account recital 86 of the GDPR underlines, among other things, that: "Controllers should remember that notification to the supervisory authority is mandatory, unless it is unlikely that a risk to the rights and freedoms of persons will be created as a result of the breach. In addition, when persons' rights and freedoms may be put at high risk as a result of a breach, persons must also be informed. The threshold for reporting a breach to persons is therefore higher than for notification to supervisory authorities and, consequently, not all breaches will require notification to persons, which protects them from unnecessary burden fatigue notifications. 21. In this case, regardless of whether the cases under consideration occur in the case under consideration. a' and/or b' of par. 3 of article 34 GDPR, the Authority considers that, although there was a risk to the rights and freedoms of the complainant, there was no obligation to notify the data subject, A, of the breach, as the actions which the latter could do to prevent the risks caused by the disclosure of his health data in order to protect himself were limited. From the history of the case, it appears that as soon as A was informed about the transmission of the medical certificate in question, he submitted his request from ... to the Independent Support Department of the Ministry of Internal Affairs of AADE in order to be informed about the processing of his personal data, and after the relevant response he received, the only possibility left to him was to exercise the right of erasure, as well as to submit a complaint to the Authority. 22. The Authority, taking into account the above, judges that for the established failure

to notify the incident of violation to the Authority, according to article 33 GDPR, based on the circumstances established, it must be imposed, pursuant to the provision of article 58 par. 2 pcs. i GDPR, effective, proportionate and dissuasive administrative fine according to article 83 GDPR in accordance with the Guidelines "for the application and determination of administrative fines for the purposes of regulation 2016/679" of the working group of article 29. According to evaluation of the data, in order to choose the appropriate and corrective measure, the Authority takes into account that the specific violation concerned the processing of a special category of personal data (health data, article 83 par. 2 letter g) and that it constitutes an isolated case (article 83 par. 2 item a'). 27 23. Because, finally, in accordance with the provisions of article 13 paragraph 1 GDPR, the controller must provide the data subject in fulfillment of the obligation to satisfy the right to information, among other things, the identity and contact details of controller, the contact details of the DPO, the processing purposes and the legal basis for their processing, the recipients of the data. Furthermore, in accordance with the provisions of paragraph 2 of the above article, "In addition to the information referred to in paragraph 1, the data controller provides the data subject with the following information that is necessary to ensure legitimate and transparent processing regarding the data subject: (…) b) the existence of the right to submit a request to the data controller for access and correction or deletion of personal data or restriction of processing concerning the data subject and the right to object to the processing, as well as the right to data portability data (…)". And the concept of transparent information is explained, among other things, in recital 60 GDPR as follows: "The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed. Furthermore, the data subject should be informed whether he is being profiled and what the consequences are. If the personal data is provided by the data subject, the data subject should also be informed of whether he is obliged to provide the personal data and of the consequences when he does not provide said data (…)'. 24. Taking into account the information contained in the immediately preceding considerations of the present and the elements of the entire file of the case, the 28th Authority considers, in this case, that AADE, as the controller, through the answer provided by D.O.Y. X with the no. first ... document, satisfied the right of information exercised by the complainant with his request from ..., in terms of the individual information he requested and in fact on time, that is before the expiration of the one-month period, in accordance with the provisions of article 12 par. 3 GDPR. However, AADE, as the controller, had to ensure legitimate and transparent processing

to provide the data subject with the information that he has the right to exercise the rights of deletion and/or restriction of the processing in question, according to article 13 par. 2 item. II of the GDPR. In this way, the risk caused to the rights and freedoms of the complainant by the illegal processing of the disclosure of his health data would be mitigated, through the transmission of the medical opinion in question to the Association of Workers in D.O.Y. PHI. Consequently, the Authority considers that, based on the circumstances established, it should be imposed, pursuant to the provision of article 58 par. 2 sub. i GDPR, effective, proportionate and dissuasive administrative fine according to article 83 par. 5 item II GDPR, according tothe aforementioned Guidelines “for the implementation and determination
administrative fines for the purposes of Regulation 2016/679" of the group
work of article 29, both to restore compliance, and for
the punishment of illegal behavior, considering that the specific
violation was an isolated case (article 83 par. 2 letter a').

The beginning

FOR THOSE REASONS

a) deems that the reported transmission of the disputed medical opinion with the
under no. first ... document of the D.O.Y. X to the Association of Workers in D.O.Y. F happened
in violation of the provision of article 5 par. 1 item 1 GDPR, and imposes on
AADE, as controller, administrative fine of two thousand (2,000)
euro,

b) gives an order, pursuant to article 58 par. 2 item. 4 GDPR, in the AADE, as
controller to delete the no. first ... document issued
from D.O.Y. X, in which in violation of the principle of article 5 par. 1 item c
GDPR, the complainant's condition was listed,

c) deems that the complained processing constituted a data breach
of a personal nature, in violation of the provisions of the articles
5 par. 1 item f and 32 GDPR, which, pursuant to article 33, had to

notified to the Authority and imposes on AADE, as controller for

failure to notify, an administrative fine of one thousand five hundred

(1,500) euros and

d) deems that the satisfaction of the right to information exercised by A was incomplete,

in violation of the provision of article 13 par. 2 item II GDPR and imposes on

AADE, as controller, administrative fine of one thousand five hundred

(1,500) euros.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou