Athens, 29-08-2022 Prot. No.: 2131 DECISION 43/2022 The Personal Data Protection Authority convened at the invitation of its President in a teleconference meeting on Tuesday 21.12.2021 at 10:00, in order to examine the case referred to in the history of the present. Konstantinos Menudakos, President of the Authority, and regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, and Charalambos Anthopoulos were present. At the meeting, without the right to vote, the audit specialists Georgia Panagopoulou and George Roussopoulos, 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 auditing expert scientist Konstantinos Limniotis, also an assistant rapporteur, did not attend due to disability. The Authority took into account the following: On the occasion of announcements by the company Palantir Technologies and a number of relevant publications in the press regarding the cooperation of the Greek Government with this company to deal with the pandemic, the Authority, within the framework of its powers based on article 58 of the GDPR and Articles 13 and 15 of Law 4624/2019 sent to the Ministry of Digital Governance and the Ministry of Health the no. prot. C/EX/8717/18-12-2020 document with which he requested information about the types of data that are the subject of processing and the exact purpose of the processing. He also requested the relevant 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 full contract for the assignment of processing, including any annexes, as well as any Personal Data Impact Assessment or which has been prepared in this regard. The Ministry of Health responded with no. prot. C/EIS/8936/31-12-2020 document, while the Ministry of Digital Governance responded with the no. prot. G/EIS/236/12-01-2021 document. The Authority then sent the no. prot. C/EXE/414/18-01-2021 document to the Ministry of Digital Governance in which he requested additional clarifications and information, in relation to his collaborations with the General Secretariat of Civil Protection (hereinafter GPP) and the National Public Health Organization (hereafter EODY). In particular, he requested: "a) The Memorandums of Cooperation between the Ministry of Digital Governance and: a) the Deputy Ministry of Citizen Protection/ General Secretariat of Civil Protection (the memorandum of cooperation dated 20.3.2020), and b) the National Public Health Organization (the 30.10.2020 memorandum of cooperation). b) Detailed description of all the data (the type and exact format) that EODY and GIS were transferring to the Palantir Technologies platform. In the event that these are considered pseudonymized or anonymized, the type of primary data, the databases from which they originate and the analysis of the method of pseudonymization or anonymization applied should be mentioned. c) Detailed description of the procedures, the platforms, the security measures, the frequency, the persons and the way of access to the information that

was uploaded by the PGPP and the EODY to the Palantir Technologies platform. d) Sample files uploaded to the Palantir Technologies platform. e) Evidence documenting the deletion of the data, after the end of the contractual relationship, both by Palantir Technologies and by the sub-processing companies referred to in the contract." The Ministry of Digital Governance responded with no. prot. G/EIS/1838/16- 03-2021 document. The Authority then sent the documents with no. prot. C/EXE/925/26-03-2021 and C/EXE/926/26-03-2021 documents to EODY and GPP, respectively, with which he invited the two agencies to state "the type of primary data, the 2 databases from which these data originate and describe in detail the method of pseudonymization or anonymization that was applied." EODY replied with no. prot. C/EIS/3030/07-05-2021 document, while the General Secretariat of Civil Protection did not respond. Then the Authority called for a hearing with no. prot. C/EXE/1442/08- 06-2021, C/EXE/1443/08-06-2021, C/EXE/1444/08-06-2021 and C/EXE/1445/08-06-2021 documents the Ministry of Health, the Ministry of Digital Governance, the EODY and the General Secretariat of Civil Protection, respectively, at the meeting on 6-29-2021, with an attachment to each call of the documents that had been exchanged between the Authority and the other bodies and a deadline for submission of additional information until 06-22-2021. The General Secretariat of Civil Protection submitted, after receiving the above-mentioned summons, with no. prot. G/EIS/3854/11-06-2021 document in response to no. prot. C/EXE/926/26-03-2021 of the Authority's document. The main points included in the response documents of the involved bodies are as follows: The Ministry of Health indicated that it has no knowledge of the matter. The Ministry of Digital Governance reports that on 24.3.2020 the "Technology Agreement" ("Technology Agreement") was signed between the Ministry and the company with the name "Palantir Technologies UK LtD" on the same date, which was amended on 26.03.2020 . The object of the technological pact was to provide the Greek Government with the right to access and use the software (platform) of the above company, exclusively for the analysis of statistical data and the extraction of data and results for the predetermined purpose of dealing with the pandemic against the Covid-19 coronavirus. 19, for a trial period of six (6 months) without compensation. The above trial period of the pact was extended under the same conditions for another three (3) months with the extension letter dated 18.09.2020, and ended on 23.12.2020. The intended result produced by the trial use of the software of the above company, was the visualization of 3 numerical data and their projection as layouts, graphs and data curves, as well as the extraction of further statistical data, which constituted auxiliary tools of the Greek Government and especially of the Commission of Infectious Diseases, in order to select, plan and then take the - case by case and phase - absolutely appropriate and necessary measures to combat and stop

the spread of the coronavirus and support the individuals and businesses affected by the pandemic health crisis. In order to visualize the data and extract further statistics, anonymous, statistical and demographic data were uploaded to the company's software by the public bodies themselves, which did not provide and did not contain information from which it was possible to directly or indirectly identify natural persons. persons (data subjects). The uploaded data were: either open data of the competent bodies, which helped to visualize the consequences of the pandemic in society more broadly in various sectors, and then posted on the page data.gov.gr, Greece, (https://data.gov .gr/datasets/internet_traffic), electricity consumption in Greece from (https://data.gov.gr/datasets/electricity_consumption), the stations of Attica (https://data.gov.gr/datasets/road_traffic_attica), stations STASY tickets and tickets on bus lines (https://data.gov.gr/datasets/oasa_ridership), company traffic itineraries (https://data.gov.gr/datasets/sailing_traffic), and demographic data, which are not provided and did not contain information from which it was possible to directly or indirectly identify natural persons (data subjects), and which were arranged to achieve the purposes described in this document, in accordance with articles 60 et seq. of Law 4727/ 2020 (A΄184) in combination with special further Memorandums of Cooperation between the Ministry of Digital Governance and: aa) the Deputy Ministry of Citizen Protection/ General Secretariat of Civil Protection (the memorandum of cooperation dated 20.3.2020), and bbb) the National Public Health Organization (the memorandum of cooperation dated 30.10.2020), and specifically: tracking network traffic measurements either anonymously, shipping internet traffic statistics as in and 4 a. From the GPP: aa. hospital details such as hospital name, address, hospital id, municipality, district, health district, ICU availability, covid-19 ICU availability, total number of ICU beds, total number of covid-19 ICU beds, total number of covid-19 beds 19, availability of beds for covid-19, number of total beds, availability of total beds, pp. details of ships quarantined after voyage, such as ship name, number of passengers, ship number, ca. Details of covid-19 cases, such as regional unit, municipality, age, gender, type of hospitalization (structure/hospital), status (quarantine, hospital, discharge, ICU, death), s. Travel Form details, such as date of connecting flight, date of flight, number of passengers declared, date of entry into the country, point of entry, date of completion of the form, type of point of entry, country and city of origin, country and city of origin, professional driver, shipping company and ship name, conduct test forcovid-19, test result. b. From EODY: aa. Number of patients admitted to Hospitals due to covid-19 nationwide, date of entry/exit, date of entry to ICU, date of intubation/extubation, outcome (exit, recovery, death, date of death), pp. cases, such as sample date, age, regional unit, imported or not, number of contacts with another covid-19 case, date of symptoms. The company's software never had

access to Government information systems, and the data was in any case uploaded by the above entities to the platform collectively, anonymously, with secure encryption, and the transfer of information was carried out in an absolutely secure manner. In particular, the company never had access to the production systems or registers of the entities that provided the data streams. The data to be transmitted was uploaded in each case by the above entities to a specific server and access was given to the company by each entity through encrypted communication channels, with access codes, and only for specific IPs in a remote folder (and only 5 of them), which contained the above anonymous, statistical or demographic data. Finally, according to the point under item 7 of the above Agreement, upon the expiry of the Agreement, which has occurred, the company deletes all the above data that had been uploaded to the platform. In any case, taking into account that the data was anonymous and there was no possibility of identifying a natural person, in the context of the Agreement in question, no processing of personal data, within the meaning of European and national legislation on personal data protection, has taken place and specifically as defined in article 4 par. 1 of the GDPR. The purpose of concluding the above Technology Support Agreement was to deal with the pandemic and protect the public interest in the field of public health, to visualize the trends that exist in this sensitive phase of the pandemic in various sectors, as well as to extract further statistical data /information within the framework of Directive (EU) 2019/1024 of the European Parliament and of the Council of 20.6.2019 on open data and the further use of information in the public sector, which has been incorporated into national legislation with Law 4727/2020 (A ´184). The Ministry points out that it was deemed unnecessary to carry out an impact assessment as the anonymous, numerical, statistical and demographic data that were transmitted did not relate to personal data, from which any natural person could be directly or indirectly identified, and were transmitted with secure encryption, and therefore the rights and freedoms of natural persons are not endangered. A copy of the Technological Support Agreement dated 24.03.2020 between the Ministry of Digital Government and the company Palantir Technologies, its amendment and the extension letter is attached. The original technology support agreement also included a special agreement regarding the protection of personal data ("GDPR Data Protection Agreement") as an excess to cover the possible transmission of personal data, which did not take place. character 6 The Ministry of Digital Governance also forwarded to the Authority the memorandums of cooperation between this Ministry and: aa) the Deputy Ministry of Citizen Protection/ General Secretariat of Civil Protection dated 20.03.2020, and bbb) the National Public Health Organization dated 30.10.2020 . He also clarified the following: The primary data of the finally uploaded data came exclusively from the databases and information systems of the General Directorate of

Public Security and the EODY, while, moreover, in the above memorandums of cooperation it was foreseen that all the data that would be uploaded by the above two bodies "do not concern personal data from which it is possible to identify directly or indirectly any natural person" (see article 1 par. 2 of the memorandum of cooperation from 30.10.2020), while in any case the data, which were visualized for the purpose of response to the pandemic, were anonymous, statistical and demographic data (see article 1 of the 02.03.2020 memorandum of cooperation), so the exact method of anonymization followed by the above bodies was within their exclusive competence. The committee of infectious diseases, within the framework of its responsibilities, defined - at regular intervals - the necessary data that needed to be visualized in order to depict the current epidemiological situation of the country, and then the above two bodies transferred these (anonymous, statistical and demographic data) . Only authorized users of the organization itself had access to the databases and information systems of each organization, while each organization had designated specific authorized persons for uploading the above described data. The frequency of uploading was on a daily basis, without this meaning that there was necessarily new data from each operator every day. Samples of the format of the files from the sub-categories 'data of Covid-19 cases' and 'cases' were also submitted. Regarding the deletion of data, the letter dated 29.01.2021 from the company Palantir was submitted, in which it is confirmed that the company has permanently deleted and destroyed all data (content) in relation to the "Technological Support Agreement" dated 24.03.2020, in accordance with the provisions in par. 7 thereof. 7 To the question about the type of raw data, the databases from which this data comes and the pseudonymization or anonymization method applied, EODY replied as follows: EODY was uploading to the company's platform under the name "Palantir Technologies UK ltd" only anonymous, statistical and demographic data, which contained information from which it was not possible to directly or indirectly identify natural persons (data subjects) nor was such information transmitted in any other way. Specifically, the data in question were as follows: a) In relation to the cases: Serial number, Date of sample, Age, Regional unit, Imported or not (Yes/No), Had close contact with a possible or confirmed case (Yes/No), Date of onset of symptoms. b) In relation to hospitalization: Serial number, Date of admission to hospital, Date of discharge from hospital, Date of admission to ICU, Date of discharge from ICU, Date of Outcome (Death/Hospitalization/Discharge), Date of death. of extubation, intubation, Date The information came from the Covid191 Patient Registry and the EODY database, where the primary data for epidemiological surveillance and investigation of the said disease are registered2. From the above databases (Covid Registry and epidemiological investigation) and after the application of two queries3 (SQL queries), two new "csv" (comma separated values) format files were produced,

completely distinct, which included only the crucial anonymized information of a statistical nature that were "uploaded" to a web space (platform) of the company "Palantir 1 According to no. 29 PNP 30.3.2020 (sanctioned by Law 4684/2020). 2 According to no. 2, 10 Law 4633/2019 and no. 12 PNP 10.8.2020 (sanctioned by Law 4722/2020). 3 Query 1: SELECT cases [A/A], cases.[SAMPLE HM/N], cases.AGE, cases.[REGIONAL UNIT], cases.IMPORTED, cases.[CLOSE CONTACT WITH COVID-19 PHI/HIV], cases.[BEGIN SYMPTOMS] FROM cases; Query 2: SELECT [hospitalizations(2)]. ID, [hospitalizations(2)].[ICU Admission], [hospitalizations(2)].[ICU Out], [hospitalizations(2)].[ICU Admission], [hospitalizations(2)].[ICU Out], [hospitalizations(2)].m/ndiasol], [hospitalizations(2)].[n/n/diasol], [hospitalizations(2)]. Output, [hospitalizations(2)].[Date of Death] FROM [hospitalizations(2)]; 8 Technologies" using the secure file transfer protocol "sftp". That is, using encryption as well as a limited range of IP addresses. After receiving the summons, the General Secretariat of Civil Protection submitted with no. prot. G/EIS/3854/11-06-2021 document in response to no. prot. C/EXE/926/26-03-2021 of the Authority's document, in which it states the following: Pursuant to the 20-03-2020 Memorandum of Cooperation between the Ministry of Digital Governance and the Deputy Ministry of Citizen Protection/General Secretariat of Civil Protection (GPP), anonymous, statistical and demographic data were collectively uploaded by GPP to a specific server of GPP, where through encrypted communication channels (API), with access codes and only for specific IP addresses, the above data were transferred to Palantir. In particular, they were uploaded from GPP: a. hospital details such as hospital name, address, hospital id, municipality, district, health district, ICU availability, covid-19 ICU availability, total number of ICU beds, total number of covid ICU beds -19, number of total beds for covid -19, availability of beds for covid -19, number of total beds, availability of total beds, b. details of ships quarantined after voyage, such as ship name, number of passengers, ship number, c. data on covid-19 cases, such as regional unit, municipality, age, gender, type of hospitalization (quarantine, hospital, discharge, ICU, death), d. Travel Form data, such as date of connecting flight, date of flight, number of passengers declared, date country of entry, point of entry, date of form completion, type of point of entry, country and city of origin, intermediate country and city of origin, professional driver, shipping company and ship name, covid-19 test performed, test result. (structure/hospital), situation The EODY then submitted the no. prot. C/EIS/3923/15-06-2021 postponement request, which the Authority accepted during the meeting of 29-6-2021 and informed the invited parties about the new date of the meeting, which was set to be the 26 -7-2021. In view of the discussion of the case at the adjourned meeting, the Authority with no. prot. C/EXE/1689/13-07-2021, C/EXE/1690/13-07-

2021 and C/EXE/1691/13-07-2021 documents sent to the Ministry of Digital Governance, the EODY, and the Ministry of Health, respectively, with no. prot. C/EIS/3854/11-06-2021 document of the General Secretariat of Civil Protection. the: General Demosthenes Anagnostopoulos, During the meeting on 16-7-2021, which was held by teleconference, the Secretary of Public Administration Information Systems was present, A, partner of the Minister of Digital Governance, B, Data Protection Officer of the above Ministry, Elena Rapti, Legal Advisor to the Minister of Civil Protection, C, Data Protection Officer of EODY and D from the office of the Data Protection Officer, Georgios Dellis with AM..., legal advisor of EODY, Panagiola Makri with AM..., Legal Advisor to the Minister of Health and E, Responsible of Data Protection of the aforementioned Ministry. All parties were given a deadline of 10-9-2021 to submit a memorandum. The Ministry of Health submitted the no. prot. C/EIS/5656/08-09-2021 and C/EIS/6121/24-09-2021 requests to extend the deadline for submitting a memorandum until 24-09-2021 and 1-10-2021 respectively, which were accepted and the other involved bodies were also informed. They were then filed with no. prot. G/EIS/6104/24-09-2021 memorandum of the EODY, with no. prot. G/EIS/6337/01-10-2021 memorandum of the Ministry of Health, with no. prot. C/EIS/6387/04-10-2021 memorandum of the Ministry of Digital Governance and the one with no. prot. C/EIS/6401/04-10-2021 memorandum of the General Secretariat of Civil Protection. In the memorandum of the Ministry of Health, it is stated, once again, that the Ministry was not aware of the matter and that, as clearly emerges from the relevant provisions governing the establishment and operation of the National Registry of Covid19 Patients, for the Ministry of Health, as controller, never the issue of any assignment of services to the company Palantir Technologies, let alone the processing of personal data, for which additional (based on articles 35, 36 of the GDPR) an impact assessment is required. The memorandum of the EODY includes a detailed description of the legal framework for the operation of the organization as well as the legal framework for access to the data of the Covid19 Patient Registry. In order to clarify the nature of the data transmitted to Palantir, i.e. whether it was personal data or not, anonymous or pseudonymized, a technical report entitled "Description of Data Processing for Statistical Evaluation by Palantir Software" is provided. The main points of the technical report are as follows: On a daily basis, the competent and specially authorized officers of the EODY, create two (2) spreadsheet files (excel) of the Covid19 patients, with a date of last modification up to 48 hours before moment of creation. The files are titled "cases" and "hospitalizations" respectively. The purpose of the creation of said files is to enable the authorized officers of the EODY to process the data within the framework of the EODY's responsibilities, namely: the epidemiological surveillance and investigation of the disease, the extraction of statistical data for the compilation of daily

reports, the updating of scientific and governmental actors, informing the European Center for Disease Control and Prevention and informing the World Health Organization. At the time the files are created, each record is assigned a serial number, starting with 1. The above assigned serial number has nothing to do with the "UPI" ("Unique Patient Identifier") number of the National Covid Registry, nor exists in the Covid Patient Registry or in any other file, except for the files that are created according to the above and were uploaded to a special common electronic folder on the EODY server, access to which was given to competent officials. This number cannot be combined with any item included in the National Covid19 Patient Registry or any other record. Further, no mapping table of each sequence number with the sequence 11 number drawn from the base is maintained. Therefore, it is impossible to use the serial number for the identification of a natural person (patient) by any person, other than the authorized officers of EODY. It is noted that only specific and expressly authorized users and analysts of the EODY, mainly health professionals, have access to the created excel files, as well as to the Covid Registry. Given that not all patients affected by Covid19 are hospitalized, the purpose of the performance of the ascending number is to control the course of the health of the patients and the correctness of the results of the statistical epidemiological analysis for the purposes of managing the pandemic. The serial number of each record is the same in both created files (for those records that are common to both files), and serves to read the variables from the used scripts that "apply" the algorithms for the use of anonymous data. E.g. the entry with a/a 528 in the "cases" file / sheet is identical to the entry with the same a/a in the "hospitalizations" file. The files being created were inserted into a temporary SQL table by executing macros (ie without being accessed by a user-executive of EODY). During the execution of each macro, two queries (SQL queries) are applied to isolate the fields. Then, again with the same macros without any other intervention, the contents of the SQL tables were deleted. After the completion of the execution of the macros, two "csv" files were exported, with specific fields only, "cases.csv" and "hostilisations.csv". After applying the macro queries and isolating the fields and their values, two corresponding self-contained 'csv' format files with new serial numbers were created. The Authority, in order to clarify points of a technical nature that were included in no. prot. C/EIS/6104/24-09-2021 memorandum of the EODY, mainly regarding the way of assigning the unique number to the records sent to the Palantir system, proceeded to an on-site check at the EODY, with the no. prot. C/EXE/2292/12-10-2021 control order of its President. The audit was carried out on 19-10-2021 at the headquarters of EODY, following which EODY filed the no. prot. C/EIS/7093/02-11-2021 document which includes the clarifications requested by the Authority's level during the audit. The main points of the document are the following: Regarding the way of rendering the

sequential number in the "csv" files, for the production of these files, the reverse sorting command is applied to the excel files of the EODY ("cases" and "hospitalizations"), so that the entry numbered "1" in the EODY file is the last in the csv file. Since every day new case-records are added to the Covid Registry and therefore also to the EODY records, the next day in the record with serial number "1" in the EODY records, the number will change in the csv files depending on how many new cases have been added and/or removed from the Registry. The following is given as an example: Patient A today has the number (1) in the EODY file and the number (n) in the csv file. The next day it remains with the number (1) in the EODY file, but in the csv it changes to (n)+x, where x is the number of cases each day. The only case in which the number in the "csv" files should not change is if there are no new cases in one day or, in general, if the Registry entries do not change within one day, while the change must take into account that some few cases-registrations may to be deleted the next day, e.g. due to error. However, in this case, which so far has never happened, a 'csv' file would not be transmitted either. Therefore, in this way there is no logical and/or technical possibility to reveal it every day, not even by the EODY executives themselves - so more reason than Palantir company or any other person has possession of the csv files even without being authorized to do so – to which natural person the csv file number corresponds. In its post-hearing memo, the Department of Digital Government adds additional evidence regarding the nature of the data being transmitted to Palantir. The main points are as follows: a) The entities that could use legitimate processes to gain access to additional information to lead to 13 identification are likely to be the same entities that already have access to the primary information for legitimate reasons provided in legislation. Palantir cannot invoke any legitimate reason/legitimate interest that would allow it access to additional information that would lead to identification. the major then on the one hand B) In the event that an abstract potential identifiability is accepted by an attacker (in various databases / additional information) the issue is not identifiability but in general the security of information, systems and networks and on the other hand we would be led to a " absurd" that there are no "anonymous data" and therefore that the relevant legislation is always applicable. Uploaded data are elements which are computationally impossible - for a third party (in this case Palantir) - to lead to the verification, directly or indirectly, of the identity of the person to whom they refer, even with the use of additional information, because the potential population of natural persons, among whom identification could be made, is large and constantly changing in all the Municipalities and Regional Units of the Territory. C) Even in the extreme case, in which we would refer to the least populated Municipality of the Country, which has a permanent population of 975 people, as it appears based on the latest population census (2011), where in particular in the information "Permanent

Population by place of birth (Municipality, foreign country)" appear as the Municipalities per territory with the smallest recorded number of permanent population those with geographic code "4626199" Municipalities of Leipsic and Agathonisi with a total population of nine hundred and seventy-five (975), the identification of the natural person/person is impossible, because the above number of permanent population does not include groups of natural persons, who resided temporarily or occasionally in the above Municipalities, tourists, students, transferred public or other private employees, and natural persons without the possibility of being differentiated are changed military personnel so etc. , 14 of determining them "by other means", and therefore the reference in case he does not identify with a citizen of the municipality in question who is recorded in the census. d) Based on the above, the identification of the case becomes unfeasible (always subject to the cross-checking of data collected in a legal way), given on the one hand the number of the permanent population and on the other hand that this number does not reflect, in accordance with the above, the actual number of natural persons per geographic area for the given time, as the population of natural persons in the particular geographic area to which this data refers changes and varies. In particular, with regard to the data from the EODY, the said data and information refer to the entire territory, without reference to a more specific geographical unit. In this case, due to the complete generalization and wide dispersion of the data, the chances of verifying the identity of the person based on the above data are nullified, since the information that on that particular day was entered e.g. 100 people in the country's hospitals, even in combination with additional information, cannot lead to the identification of a natural person. From this particular category of data, due to: i) their generalization, ii) the reduction of the cases to a Regional Unit, i.e. a geographical area with a population multiple times that of the Municipalities and iii) the non-constant number of inhabitants, no conclusions can be drawn under any circumstances which will result in the verification of the details of a specific person. The Authority, after examining the elements of the file and after hearing the rapporteur and the clarifications from the assistant rapporteurs, who were present without the right to vote, after a thorough discussion, DECIDED IN ACCORDANCE WITH LAW 15 1. In accordance with the provisions of articles 51, 55 and 57 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR) and articles 9 and 13 of Law 4624/2019 (Official Gazette A

137), the Authority has the authority to supervise the implementation of the provisions of GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 2. Article 5 of the GDPR defines the basic

principles for the processing of personal data. These principles include the principle of legality, objectivity and transparency, according to which data are processed lawfully and legitimately in a transparent manner in relation to the data subject (par. 1 a'), the principle of purpose limitation, according to which the data are collected for specified, explicit and legal purposes and are not further processed in a manner incompatible with these purposes, while further processing for scientific or statistical purposes is not considered incompatible with the original purposes (par. 1 b)), the principle of data minimization, according to which data are appropriate, relevant and limited to what is necessary for the purposes for which they are processed (par. 1 c´). It is pointed out in particular that the data controller, in the context of observing the principle of legitimate or fair processing of personal data, must inform the data subject that it is going to process his data in a legal and transparent manner (see C-496/17 op. op. para. 59 and OJ C-201/14 of 01-10-2015 paras. 31-35 and especially 34) and be in a position at any time to prove his compliance with the authorities these (principle of accountability according to art. 5 par. 2 in combination with articles 24 par. 1 and 32 GDPR). The processing of personal data in a transparent manner is an expression of the principle of fair processing and is linked to the principle of accountability, giving the subjects the right to exercise control over their data by holding the controllers accountable. 16 3. Based on the GDPR, controllers must implement appropriate measures to ensure and be able to demonstrate their compliance, taking into account, among other things, "the risks of different probability of occurrence and severity to the rights and freedoms of natural persons of persons" (article 24 par. 1). 4. According to the definitions of GDPR, Article 4, "pseudonymization" is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that said additional information is retained separately and subject to technical and organizational measures to ensure that they cannot be attributed to an identified or identifiable natural person. 5. According to recital 26 of the GDPR, the principles of data protection should be applied to any information that concerns an identified or identifiable natural person. Pseudonymized personal data that could be attributed to a natural person using supplementary information should be considered information about an identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all means which are reasonably likely to be used, such as for example their separation, either by the controller or by a third party to directly or indirectly ascertain the identity of the natural person. In order to determine whether any means is reasonably likely to be used to verify the identity of the natural person, all objective factors, such as the cost and time required for identification, should be taken into account, taking into account the technology available available at the time of processing and technology

developments. The principles of data protection do not apply to anonymous information, i.e. information that does not relate to an identified or identifiable natural person or to personal data that has been made anonymous in such a way that the identity of the data subject cannot or 17 can no longer be be ascertained. The GDPR therefore does not concern the processing of such anonymous information, not even for statistical or research purposes. 6. In accordance with recital 28 of the GDPR the use of pseudonymisationin personal data can reduce the risks for the
data subjects and facilitate controllers
and the processors to comply with the relevant obligations regarding
data protection.
7. In this particular case, it is established that the data which
were being forwarded to Palantir can no longer be attributed to
specific data subject
(except for extreme hypotheticals
cases, such as in a regional unit with small
number of cases a third party, who knows a person who came out
positive to Covid19, and the exact time, for example due to the procedure
contact tracing, to be able to locate the specific person in the aggregate
of records, through the data: sample date, sex, age,
regional unity). It then has the ability to acquire
access to information about the individual's health outcome
(impact) through the information contained in the corresponding record (has
the same unique number) for hospitalization and its outcome (date of admission,
date of discharge, ICU admission, ICU discharge, intubation date, date
extubation, outcome, date of death). In conclusion, from the set of
elements brought to the attention of the Authority, it is concluded that the level of protection
of the data is deemed satisfactory and the possible risks to the subjects
of data extremely small.

8. In view of the above, and given that, as certified by the Ministry

of Digital Governance, the "Technological Support Agreement", which

had concluded with the company "Palantir Technologies UK LtD" expired

23.12.2020 and that the company has definitively deleted and destroyed all the

data (content) in relation to this Agreement, in accordance with

defined in paragraph 7 hereof, there is no case of exercising the

corrective powers of the Authority.

18

FOR THOSE REASONS

The Authority considers that its ex officio examination as above has been completed

case, unless new evidence emerges.

The president

The Secretary

Konstantinos Menudakos

Irini Papageorgopoulou

19