Athens, 29-12-2021 Prot. No.: 3028 DECISION 55/2021 The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting via video conference on 6-

10-2021, following its extraordinary meeting from 19-07-2021 and the postponement of its meeting from 23-06-2021, in order to examine the case mentioned in the history of the present. Konstantinos Menudakos, President of the Authority, regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, and Charalambos Anthopoulos were present. At the meeting, without the right to vote, the auditors Konstantinos Limniotis and Georgios Roussopoulos, specialist IT scientists, as assistant rapporteurs, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary, attended the meeting, by order of the President. The Authority took into account the following: A report No. C/EIS/4545/01-07-2020 was submitted to the Authority, via e-mail, according to which, during his attempt to submit an application to the platform tourism4all.gov.gr, found a problem of leakage of personal data of third parties. In particular, by entering his credentials (TAXISNET codes), application details of a third party (who has no relation to him) appeared on his screen, which included full name, Tax Identification Number (TIN), Social Security Number (AMKA), postal address, telephone, e-mail address (email), while there were also fields with any information on disability and if care is needed for both the applicant and the spouse. A screenshot has been attached as proof. At 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr due to an email message sent to ... also to the email address tourism4all@mintour.gr which was listed on said platform. The Authority, finding that the platform's personal data protection policy states that "...you can address all your questions or requests regarding the protection of your Personal Data held by the Ministry of Tourism in its capacity as Data Controller as per the above , to the Data Protection Officer of the Ministry of Tourism by sending e-mail: dpo@mintour.gov.gr..." and as no notification of a breach had been submitted, he sent an e-mail to the said address on ..., which, however, after two days, returned as unsubsidized. Furthermore, following a search in the register of Data Protection Officers maintained by the Authority, no communication of contact details of the Data Protection Officer from the aforementioned Ministry was found during the disputed time period, as required in accordance with article 37 par. 1 and 7 of the General Protection Regulation Data (Regulation (EU) 2016/679 - hereinafter, GDPR). Subsequently, the Authority sent the document No. C/EX/4914/15-07-2020 to the Ministry of Tourism, informing about all the above and asking for his opinions on what is described in A's report, specifically asking for clarifications regarding the following issues: 1) What exact actions did he take when he became aware of the incident in question, as well as whether the actions in question have been foreseen in the

context of a more general policy for handling personal data breach incidents, 2) How did he evaluate the said incident incident based on the risks that may arise from it to the affected persons, 3) If a Data Protection Officer has been appointed and if the one referred to in the rights (dpo@mintour.gov.gr) is functional. contact website exercise address and 2 Subsequently, due to not receiving a written response from the Ministry after months have passed, the Authority sent a relevant reminder with document No. C/EXE/534/01-02-2021. Following this, the Ministry responded to the Authority with document No. ... (Authority No.: C/EIS/1080/12-02-2021), in which it states the following: A) The implementation of the digital application for the "Tourism for All" program was developed in collaboration with the Ministry of Digital Governance, which, through the Interoperability Center of the General Secretariat of Public Administration Information Systems (hereafter, GIPSDD), guided the partner company THREENITAS A, which cooperates with the Ministry of Digital Governance .E. for interoperability design and development issues. Because of this, the Department of Strategic Planning of the Ministry, which has undertaken the implementation of the "Tourism for All" program for the year 2020, immediately informed the Ministry of Digital Governance and the GGPSDD supervised by it. In more detail, the above email from A (dated ... and time ...) to the email address tourism4all@mintour.gr was forwarded immediately (at ...), with the indication of extreme urgency and with high importance, to the relevant services involved, namely the General Secretariat of Public Administration Information Systems, in the Ministry of Digital Government, in the contractor company of the Ministry of Digital Government, Threenitas A.E. and internally at the General Directorate of Tourism Policy and the Minister's Office. B) The involved agencies proceeded with immediate technical investigative actions in order to identify the error in the process. In the meantime, with the intervention of the Office of the Minister of Tourism and until the necessary explanations are given, the operation of the application was suspended as a precaution on ... and time ... to avoid similar incidents. C) Subsequently, and as no mistake was detected until time ..., an error in the implementation, i.e. at the level of application by the contracting company, it was proposed to add a second level of control during the authentication of the user through the Interoperability of the GISDSD (oAuth2 service) and specifically 3 confirmation of IBAN1 after entering taxisnet codes. The proposal of the contractor company of the Ministry of Digital Governance was accepted, with the agreement of the Directorate and the Minister's Office and the application returned to normal operation on the same day ... and time ... and the Ministry of Digital Governance undertook the further investigation of the matter in cooperation with the GPSDDD, as the problem appeared to occur during the user authentication phase. The electronic messages exchanged are attached to the Ministry's response to the Authority. Furthermore, the Ministry of Tourism

states in its above response that the online application www.tourism4all.gov.gr, according to the no. 9126/17.06.2020 Public Invitation (ΦΣΠ73465ΧΘΟ-51Θ), opened for the submission of beneficiary applications on … and the incident in question occurred on its second day of operation and indeed within the first 24 hours of its operation (…). For the first time, the Interoperability Center of the GISDSDD received a huge volume of requests, as the potential beneficiaries of the Program, according to AADE data, were approximately 5 million citizens. Throughout the operation of the electronic application, the service of the Ministry of Tourism was in constant communication with the involved services, in order to deal with the problems that arose during the process, as was successfully done - as reported by the Ministry - also in this particular case. In this regard, the Ministry also states that with the no. ... document, the above initial document of the Authority was forwarded to the Ministry of Digital Governance for its assistance by reason of competence. As the response of the relevant services involved (Ministry of Digital Governance and GISPSDD) was pending, on October 27, 2020 an electronic reminder message was sent to the Ministry. Digital Governance. The relevant correspondence, including the Authority's second reminder document, was forwarded again on ... to the Ministry of Digital Governance via email and after a relevant 1 Note: as was said in later documents, but also during the hearing of the Ministry of Tourism before the Authority, no it is the IBAN but the Tax Registration Number (TIN). 4 of telephone communication, as well as the one with no. ... document from the Ministry of Tourism to the Ministry of Digital Governance to provide information. Finally, with regard to the matter of the appointment of a Data Protection Officer and functionality of the electronic address for communication and exercise of rights, which escapes - as stated in the above letter from the Ministry to the Authority - the competences of the General Directorate of Tourism Policy, it is stated that the draft invitation to submit tenders for the assignment of services aimed at the design and development of a Compliance System with the requirements of the General Data Protection Regulation (GDPR) and the provision of Personal Data Protection Officer services is being processed and until the completion of the process the contact address has been replaced at " Terms of Use & Data Protection Policy" of the online application with the email address tourism4all@mintour.gr. Subsequently, the Authority invited the Ministry to a hearing, via video conference of Tourism at the Plenary meeting of 23-06-2021 (see call with prot. no. C/EXE/1344/31-05-2021). One day before the date of the meeting, the Ministry of Tourism submitted by e-mail (authority reference number: Γ/EIS/4112/22-06-2021) its documents numbered ... and ..., with the first of which he lists more detailed information regarding the issues that would be discussed before the Authority, while with the second he requested a postponement of the upcoming discussion. In particular, in the first document the Ministry of Tourism

states the following: A) With the under no. 9022/16.06.2020 Joint Ministerial Decision of the Ministers of Finance, Development and Investments, Tourism and State approved the preparation of a program with the aim of strengthening the demand for domestic tourism "Tourism for all" in 2020 through the holiday subsidy (B' 2393). According to paragraph 1 of article 7 of the aforementioned joint ministerial decision, an application is required for inclusion in the program, which is submitted by the beneficiaries to the electronic application of the Ministry of Tourism www.tourism4all.gov.gr through the Unified Digital Portal of the Public Administration. 5 of the application is available through submission, In order to submit the application, the prior authentication of the beneficiaries using the codes - credentials of the General Secretariat of Public Administration Information Systems of the Ministry of Digital Governance (taxisnet) is required. According to paragraph 3 of the same article, according to the electronic Interoperability Center of the General Secretariat of Public Administration Information Systems of the Ministry of Digital Governance online services, in order to draw from the information systems of A.A.D.E., the U. D.I.K.A. S.A. and the Civil Registry of the Ministry of the Interior, and granting to the Ministry of Tourism, the following personal data of the applicant: a) from the information systems of A.A.D.E.: i. Indication of a cleared tax return for the tax year audited in terms of the income criterion (0 or 1), ii. Indication of a cleared tax return for the tax year preceding the tax year of the above case i (0 or 1), iii. Income according to the provisions of the above K.Y.A. for the TIN of the applicant and any remaining members of his family and b) from the "AMKA-EMAES" information systems of H.D.I.K.A. S.A. and the Civil Registry of the Ministry of the Interior: i. Current marital status based on the details of the applicant and the spouse or other party to the cohabitation agreement, if any ii. Confirmation of the list of minor dependent children of the applicant. Finally, in article 14 of the above K.Y.A. it is stated that the production operation of the above online services starts following the approval of the General Secretary of Public Administration Information Systems of the Ministry of Digital Governance, in accordance with article 47 of Law 4623/2019 (A´ 134), while the availability is carried out through the Interoperability Center (hereinafter KED) of the General Secretariat of Public Administration Information Systems and in accordance with the current Information Systems Security Framework of the General Secretariat of Public Administration Information Systems of the Ministry of Digital 6 Governance and with the provisions on the protection of personal data. B) The submission of applications started at 21:30 on ..., and was scheduled according to the last number of the applicants' VAT number. The e-mail of A (... - ... from the e-mail address: ...) with the subject: "Leakage of information on the platform tourism4all.gov.gr" was shared at the e-mail address tourism4all@mintour.gr created exclusively for the immediate management of any kind communication regarding the TOURISM FOR ALL YEARS

2020 program. The message was addressed to the email address: complaints@dpa.gr and another notification to another email address (which is said to be that of the affected person). Although, as the Ministry claims, the authenticity of the message could not be verified, it was nevertheless investigated as a real incident, while the Ministry notes that A did not gain access to the other person's tax information but to his application information to the program in question . Since the implementation of the digital application for the "Tourism for All" program was developed in collaboration with the Ministry of Digital Governance, which guided the Ministry of Tourism in the planning and development of interoperability of services through the Interoperability Center of the GGPSDD, the Ministry of Digital Governance referred to the cooperating contractor company THREENITAS S.A. Therefore, the Directorate of Strategic Planning immediately informed the GISPSDD supervised by it about the incident in question, in relation to which the sequence of actions is described in the above Ministry document. In particular, the actions that took place are summarized as follows: of the Ministry of Digital Governance and ..., ... p.m. - Incoming reference message from … (A) to tourism4all@mintour.gr …, … p.m. - Outgoing message reporting the incident to GIS, Ministry of Digital Governance, Contractor, Directorate, General Directorate of Tourism Policy of the Ministry of Tourism, Office of the Minister of Tourism 7 ..., ... p.m. - Question from the contractor to GIS about the exact time when authentication requests were made to the Auth2 service of the two TINs which, from the registration in the application, appear to have created requests with a difference of 10 minutes ..., ... p.m. - An order was given to shut down the application from the Minister's Office until the resolution of ..., ... pm. - Locking of the application by the contracting company until the relevant communication is completed. ..., ... p.m. - GIS response regarding the times when the authentication requests were made to the Auth2 service of the two TINs ..., ... p.m. - Request from the Service to locate the IP addresses ..., ...pm. - Contractor's response that no error has been identified in the implementation and efforts to identify the error with all involved are ongoing. Proposal to adopt double verification of VAT number when entering the application. ..., ... p.m. - GPS response regarding IP addresses (detailed information is given in the Ministry's document). ..., ... p.m. - Request to open the application by the service by order of the Office of the Minister of Tourism in accordance with the proposal for a double check of VAT number made by the contractor. Furthermore, according to the relevant report dated 18.06.2021 (A.P. 10906/22.06.2021) of Mr. B, Data Protection Officer (DPO) of the contracting company THREENITAS A.E.2 (which was submitted to the Authority together with the said document of the Ministry of Tourism), the first phase of the response was aimed at evaluating the extent and seriousness of the incident. “In terms of extent: It was determined that the incident could not be reproduced in the normal flow of application usage. An

analysis of the logs did not identify any other case, other than the one that led to the relevant report." In detail, the DPO of the contracting company records the following: "Information was received that 2 It should be noted that the company has not announced to the Authority the details of a Data Protection Officer based on article 37 paragraph 7 of the GDPR. 8 had been requested by the KED regarding the use of the TaxisNet Login service, and data was retrieved from the platform's logging system. A series of extensive checks were performed on the application code, and all supported scenarios were confirmed to be handled correctly. No problem was found in the implementation and the event could not be reproduced. Therefore, any possibility that the incident was due to an implementation error related to the digital platform was ruled out. Then, elements related to the implementation of OAuth2.0, on which the GIS TaxisNet Login service is based, as well as the service infrastructure of the application, were examined. However, the implementation of OAuth2.0 was used as it is by a related software library, on which other service implementations of HDIKA have been based, and the service infrastructure is provided by the Amazon Web Services service, and makes use of elements that allow the support of a large volume of incoming requests, such as load balancer and multiple server instances. In any case, both possibilities concern functions and systems that are outside the control of the company and the Ministry of Tourism, and could not be further analyzed. The above findings were also reported to the KED in order to carry out a parallel check on the infrastructure that supports the authentication mechanism, but without mentioning any technical problem. It is noted that only during ... the tourism4all digital platform was visited by approximately 80,000 users, who performed 1,200,000 content views. However, apart from the incident reported by this user, no other similar incident could be found in the other 1,200,000 content views." Furthermore, as already mentioned above, an improvement proposal of the contractor company was implemented, i.e. the addition of a second level of control during authentication of the user through the Interoperability of the GISDSDD (oAuth2 service) and specifically confirmation of the VAT number after entering the taxisnet codes. In other words, the citizen is asked to enter his tax identification number as this element is also part of the authentication. According to the proposed extension, the TIN entered by the user is compared with the TIN returned during TaxisNet Login. In the information retrieved by 9 if the two differ, the user is logged out in order to try to log in again. The proposal of the contractor company of the Ministry of Digital Government was accepted, with the concurrence of the Directorate of Strategic Planning and the Office of the Minister of Tourism and the application returned to normal operation on the same day ... and time ... while the Ministry of Digital Government undertook the further investigation of the matter in collaboration with the GISDSDD, as the problem appeared to have arisen in the user authentication phase and in

any case did not concern the competences of the Ministry of Tourism due to its technical nature. As the Ministry of Tourism also mentions in its document, according to data from AADE, the potential beneficiaries of the Program were approximately 5 million citizens, a fact about which both the contractor and the GGPSDD had been informed by the Ministry of Tourism (e-mail...) in order to take all the necessary measures at a technical level due to competence. In fact, the Interoperability Center of the GISDSDD received a huge volume of calls and throughout the entire period of operation of the electronic application, the Service was in constant communication both with the K.E.D. of the PGPSDD as well as the contracting company, in order to deal with the problems that arose during the process and to ensure the smooth operation of the application when submitting the applications. C) The contractual framework for the cooperation of the Ministry of Tourism with those involved bodies mentioned above, namely with the Ministry of Digital Governance, with the General Secretariat of Public Administration Information Systems, with the contractor THREENITAS S.A. and the contracting authority EDYTE S.A., a supervised entity of the Ministry of Digital Governance, was formed as follows: 1) With the Memorandum of Cooperation of the Ministry of Digital Governance with the Ministry of Tourism dated 01.09.2020 (attached to the aforementioned document of the Ministry of Tourism to Authority), which was forwarded to the Office of the Minister of Tourism for signature on 11.11.2020 (A.P. Secretary of the Minister … /…) it is specified that the subject of the contract, i.e. the creation of an electronic application/platform for the provision of e-vouchers in the context of the 2020 program 10 "Tourism for all", through the Unified Digital Portal of the Public Administration, is carried out by the Ministry of Digital Governance, which develops the technical and regulatory framework for its creation in accordance with the guidelines of the Ministry of Tourism, which prepares the program. From the date of delivery of the above application/platform, the Ministry of Digital Governance no longer participates in its management and operation nor is it responsible for the processing of personal data, which is carried out in the context of managing the electronic application/platform, while the Ministry of Tourism undertakes its general management, acquires the information contained therein and is responsible for its management, maintenance and updating. Furthermore, the Ministry of Tourism is the person responsible for processing the personal data of the platform, whose technical analysis, design and implementation will be carried out by EDYTE SA, a supervised body of the Ministry of Digital Governance. With the signing of the Memorandum, the Ministry of Digital Governance hands over all the data and information related to the website for all", "tourism4all.gov.gr" and the online platform "tourism4all". 2) The with no. 10183/14.09.2020 Contract regarding the "Creation of a platform for the provision of e-vouchers within the framework of the "Tourism for All" program between the Contracting

Authority EDYTE S.A. and the contractor THRINITAS SOFTWARE SYSTEMS SA. (pp. THREENITAS) (attached to the above document of the Ministry of Tourism to the Authority), has as its object the technical analysis, design and implementation of the platform for the provision of evouchers within the framework of the "Tourism for All" program for productive operation through of gov.gr. Also, it is stated that "The connection is made through the TAXISnet codes with the parallel declaration of the AMKA. The application interfaces with WebServices provided by the KEP of the GIPSDD to meet the needs of retrieving VAT numbers and user details, confirmation of parent/child relationship between the beneficiary and the members declared as such, confirmation of partner/spouse relationship between the beneficiary and the member declared as such, income recovery" and the WebServices that support the execution of the "Tourism on 11 checks" program are listed: "User Authentication, parent/child relationship check using AMKA, spouse/partner relationship check using AMKA, Income, IBAN /VAT NUMBER". With reference to the protection of personal data, in this contract it is stated that "the processing of personal data will be carried out in accordance with the terms and agreements of this Contract and the Instructions of the Contracting Authority. The Contractor undertakes to implement and comply with the applicable legislation for the protection of personal data (…)" and "The Contractor assures and guarantees to the Contracting Authority that it will take all necessary organizational and technical measures for the security of information that may to contain personal data, and in general all similar forms of files and IT of the Contracting Authority, as well as to protect them from accidental or unlawful destruction, accidental loss, alteration, prohibited dissemination and any other form of unlawful processing, in the context of its duties stemming from the present". 3) By the 12.11.2020 Appendix C' "Data Processing Agreement-DPA", which was attached to no. 10183/14.09.2020 Agreement (also attached to the above document of the Authority), it is stipulated that the Ministry of Tourism is the data controller and processes personal data in the context of the "Tourism for All" program, as well as that the executive-EDYTE A .E. processes personal data on behalf of and in accordance with the orders of the person in charge (Ministry of Tourism) within the framework of the platform for productive operation through gov.gr. The subcontractor (Contractor - Threenitas) must: a) provide its assistance to EDYTE SA and through it to the Ministry of Tourism, regarding ensuring its compliance with its obligations arising from the GDPR and the Law, regarding the exercise of the rights of the data subjects, b) to inform in writing and without culpable delay EDYTE SA, and it in turn the Ministry of Tourism, of any question, complaint, complaint or request that may be received and related to the exercise of the rights of the data subjects, c) to support EDYTE SA, in order to provide the person in charge with the assistance of 12 the provision for carrying out an impact/impact assessment study of the

processing of personal data, if this becomes necessary based on the data processing procedures of a personal nature and in accordance with the terms of the GDPR and the Law d) to provide through EDYTE SA to the Ministry of Tourism the assistance t of the consultation with the Data Protection Authority regarding the proposed and appropriate risk mitigation measures in cases where the impact assessment study indicates that the processing would cause a high risk to the rights and freedoms of the data subjects. Finally, the subcontractor (Contractor - Threenitas) is obliged: "to take all appropriate technical and organizational measures (...) in order to ensure the corresponding level of security against risks and specifically to ensure the confidentiality, integrity and availability of the processing and services on an ongoing basis (…) is generally obliged to apply appropriate measures for general services: encryption, authorized access, classified access, keeping logs, keeping backup copies, strong password for entering the systems and changing it regularly, deactivating the operation of storage media, enable firewall on computer and secure remote connection only via VPN'. 4) With no. 554/26.01.2021 contract regarding the "Expansion of the platform for the provision of e-vouchers within the framework of the "Tourism for All" program - Phase B" between the Contracting Authority EDYTE S.A. and the contractor THRINITAS SOFTWARE SYSTEMS SA. (attached to the above document of the Authority) the scope of the contract is expanded, while the content of its terms remained as it was. Directorate of Strategic Planning which prepares the Program, the Ministry of Tourism reports that after its publication with no. 5979/07.04.2021 call for tenders for the assignment of services for the design and development of a Compliance System with the Requirements of the General Data Protection Regulation (GDPR) and the provision of 13 services of a Personal Data Protection Officer (AD: 631T465XYO-Θ93)3 and the relevant tender procedure, was issued with no. 10398/14.06.2021 Decision of the Official Secretary of the Ministry of Tourism on the acceptance of 14.5.2021 (Meetings 26.4.2021 and 10.5.2021), 1.6.2021 (Meetings 28.5.2021 and 1.6.2021) and 9.6.2021 (Meeting 19.6.2021) of the tender evaluation committee's minutes no. 5979/07.04.2021 of invitation (AD: 93H9465XTHO-0MN). Therefore, the signing of a contract with an external partner-contractor of the Ministry of Tourism, who will provide the services of a Personal Data Protection Officer4, is imminent. It should be noted that, according to the above invitation, as found by the Authority following its examination by "Diavgeia" where it has been posted, the budgeted expenditure amounts to the amount of €20,000.00 excluding VAT (VAT: €4,800.00, total amount of €24,800.00) and will be borne by the Ministry's budget for financial years 2021 and 2022. Regarding the issue of the functionality of the electronic communication and exercise of rights address that appeared on the Program's website, the address in question has been replaced, until the completion of the contract award

process in the "Terms of Use & Data Protection Policy" of the online application with the email address tourism4all@mintour.gr. D) In conclusion, the Ministry of Tourism states that it considers the contribution of the bodies directly involved in the technical development of the application to be critical, namely the EDYTE, the General Secretariat of Public Administration Information Systems and the Ministry of Digital Governance, noting in fact that from the Ministry of Digital Governance and the GIPSDD has not received their written response regarding the management of the incident until 22-6-2021. It also mentions that the application was designed by the Ministry of Digital Governance and has a productive function through gov.gr (the 3 Budget 24,800 euros 4 As can be seen from the Ministry's document no. prot. 10398/14-06-2021 (AD: 93H9465XTHO-0MN) for the provision of the service the company INTERACTIVE O.E. was selected with a bid amount of €21,948.00 (including VAT) 14 technical analysis, the design and implementation of the platform was assigned to EDYTE SA and from that to an external partner - Contractor/Threenitas), while the Services of the Ministry of Tourism were not fully aware of the terms of cooperation and when this took place the application was already in full operation. It also recapitulates by stating again that the Ministry of Tourism is the data processor of the platform, but its involvement cannot be of a technical nature, while ensuring the proper functioning of the platform and taking all necessary personal data security measures is an obligation of the Contractor. Finally, the incident in question was isolated, dealt with immediately, however personal data was not widely known/exposed, so that the risk is assessed as high and combined with the uniqueness and absolutely limited extent of the incident and the impossibility of verification and fault finding , it was assessed that the affected person was not endangered. Therefore, according to the claims of the Ministry of Tourism, it is not possible to consider that the provisions of articles 33 and 34 of the General Data Protection Regulation regarding personal data breaches were violated. During the meeting of 06-23-2021, C, Legal Advisor, NSC Office, D, Paredros, NSC Office, E, Advisor to the Minister's Office, F, ... Tourism Policy, G, ... Strategic Planning, H , ... of the Department of Special Forms of Tourism and Th, an employee of the Department of Special Forms of Tourism, as representatives of the data controller, who also verbally submitted the request to postpone the discussion, which was accepted, with a new date for the discussion of the case being set on 19-7 -2021. The meeting of 19-7-2021 was attended, via video conference, by D, Paredros, NSK Office, E, Advisor to the Minister's Office, F, ... Tourism Policy, Z, ... Strategic Planning, T, employee of the Department of Special Forms of Tourism, H , ... Department of Special Forms of Tourism, as well as I and K on behalf of the contracting company that has undertaken the provision of Personal Data Protection Officer services to the Ministry of Tourism, as representatives of the 15 controller. After the meeting,

the data controller was given a deadline to submit a memorandum, which he submitted, within the set deadline, with document No. C/EIS/5104/02-08-2021. Already, before the submission of the memorandum of the Ministry of Tourism, an information note was submitted to the Authority by the GISDSDD of the Ministry of Digital Governance (No. prot. of the Authority: C/EIS/4794/20-07-2021), which, after describing again the relevant provisions of no. 9022/16.06.2020 K.Y.A., mentions the actions taken by the GHPSDD regarding the incident in question, specifically mentioning the following: a) The GHPSDD received information about the incident from the Ministry of Tourism by email on ... and time …. In connection with the mentioned incident, her assistance was requested. b) The PGPSDD proceeded to check the online service and did not find any problem in its operation and in the authentication infrastructure. Additionally check the related logs in detail. c) On the same day and time, the GISDSDD sent by e-mail the relevant logs that are kept at the Interoperability Center and related to references to calls to oAuth 2.0. d) During the first days of operation of the platform, the KE.D. /GPSDD informed the Ministry of Tourism with statistics on the use of online services to monitor the action. e) The KED's oAuth 2.0 authentication service is widespread and used in a number of electronic services of public bodies. oAuth 2.0 calls within 2020 amounted to 54,185,731, while in the first half of 2021, 86,396,905 calls have already been made, without any malfunction reported or detected in this mechanism. Furthermore, the GDPR states that in order for a web application to utilize multiple simultaneous users, the application needs to have control over the sessions that are created, so that ultimately each user is served with the functionality and data that concern them. It is noted that the calls 16 of oAuth2.0 and web services to the KE.D. as well as their responses, are controlled by the respective application that calls them. The separation of information for each distinct natural person must be carried out through the distinct management of session ids by the Web Application ("Tourism for All"). As for the further investigation of the matter, beyond issues exclusively under the competence of the KED, the PGPSDD is considered incompetent. In the aforementioned memorandum of the Ministry of Tourism, which was submitted after its hearing before the Authority, the description of the procedures followed to deal with the incident (as they had already been described in previous documents of the Ministry) is repeated, the content of the above information is attached note of the GISPSDD, while also repeating the content of the report of the Contractor's DPO (Threenitas). Furthermore, the Ministry of Tourism reports that, after its hearing before the Authority, it requested further clarifications from the contracting company, which with the no. ... (A.P. of the Ministry of Tourism) its letter (attached to the Ministry's memorandum to the Authority) clarifies: "The "Tourism for All" application uses a library based on the official Microsoft library to interface with OAuth2 providers, such as GSIS

Authentication service. The library uses without modification the methods provided by Microsoft for managing multiple sessions. In the case under consideration, where another user's credentials were observed to appear, the issue was traced to the fact that the credentials returned by the GSIS to the infrastructure after authentication redirection, were for a user other than the one for whom the authentication process was done. The authentication process and session management, i.e. the management of the sessions created in the context of the relevant user service requests, was performed exclusively using the methods provided by the library in question. Given that: a) the mechanism for managing multiple connections is made using Microsoft libraries, which does not justify questioning their correctness b) its operation was confirmed by running tests, as well as in conditions of artificial 17load, when these were applied on the server that hosts the application, c) worked in general without problems during the high load conditions observed in all the subsequent phases of the system's operation, we consider as the only possible possibility that the specific issue is created by mismanagement in any of the intermediate network infrastructures between the application and the KED. These infrastructures are not under the control of Threenitas and the Ministry of Tourism, and are used as they are. It is indicated that the infrastructure used the Application Load Balancer and Web Application Firewall services, as provided by Amazon Cloud, which could under certain circumstances lead to the incorrect management of the multiple active connections to the KED infrastructures. As mentioned in our report from 06/18/2021, after confirming the correct operation of the application, and after introducing additional checks to deal with the observed phenomenon, in order to prevent the possibility of malfunction even due to events that are not under our control checking the app, the problem was fixed and not seen again." Furthermore, from the electronic mail that took place on the day of the incident, it appears that the User with ATMHYYYYY... (L) made two (2) connections, specifically on ... ... MM (...) and ... ... MM from the same IP address ..., and the User with TIN YYYYMMDD... (A) also in two (2) connections on ... ... MM and on ... ... MM, from two different IP addresses, on ... and ... and the Ministry of Tourism assumes that during the first connection the application was submitted and in the second one an attempt was made to recover it, whenever the incident of recovery of the other user's request was observed. The reason why the incident was not reported to the Authority, in accordance with Article 33 of the GDPR, is that: a) The report had been made directly to the Data Protection Authority by the citizen (A) with notification to the affected person, who did not did not take any action, b) The controller took actions and took appropriate measures by introducing an additional level of security during the login and identification of users, which ensured that such an incident does not occur again. The incident was assessed as minor and the risk negligible to non-existent, i.e. there is no

possibility of causing a risk to the rights and freedoms of natural persons. In its memorandum the Ministry also states that since a) the implementation of the digital application for the "Tourism for All" program was developed in collaboration with the Ministry of Digital Governance, which guided the Ministry of Tourism in the design and development of interoperability of services through of the Interoperability Center of the GISDSD and the contracting company THREENITAS S.A., which cooperates with the Ministry of Digital Governance. and b) on ... the project had not been contracted, which proceeded as an emergency due to the pandemic in order to strengthen domestic tourism and support the domestic tourism market with the direct cooperation of the Offices of the two Ministers (Tourism and of Digital Governance), the Department of Strategic Planning of the Ministry of Tourism immediately informed the Ministry of Digital Governance and the GISPSDD supervised by it about the incident in question as mentioned. The Ministry of Tourism was not aware of the terms of the contract with the contracting company. For the above reasons it was also considered - wrongly - that the e-mail address dpo@mintour.gov.gr included in the terms of use of the application was an e-mail address that would be operated by the Ministry of Digital Governance and that it would not be managed by the Ministry of Tourism . After all, as mentioned in the Memorandum of Cooperation, the content of the platform was designed according to the instructions of the Ministry of Tourism, which had never provided this e-mail address for the Program, but only its own e-mail address tourism4all@mintour. Gr. Besides, all the e-mail addresses of the Ministry of Tourism are of the form xxxxxxx@mintour.gr without including the word gov and on the part of the Ministry this e-mail address was created on 16.06.2020 in order to receive questions/complaints/complaints etc. Pi. regarding the Program. The said complaint was also sent to this electronic address and there was an immediate reaction, as described in all the Ministry's documents to the Authority. Finally, the Ministry of Tourism states that with the no. 23/2021 (ADMA: 19 21SYMV008841946 2021-06-30) contract assigned the provision of Personal Data Protection Officer services to the company Interactive OE and submitted the no. ... notification to the Data Protection Authority (DPA) for the appointment of the Data Protection Officer. Therefore, the Ministry of Tourism has already appointed a Data Protection Officer. On 16.07.2021, the Terms of Use and Data Protection Policy of the application www.tourism4all.gov.gr were updated with the electronic contact address of the Ministry of Foreign Affairs, i.e.: dpo@mintour.gr. The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteurs, who (assistants) left after the discussion of the case and before the conference, after a thorough discussion OLD IN ACCORDANCE WITH THE LAW 1. According with the provisions of articles 51 and 55 of the General Data Protection Regulation (EU) 2016/679 (hereinafter, GDPR) and article 9 of Law 4624/2019

(Government Gazette A

137), the Authority has the authority to supervise the implementation of provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 2. According to article 4 par. 7 of the GDPR, a data controller is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of personal data processing; when the purposes and way of this processing are determined by the law of the Union or the law of a member state, the controller or the special criteria for his appointment may be provided by the law of the Union or the law of a member state", while in the same article para. 8 is defined as the processor "the natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller". 20 3. The same article defines a personal data breach as "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed" . 4. According to article 5 paragraph 2 of the GDPR, the data controller bears the responsibility and must be able to prove his compliance with the processing principles established in paragraph 1 of the same article, which include legality, objectivity and transparency of the processing in accordance with article 5 par. 1 item a', and the confidentiality and integrity of the data in accordance with article 5 par. 1 item at. As can be seen from this provision, with the GDPR a compliance model was adopted with a central pillar being the principle of accountability in question, according to which the data controller is obliged to plan, implement and generally take the necessary measures and policies, in order for the processing of data to be in accordance with the relevant legislative provisions and, in addition, he must prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 5. With reference to the principle of processing transparency, the GDPR imposes specific obligations on data controllers regarding the information they must provide to data subjects. In particular, in accordance with Article 12 para. 1 of the GDPR, the data controller takes the appropriate measures to provide the data subject with any information referred to, among others, in Article 13 - which states that "when personal data concerning a subject of the data are collected from the data subject, the data controller, when receiving the personal data, provides the data subject with all of the following information: a) the identity and contact details of the data controller and, where applicable, of his representative controller, b) the contact details of the data protection controller, as the case may be, c) the processing purposes for which the personal data are intended, as well as the 21 legal basis for the processing, (…)" (see par. 1 of Article

13 of the GDPR). Furthermore, in paragraph 2 of article 12 of the GDPR it is provided that "the controller facilitates the exercise of the rights of the data subjects (…)" 6. In article 28 paragraph 2 of the GDPR, regarding the processors, it is provided that " the processor does not engage another processor without the prior specific or general written permission of the person in charge processing. In the case of general written consent, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby providing the controller with the possibility to object to these changes.' Furthermore, in paragraph 3 of the same article, it is provided that the processing by the processor is governed by a contract or other legal act subject to the law of the Union or the Member State, which binds the processor in relation to the controller and determines the object and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller. Furthermore, in paragraph 4 of the same article it is defined: "When the processor hires another processor to carry out specific processing activities on behalf of the controller, the same obligations regarding data protection provided for in the contract or other legal act between controller and processor, as provided in paragraph 3, are imposed on the other by means of a contract or other legal act in accordance with the law of the Union or the Member State, in particular to provide sufficient assurances for the application of appropriate technical and organizational measures , so that the processing meets the requirements of this regulation". And in paragraph 9 of the same article it is clearly stated that "the contract or other legal act referred to in paragraphs 3 and 4 exists in writing, including in electronic form". 22 7. Pursuant to Article 24 para. 1 of the GDPR, the controller, taking into account 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, implements appropriate technical and organizational measures in order to ensure and be able to prove that the processing is carried out in accordance with the GDPR, and said measures must be reviewed and updated when deemed necessary. Furthermore, according to Article 32 of the GDPR, "taking into account the latest developments, the costs 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 liberties of natural persons, the controller and the processor implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks, including, among others, as appropriate: (…) d) procedure for regular testing, assessment and assessment of the effectiveness of technical and organizational measures to ensure the security of processing'. Furthermore, in paragraph 2 thereof, it is provided that "when assessing the appropriate level of security, the risks

deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed'. 8. In relation to personal data breaches, the GDPR imposes specific obligations on data controllers. Specifically, in article 33 thereof, it is defined that in the event of a personal data breach, the data controller shall notify the competent supervisory authority without delay and, if possible, within 72 hours of becoming aware of the personal data breach5, except if the breach of personal data does not 5 Taking into account Article 55 of the GDPR on the competences of the supervisory authorities, the Authority for the Protection of Personal Data 23 is responsible for the incident in question may 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. Paragraph 3 of article 33 defines the information that must be contained as a minimum in such a notification, which includes - among others - "b) ... the name and contact details of the data protection officer or other contact point from which they can to obtain more information, c) ... the potential consequences of the personal data breach, d) ... the measures taken or proposed to be taken by the data controller to deal with the personal data breach, as well as, where appropriate, measures to mitigate its possible adverse consequences." In the event that it is not possible to provide the information at once, it may be provided gradually without undue delay. Furthermore, in accordance with Article 34 of the GDPR, when a personal data breach may place the rights and freedoms of natural persons at high risk, the controller shall promptly notify the data subject of the personal data breach. This notification clearly describes the nature of the personal data breach and contains at least the information and measures referred to in Article 33(3)(b), (c) and (d). Notification to the data subject is not required if one of the conditions described in this paragraph is met. 9. According to article 37 par. 1 of the GDPR, "the data controller and the processor appoint a data protection officer in every case in which: a) the processing is carried out by a public authority or body (…)". Furthermore, in paragraph 7 of the same article, it is stated that the data controller or processor publishes the contact details of the data protection officer and communicates them to the supervisory authority. 24 Besides, as mentioned above, contact details of the data protection officer must also be made available to the data subjects. With reference to the role of the data protection officer, it is pointed out that, among other things, as provided for in article 38 paragraph 4 of the GDPR, "data subjects can contact the data protection officer for any issue related to the processing of their personal data character and with the exercise of their rights (...)". 10. In this particular case, the Ministry of Tourism is responsible for processing, within the meaning of article 4 par. 7 of the GDPR, for the processing of personal data which takes place within the framework of the

"tourism4all" platform, in accordance with what is stated in the above Ministry documents and based on the relevant information provided by the platform. This does not follow from the Joint Ministerial Decision No. 9022/2020 "Tourism for all" program of the year 2020" (Government Gazette B

2393). In particular, in article 1 par. 2 of K.Y.A. under no. 9022/16.06.2020 as amended by the no. 12181/31-07-2020 K.Y.A. (Government Gazette B' 3155), it is provided that "For inclusion in the program an application is required, which is submitted by the beneficiaries to the online application of the Ministry of Tourism www. tourism4all.gov.gr through the Unified Digital Portal of the Public Administration" while in article 7 par. 4 of the same GPA it is provided that "By submitting the application for participation, consent is provided to the Ministry of Tourism for the processing of the above personal data of the applicant and of its beneficial members, exclusively for the purposes of inclusion in the present Program. The above data is kept by the Ministry of Tourism for two (2) years from the issuance of the Final Register of Beneficiaries and the Final List of Excluded and in any case until the completion of the program". Therefore, despite the incorrect reference to consent (which cannot be used as a legal basis for processing personal data for the fulfillment of a task performed in the public interest or in the exercise of a public authority delegated to the controller) it becomes clear that intention of the legislator is to make the Ministry of Tourism responsible for processing. 25 11. The Ministry of Digital Governance, through the PGPSDD, is in charge of the processing for the implementation and operation of the platform, since in article 7 of the above C.Y.A. it is defined that, "for inclusion in the Program, an application is required, which is submitted by the beneficiaries to the electronic application of the Ministry of Tourism www.tourism4all.gov.gr through the Unified Digital Portal of the Public Administration. To submit the application, prior authentication is required (identity verification) of beneficiaries using the credential codes of the General Secretariat of Information Systems of Public Administration of the Ministry of Digital Governance (taxisnet)" and that "During the online submission of the application, online services are available through the Interoperability Center of the General Secretariat of Public Administration Information Systems of the Ministry of Digital Governance, in order to retrieve and grant to the Ministry of Tourism, from the information systems of A.A.D.E., H.D.I.K.A. S.A. and the Civil Registry of the Ministry of the Interior, (…) personal data of the applicant (…)". And the company THREENITAS S.A., a contracting company, collaborating with the Ministry of Digital Governance for the aforementioned processing, is also the processor (and since it has a contract with processors, it is essentially a sub-processor, as described in article 28 para. 2 of the GDPR). Furthermore, this conclusion also

follows from the actual facts, as it appears from the file of the case, even in the initial period in which there was no contract and no written assignment of the processing, the application was implemented in the manner described above. Furthermore, as appears from the documents submitted by the controller to the Authority, EDYTE SA, a supervised body of the Ministry of Digital Governance, is also the processor. 12. In relation to the data breach incident under consideration, it appears that there were immediate actions by the data controller to investigate and deal with it. It is noted that for technical security issues of the processing, it appears that the relevant authority lies with the processors, i.e. the Ministry of Digital Governance with regard to section 26 in particular of user authentication and THREENITAS S.A. regarding the implementation of the platform for the provision of evouchers within the framework of the program – therefore, the action of the data controller to immediately report to the Ministry of Digital Governance, but also to temporarily stop the operation of the platform, is considered correct. Also, the additional security measure implemented to deal with it, as proposed by THREENITAS S.A. (ie the use of a second factor of authentication) is in the right direction, although it is not related to the root cause of the incident - which indeed could not be determined. The issues raised regarding the said incident of infringement are the following: A) For the said processing there was no contract or other legal act during the period when the said incident took place. Specifically, there was no contract between the Ministry of Digital Governance (executing the processing) and THREENITAS S.A. (sub-executor of the processing), since it was signed in September 2020, while it does not appear that the (even general) permission of the Ministry of Tourism, as data controller, was requested for the assignment in question (although it appears that the data controller was aware of the assignment in question). Furthermore, the memorandum of cooperation between the Ministry of Tourism, responsible for the Ministry of Digital Governance, performing the processing, in which the role of EDYTE SA is also defined, was also drawn up in September 2020, i.e. after the said processing had started and after the breach in question. As the data controller states, the said delay is due to the fact that it was urgent to start said processing, due to the pandemic and with the aim of strengthening domestic tourism and supporting the domestic tourism market (a purpose that is clearly in the public interest). However, the unwritten contract or other legal act, in addition to being a violation of article 28 par. 9 of the GDPR6, does not allow the definition of a processing, and 6 See also the Guidelines 7/2020 of the European Data Protection Board on the concepts of controller and processor, which clearly states: "(...) non-written agreements (regardless of how thorough or effective they 27 clear procedure for the dealing with incidents of infringement, with a clear distinction and definition of the role and responsibility of each body (both the data controller and the executors). It therefore seems that an "ad hoc" procedure was

followed to deal with the incident, from which the data controller ultimately it was not possible to discover, through the processors, the source of the incident in question: as it appears from the data in the case file, the controller, in addition to the electronic messages exchanged during the first 24 hours from the moment it became known the incident, he requested - after the Authority's documents asking for his opinions - adjournment ero opinions from the Ministry of Digital Governance, without receiving a response. Approximately one year after the incident (i.e. in June 2021), he requested and received a response from the DPO of the contractor Threenitas, according to which there was no extent to the incident while the specific error was not possible to reproduce, and finally, the opinions of the General Directorate of Public Safety of the Ministry of Digital Governance were sent after the hearing of the data controller before the Authority, while also after the hearing the views of THREENITAS were again requested and received. In any case, only guesses are made as to the root cause of the incident, which relates in particular to the possibility of a bug in the off-the-shelf software libraries used, without clearly identifying its cause. The above constitute a violation of the fundamental conditions for taking appropriate organizational and technical measures for the security of processing, in accordance with Article 32 of the GDPR, in conjunction with Article 24, as the data controller did not take into account the risks to rights and freedoms of natural persons to determine security measures. It is also pointed out that the absence of defining the processors leads to increased risks, such as the use of sub-processors who may not meet the requirements of the GDPR, or appropriate measures have not been taken for the use are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR" https://edpb.europa.eu/system/files/2021-(available 07/eppb_guidelines_202007_controllerprocessor_final_en.pdf) online link to 28 of them. Of particular note is the reference to the use of Amazon's "cloud" services, which may mean that there has been a transfer of personal data outside the EU. In any case, the use of said cloud adds another processor in the activity in question for which, given that the Amazon company appears to belong to a group of companies subject to US law, an analysis should have been carried out in relation to its legality and based on what is understood in recommendations 01/2020 of the ESPD7, while the Ministry of Tourism, as controller, did not demonstrate that it was aware of this during the time period when the incident took place since, apart from the absence of contracts, it does not make any relevant reference. B) There was no notification of the incident in question to the Authority as required by article 33 of the GDPR. It is noted that, in accordance with this article, notification is made without delay and, if possible, within 72 hours of becoming aware of the fact, unless the breach of personal data is not likely to cause a risk to the rights and freedoms of the natural persons. Based on the data in the case file, the data controller, with the

knowledge of the data he had within the first 72 hours from the moment he became aware of it, could not consider that there was no risk to affected persons, since he did not have clear picture of the source of the incident, while the incident itself, based on the knowledge of the controller, already involved sharing data, including health data, with third parties. Therefore, the notification should be submitted to the Authority, also taking into account that, according to paragraph 4 of the same article, "in the event that it is not possible to provide the information at once, it can be provided gradually without undue delay". The controller's claims that he did not notify the Authority because, on the one hand, the citizen had already informed the Authority and also the 7 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en 29 affected person without the latter taking any action and on the other hand the controller took immediately in actions to deal with it do not establish a reason to exempt the data controller from the obligation to notify according to article 33. 13. The controller had not appointed a Data Protection Officer againstthe time period the case concerns, in violation of article 37 par. 1
of the GDPR, as the definition of this was made in July 2021 – i.e. after the expiry
three (3) years from the implementation of the GDPR, while the notification process
started in April 2021. Further, despite the lack of definition of DPO, there was
inaccurate information on the website of said platform about existence
DPO with his contact information, which - as the Authority found - no
were valid. The data controller states that the data in question
communication were raised by the processor and considered that
this is an email address corresponding to the performer. THE
but this claim is irrelevant in relation to the issue of whether it occurs
violation of the above provision since, as a data controller, he has at
intact the obligation of full and correct information to its subjects
data, as well as the obligation to facilitate the exercise
of their rights (purpose for which art

due address, in accordance with article 38 par. 4 of the GDPR). In any case,

it does not appear that the controller had made such an assignment to

processors (see also above regarding the lack of documentation

contract or other legal act). Therefore, there was also a violation of

obligations of article 13 of the GDPR regarding the information that

provided to the data subjects.

14. Based on the above, the Authority considers that there is a case to exercise the v

the article 58 par. 2 of the GDPR corrective powers in relation to

found violations.

15. The Authority further considers that it should, based on the circumstances established,

to be imposed, pursuant to the provision of article 58 par. 2 sec. i of the GDPR,

effective, proportionate and dissuasive administrative fine according

30

article 83 of the GDPR both to restore compliance, and for

punishment of illegal behavior.

16. Furthermore, the Authority took into account the criteria for measuring the fine which

are defined in article 83 par. 2 of the GDPR, paragraphs 4 and 5 of the same article

which apply to the present case, article 39 par. 1 and 2 of the law

4624/2019 concerning the imposition of administrative sanctions on its entities

public sector, and the Guidelines for the implementation and

determination of administrative fines for the purposes of Regulation 2016/679 which

were issued on 03-10-2017 by the Article 29 Working Group (WP 253)8,

as well as the actual data of the case under consideration and in particular:

i)

i)

(iii)

iv)

v)

the fact that the breach resulted in a leak

sensitive health data of the affected person to a third party

face,

the fact that the controller delayed to

respond to the Authority's documents,

the fact that the controller has not yet clear

image, nor by the processors, as to the source

of the breach incident,

the fact that the data subjects were not facilitated

in the exercise of their rights, due to its incorrect registration

e-mail address of the Ministry of Foreign Affairs,

the fact that the designation of the DPO by the controller

was made with a delay of more than three years, while the relevant

procedures, which led to a designation as an external DPA

company, they did not act even after the initial document of the Authority

which pointed out the said matter only after the lapse of two

months from the Authority's reminder document on 02-01-2021, with

result, among others, that the controller has

significant financial benefit from the violation of the relevant

of his obligation, if the amount of expenditure is taken into account, which will

8 See https://ec.europa.eu/newsroom/article29/items/611237 (last accessed: 10/9/2021)

i)

vii)

viii)

i)

withdrawn the timely appointment of the YPD according to the law, as it follows from

the aforementioned in the history of the case concerning the

budgeted expenditure for the assignment of ODA services,

the fact that the controller carried out immediately

actions to deal with the incident,

the fact that no previous counterpart has been identified

breach by the controller,

the fact that from the elements brought to the attention of the Authority and

on the basis of which it found the above violations of the GDPR,

it does not appear that the controller caused, of

of a data breach incident that took place, material damage

to the affected person,

The fact that the violation of the provisions on rights

of subjects falls under, in accordance with the provisions of article 83

par. 5 sec. II GDPR, in its highest category

grading system of administrative fines.

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

notified controller

those referred to in the ordinance

administrative sanctions, which are judged to be proportional to the severity of the

violations.

FOR THOSE REASONS

The beginning,

It imposes on the Ministry of Tourism, as controller,

the

effective, proportionate and dissuasive administrative fine which

appropriate in the specific case according to the special circumstances

thereof, in the amount of seventy-five thousand euros (75,000.00) euros, for the above

established violations of articles 13, 32, 33, and 37 of the Regulation (EU)

2016/679, in accordance with article 58 par. 2 i) of the GDPR in conjunction with article

83 par. 4 and 5 of the GDPR and article 39 par. 1 of Law 4624/2019.

32

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou

33