DECISION 50/2021 Athens, 16-11-2021 Prot. No.: 2614 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via video conference on 23-07-2021, 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 and Charalambos Anthopoulos were present as rapporteur. At the meeting, without the right to vote, the auditors Kalliopi Karveli, Fotini Karvela, legal experts and George Rousopoulos, IT expert, as assistants to the rapporteur, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary, attended the meeting, without the right to vote. The Authority took into account the following: The Authority issued its opinion No. 4/2020 to the Ministry of Education and Religious Affairs (hereafter Ministry of Education) in order to ensure the compatibility of modern distance education in primary and secondary school units with the provisions of the General Data Protection Regulation (hereinafter GDPR) and Law 4624/2019. The Authority considered that the provision of modern distance education is in principle legal, but called on the Ministry of Health to take into account the recommendations mentioned in the reasoning of the opinion, as well as to modify and complete the relevant data protection impact assessment (DPA) accordingly. within an exclusive period of three (3) months. 1-3 Kifissias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 The Authority with case number C/EX/6743-1/16-11-2020 In her letter, the Ministry of Education and Culture invited the Ministry of Health to inform the Authority if it has completed and amended the EAPD for modern distance education, in accordance with the recommendations mentioned in opinion 4/10, providing all relevant documents. With the same document, he forwarded to the Ministry the request No. C/EIS/6153/10-09-2020 and the report No. C/EIS/6743/05-10-2020 of OIELE since are related to issues that were raised with the initial reports of OIELE and to which the Authority reserved its opinion to return, asking the Ministry to respond in writing to the reported issues within the same deadline. In the first of these documents, OIELE raises the issue of whether the Authority considers the EAPD document to be an administrative entity, while in the second of these documents, OIELE briefly mentions that: 1) The wording of the provision of par.1 of No. 120126/GD4 WILL. (Government Gazette B' 3882/12.09.2020) ("as long as the risk of the spread of the COVID-19 coronavirus remains"), is vague and causes significant uncertainty in relation to the circumstances and the determination of the circumstances under which the modern ex distance education. It does not sufficiently specify what is meant by the risk of the spread of the coronavirus, and no tools are provided on how to establish the existence of the risk. Therefore, he considers that the application framework of modern distance education is dangerously widened, as it is not linked to the start, extension or end of the protection measures against

the pandemic. 2) The EAPD document is administratively non-existent. 3) The contracts with CISCO have not been made public and it is doubtful if they exist as public documents while the Authority must not rely only on them, but seek and judge the real relationship between the parties, in order to properly determine the role of the parties . 4 - 5) New risks have arisen especially in relation to those students who belong to an increased risk group or who live with a person who is sick or are sick themselves or who are waiting for examination results, who receive mandatory distance education and in relation to teachers who belong in an increased risk group. For these categories, the Ministry has not carried out a risk reassessment procedure. 6) The Authority's guidelines for taking security measures 2 in the context of telecommuting do not apply, as it is doubtful whether "end to end encryption" is applied when transmitting audio and video in the context of using the Webex platform. 7) The Webex application is not certified by I.T.Y.E. Diophantus. 8) The principle of transparency is violated, especially in relation to the provision of information and the terminology used of the metadata that is kept, even in relation to children. 9) The personal data of the members of the educational community are likely to be processed for a purpose other than its declared purpose, for the commercial purposes of the processor. 10) There is an impermissible profiling process, with an indefinite retention time and anonymization process. 11) There is an illegal transmission of data outside the EU. 12) There is no right of deletion. OIELE also points out that following the aforementioned Y.A. it is directly concluded that both public and private schools can use the WEBEX digital platform, therefore it is legal for submitting the report-complaint. The Ministry of Health sent the updated EAPD to the Authority with document No. C/EIS/{8419,8421,8422}/08-12-2020 and with document No. 230-6759/11-12 -2020 his document (no. prot. Authority C/EIS/8553/11-12-2020) provided his views, in relation to the issues raised by the Authority and the reports of OIELE. With its memorandum, the Ministry of Education and Culture describes in detail the procedure followed for distance education, which it considers to follow the principles of data protection already from the design and by definition according to the requirements of the GDPR, while as the Data Controller it has taken the appropriate measures security- protection of personal data, ITYE as the processor implements appropriate security measures in relation to the Central User Certification service and Cisco as the processor implements appropriate technical and organizational information security measures regarding the e-learning platform. According to the Ministry, the updated EAPD was implemented based on the Authority's recommendations, identified and assessed the risks involved in the process of modern distance education and described the 3 methodology for dealing with them. The EPA concludes that the fundamental principles of personal data processing are not violated and the principle of proportionality is satisfied, while the risks were

considered acceptable, provided the appropriate measures are applied. In relation to the issues raised by OIELE with its memoranda, the Ministry of Defense points out that: 1) the Ministerial Decision was issued within the limits of the legislative authorization and complied with its terms, while it is not at all vague and does not cause any uncertainty in relation to the circumstances under which the distance learning process will be applied. 2) the EAPD was submitted to the Authority and had already formed the basis for the issuance of opinion 4/2020. 3) the contract with Cisco from 13/3/2020 had already been submitted to the Authority and had been used to issue the 4/2020 opinion, while the newer contracts were also submitted accordingly. 4-5) In the EAPD of 7/12/2020, the risks related to the protection of personal data that may arise from the individual procedures of distance education were identified and thoroughly examined, while the provision regarding the obligation to provide distance education during the 2020 school year -2021 contrary to the provision regarding the possibility of providing distance education during the 2019-2020 school year, not only is it not a source of new risks for students, but on the contrary it is a guarantee and fulfillment of the state's obligation to provide them with the public good of education at the same time as protecting their own health and that of the persons who live with them. 6) The Controller implements appropriate technical and organizational measures designed to implement data protection principles. End-to-end encryption would have the consequence of reducing the functionality of the platform, as certain functions become significantly more difficult, so that even the inability to provide the service is not ruled out. At the same time, it is not the only technical measure to protect personal data. The communication of the client application (client app) that is installed on the user's computer up to the exit point that is in the Cisco internal network is encrypted and absolutely secure for this reason, while 4 for the rest of the network, appropriate security measures are applied. 7) ITU has approved the Cisco Webex application. For this purpose, the contract between the Ministry of Health and the ITU was signed on 11/9/2020. 8) The metadata that is processed is referred to both in the Ministerial decision and in the Circulars given to the Data Subjects (educators, parents, students). Given the technical nature of certain terms and to ensure their exact performance and therefore the absolutely correct and transparent informing the Subjects it was deemed appropriate to use their official and widely known term. The specific information (metadata) cannot be linked to a user and lead to the identification of his person except through the data declared when entering the platform, namely the name and/or e-mail address. From them, on the one hand, information of a technical nature and on the other, information related to the videoconference process itself, i.e. the course, can be obtained. No information regarding the course itself is known to the data controller, as the course is not recorded. Carrying out statistical analyzes and research is an

obligation of the Ministry of Education and Culture as part of its mission to develop and continuously upgrade education. No other conclusion can be drawn from the generated metadata, such as in relation to the evaluation of employee efficiency. Metadata, as well as all personal data processed in the context of distance education, excluding data that CISCO is required by law to keep further, is deleted without delay once the purpose of the contract has been fulfilled. In this case, the agreed special condition of the concluded contract prevails. Cisco's general term contained in the Master Data Protection Agreement document does not apply. 9) The Ministry of Education and Culture remains the Data Controller for the process of providing modern distance education and Cisco processes on its behalf all the metadata necessary for the provision of this service, which also includes the resolution of technical issues. Different is the issue that Cisco is required to comply with the legislation to which it is subject (eg tax 5 legislation) and therefore for this purpose it is necessary to act as a Data Controller. 10) There is no profiling-related concept component. 11) The Ministry of Health amended the contract with Cisco and in this matter the general terms and conditions of the Cisco company do not apply, but the special agreement it has concluded with the Ministry of Health and, in case they are forwarded, the conditions of the GDPR will be exceeded. 12) The Ministerial Decision does not in itself have the role of informing the Subjects but functions in addition to the informational text issued to them, the circulars and the EAPD. The Authority, taking into account the above documents, with its document No. C/EXE/613/11-02-2021 invited the Ministry of Health to clarify a series of issues by asking specific questions, namely: 1. On page 18 of the Authority's opinion 4/2020 it is pointed out that "the differentiation of needs and conditions should be taken into account by level of education (and perhaps by group of classes, e.g. A-B Primary, C-D etc). It is therefore necessary to study more alternatives/methods and identify specific measures and techniques (including educational methods) to minimize the impact on the rights of data subjects, adjusted by age group, to document necessity and proportionality. In the updated EAPD and in the attached studies (of the IEP and academics) the needs and differences are analyzed and appropriate methods are identified as tools for each teacher. The organization of online courses and the utilization of the guide "for the educational planning of distance courses" of the IEP are suggested as examples. Question: How have all the teachers been informed about these methods so that they can be implemented effectively? 2. According to the EAPD (p. 53) "The opinions of the representatives of the Subjects were formulated: 1. On 13.07.2020, in the context of a relevant meeting with the Minister of Education and Religion. 2. With the petitions respectively of OIELE, IOE and student's parent/guardian against the Ministry of Education. 3. On 14.07.2020, at meeting 6 of the Plenary Assembly of the APDPH, in the context of which the above (under 2) petitions were discussed." In

fact, while the Legal Informatics Laboratory of the Faculty of Law of the EKPA was entrusted with the revision of the EAPD Study from 15.5.2020, no consultation with representatives of subjects was carried out after this assignment. Question: Do you consider this procedure sufficient in relation to the Authority's recommendations? Have you considered other methods of voicing the opinion of data subjects or their representatives (eg through platforms such as opengov) and indeed after input from the IEP and academics? 3. What form of assistance did the processors provide, taking into account the nature of the processing and the information they have, to carry out the DPA? 4. In relation to risk 1 (Illegal access to personal data) of the original EAPD, it follows from the updated EAPD that its treatment depends on an identity check that the teacher must do. Question: How have the teachers been informed so that they know that this control is a security measure or an obligation? 5. In opinion 4/2020 of the Authority, reference is made to risks from the use of equipment that is not the responsibility of the data controller, especially with regard to teachers, while at the same time it is stated that the issue of the use of a personal device for official purposes should also be examined (cf. . and decision 77/2018 of the Authority). The updated EAPD mentions that this risk has been addressed (p. 15), but without a more specific explanation on pages 47-51 thereof. In the attached opinion of Professor Mr. A, reference is made to appropriate measures to protect user equipment, which are practically implemented through information and awareness among users. Question: What measures exactly were taken to mitigate this risk? Have the issues that arise when using a personal device for a business purpose been addressed? 7 6. In relation to the issue of the transfer of data outside the EU, as it appears from the response documents, the ministry amended the contract with Cisco and you argue that in relation to this issue the general terms and conditions of the Cisco company do not apply, but the special agreement. The Authority in opinion 4/2020 had raised a number of issues in relation to transfers outside the EU. Question: Have the issues arising from the CJEU decision C-311/18 been addressed? Has the applicable legal regime in the importer's country been examined to ensure that the rights of data subjects are implemented in each case? This taking into account that with the data available to the Authority it appears that the main company of the Cisco group is based in the USA, while a computing cloud platform (Cisco universal cloud) is used and therefore the application of the legislation of this country is possible. Were these issues considered in detail? 7. The Authority, in opinion 4/2020, had pointed out risks deriving from the terms of the contract (see page 26). Regarding them, the updated EAPD refers to the additional contracts (fig. 10 and 11 – i.e. the 11/09/2020 and 09/11/2020 contracts with CISCO HELLAS A.E.) without further analysis. It is pointed out that the contracts show that a series of personal data are kept for seven years, which include registration data, but also pseudonymous

data for "analytics" and performance measurement purposes. For example, the additional contracts appear to include data made available by the Ministry, but not data generated during use, made known to the processor. Question: Were these issues discussed in detail? 8. In the new contracts (fig. 10-11) general reference is made to subcontractors. The supervision of these is assigned to Cisco while there is no identification of them. In footnote no. 20 it is stated that the subcontractors have been notified to the Ministry of Health, that in case there are further subcontractors they will be notified to the Ministry of Health in order for it to formulate any objections and they will be bound by the necessary obligations. In the event that they are outside the EEA, CISCO has contractually undertaken the 8 commitment to ensure compliance with the conditions of Chapter V of the GDPR and to inform the Ministry of Health. Question: In the case of a processor in a country outside the EEA, has the completeness of the legality of the transfer been checked? Please forward to the Authority the notification to the Ministry of the subcontractors from Cisco as well as any other relevant document. 9. The Authority in opinion 4/2020 pointed out the obligation of the data controller for increased transparency and for the implementation of actions to inform and raise awareness of those involved (educators, students, family) in relation to the distance learning process and personal data (see in particular p. 28). From the measures described in the GDPR in relation to the information provided to the data subjects, it appears that again a formal - official - information is followed, which is based mainly on the texts of the circulars and announcements to parents and students. Question: How is the satisfaction of the principle of transparency of the GDPR ensured (Article 5 para. 1 a' GDPR)? Apart from circulars and announcements, is information provided in any other way? Has information material suitable for each group of stakeholders been created and information and awareness actions implemented? Which of your actions are geared toward minors and the family environment? Also, the Authority pointed out in its document that under no. prot. C/EIS/3701/29-05-2020 report of OIELE to the Authority, the question arises of the competences and participation of the Data Protection Officer (DPO) in the relevant data processing. In particular, as reported by OIELE, there is no mention of the person, role, responsibilities, purposes and support group of the most central person in ensuring the protection of data subjects, as well as any mention that the "instructions" of the circular were issued after expressing an opinion of the DPO, since, as mentioned, the participation of the DPO in the planning of a processing and the expression of opinion is not formal, but constitutes an essential measure and at the same time a guarantee of the protection of individual liberties and the data of the subjects. For this reason and taking into account the particular structure and the 9 large number of organic and supervised units of the Ministry of Education, it was requested to clarify how the requirements of article

38 of the GDPR are ensured not only for independence, but also for the provision of appropriate means and resources for the execution of the duties and responsibilities of the Ministry of Foreign Affairs. It was pointed out that from the information available to the Authority, it appears that the procedure for announcing the details of the DPO to the Authority has not been followed (article 37 par. 7 GDPR) although during the examination of the case the Authority was informed of a change in the details of the DPO. Along with this document, the Authority communicated to the IOE and OIELE a copy of the updated EAPD and the views of the ministry, inviting them to submit any additional views on them. The IOC did not submit any opinions, while OIELE sent its opinions to the Authority with its document No. C/EIS/1682/09-03-2021. With this, he supports, in summary, the following: 1) The EAPD of 15/5/2020 is unlawfully accepted, while no similar issue is raised for the updated study. 2) The updated EAPD does not bear a secure time stamp, is not based on a Recognized Certificate and was not created by a Secure Signature Creation Device, being unable to bring about consequences according to substantive (and procedural) law. 3) The tactic of non-publicized documents, the violation of the principle of transparency and the violation of the rights of the subjects continues. 4) It is completely unfounded to claim that the opinion of the data subjects was sought and expressed in relation to modern distance education. 5) The scientific assumptions, on the basis of which the decisions to suspend the operation of the school units were taken, and thus to what extent the modern distance education, which involves the processing of personal data, was deemed necessary and legally implemented, have not been examined. The Authority should take into account the issue of the quality of the legislation and in particular whether the law (in a formal as well as a substantive sense) which induces data processing, is accessible and predictable. Given the non-disclosure of the recommendations of the Infectious Diseases Committee which called for the implementation of modern 10 distance education and its subsequent consequences for the subjects, it becomes clear that this measure is manifestly illegal, it must stop, without the need to assess whether the following criteria examined by the ECtHR are met (if the essence of the right is respected, etc.). Therefore, the invoked legal basis of public health protection on which modern distance education is based is not proven. 6) Modern distance education, under the technical requirements it has and the real economic and demographic data of Greek society and the immigrants and refugees residing in it, results in the exclusion of the weaker social strata from the right to education, so induces discrimination and this situation has not been adequately examined by the controller, despite the clear recommendations contained in Opinion No. 4/2020. The EAPD study also at this point demonstrates an unjustified sloppiness and reaches completely arbitrary conclusions. 7) The EAPD has not taken any notice of the existing and increasing risks for children, regarding the

abuse they receive in the family environment. 8) The Ministry's claims about the categories of data and metadata collected when using the platform, about anonymization, about the retention time and about statistical/research purposes are unproven and violate any concept of transparency and adherence to the principle of accountability. There is no cooperation of the processor and it has not been assessed whether the conditions of legality are met in relation to the processing of this data. Applicable law in relation to these is not primarily the GDPR, but the e-privacy directive and national law 3471/2006, although there are points of intersection between them. The conditions for the application of this legislation have not been highlighted or evaluated. 9) The EAPD does not report on the issue of data transfers outside the EU. 10) From 12/2/2021 no. prot. Φ1/17598/GD4 circular of the Ministry of Education and Culture it appears that the digital infrastructure that has been developed for the implementation of the modern distance education of students is used, uncritically, for uses for which it has not been examined whether they can legally be served through it, such as to provide remote support 11 and consulting. 11) The letters of the university professors cited by the Ministry of Education prove the fact that the EAPD study from 7/12/2020, as well as the general organization of the processing, did not take into account the high requirements for the correct organization of distance education as well as the collateral and serious consequences for the right to education and the mental health of students and teachers. 12) The position of the technical consultant, who appeared before the Authority in the procedure on behalf of the data controller, can hardly be reconciled with the guarantees of independence required in the person of the person conducting an EAPD study, for the same data controller. It is noted that the Authority with its document No. G/EXE/824/10-03-2021 granted OIELE a series of documents following document No. G/EIS/1182/18-02-2021 of, while after these OIELE did not come back with a newer document. The Ministry of Health with its document no. 42593/YPD/13-04-2021 (authority no. C/EIS/2553/14-04-2021) responded to the Authority's document of 11-02-2021 , providing his views in relation to the questions raised which are summarized as follows (numbering corresponding to the numbering of the Authority's document follows): 1. Regarding informing all teachers about distance education methods. The Ministry lists a series of actions, specifically: a) Following the initiative of the Ministry of Health implemented in collaboration with the IEP and the University of the Aegean, a fast-paced training program - especially for teachers - in the methodology of distance school education b) The "Guide for the educational planning of courses" was forwarded to the competent services of the Ministry of Education and Culture, after a relevant recommendation from the IEP of distance education during the 2020-21 school year". The teachers declared in writing that they were informed about the "Guide". 12 c) A "Rapid training of teachers in

distance education" program was implemented through a partnership of the Ministry of Education and Culture with eight (8) institutions (AEI and ITU-Diofantos). The purpose of the specific action is "the further cultivation of the knowledge and skills of teachers in pedagogical and teaching methods, in order to apply the methodology of distance education in qualitative terms. 2. Regarding the process of formulating the opinion of the subjects. The Ministry of Health maintains that the opinion of the representatives of the subjects was clearly formulated during the implementation of statutory procedures (meeting - reports of trade union bodies - Authority meeting). Also, data subjects addressed in several cases the competent services of the Ministry of Health either by expressing an opinion regarding the issue of distance education or by asking related questions. After the assignment to the Legal Informatics laboratory of the Faculty of Law of the Greek Academy of Sciences, the possibility of using technological solutions was examined (in accordance with the recommendations of Authority) and "given the available resources and limited implementation time" concluded that the use of a public platform (or related methods) was particularly likely to lead to erroneous and unreliable conclusions. It was decided to carry out research (in collaboration with the IEP) in order to determine the effects of moving away from live teaching. The investigation is ongoing. 3. Regarding the form of assistance of the Processors in the preparation of the EAPD The Ministry maintains that relevant provisions exist in the contracts with ITYE Diofantos and CISCO. For the implementation of the provisions, it states that the executors provided information both to the Ministry and to the editors of the EAPD upon request, in writing or orally (in the context of online meetings) and included: a) The user manuals of the systems, b) The information security policies systems and protection of personal data, c) 13 answers to questions regarding the operation of the systems and the implementation of the relevant procedures, d) Information regarding the already implemented measures to mitigate risks for personal data, and e) on the implementation of measures , the purpose of further addressing - definitive elimination of risks for personal data. 4. Informing teachers about the identity check The Ministry states that a relevant provision exists in KYA 120126/GD4 (Government Gazette 2 3882/12-9-2020), which stipulated that the classrooms are locked, the students wait in the hall waiting room and the teacher is asked to approve the entry of each participant. The Ministry accepts that identity verification is a security measure through which unauthorized access to the online classroom can be prevented. During the implementation of the distance learning process, information is provided by the Support Team of each school unit and, if required, by the user support service ("Help Desk") of the Panhellenic School Network (PSD). Also, the issue of identity verification is sufficiently analyzed in the context of training programs. 5. Regarding the use of equipment that is not subject to the control of the Controller The Ministry

states that the use of personal devices (students or teachers) is described as a "main threat" to the realization of the risk of illegal access to personal data during its transmission, and, consequently, the (illegal) recording of the electronically transmitted course, in particular in cases where the users' login credentials to the (PSD) and/or the online class link have been stored on the devices used. As a measure to deal with this threat, users of the PDS (including teachers and students) were informed that they should not choose to "remember passwords" on personal devices. It is also pointed out that over time teachers and students use personal devices to 14 access the services of the PSD, i.e. for official/educational purposes. ITYE provides technical support to PDS users, which includes awareness initiatives and providing guidance on the proper use of personal devices, as well as effectively dealing with any technical issues. The Ministry states that it is going to issue instructions in accordance with the Authority's Guidelines for the protection of data during teleworking, while at the same time ensuring the continuous support of teachers through the two (2) level service system. 6. Regarding the transmission of data outside the EU Especially in view of the CJEU decision C-311/18 (Schrems II) The Ministry reports that the donation contracts were concluded with "CISCO HELLAS SA", the company of the group that operates in GREECE. It points out that all CISCO Group companies implement appropriate procedures for compliance with the provisions of the GDPR as the processing activities it carries out are related to the offering of services to subjects located within the EU. "CISCO HELLAS A.E." contractually undertook not to transmit outside EE/EOX the personal data it processes on behalf of the Ministry without prior notification. In the event that data is transferred outside EE/EOX, it will be carried out under the conditions of Chapter V of the GDPR and provided that CISCO had previously informed the Ministry of Health and Welfare by providing sufficient information and evidence documenting that the aforementioned conditions are met. In view of CJEU decision C-311/18 (Schrems II), the Ministry addressed CISCO and received assurances, with reference to the group's relevant policies, that cross-border transfers are subject to adequacy decisions and other appropriate guarantees, which do not include the removed "Privacy Shield" mechanism. Furthermore, the CISCO executives informed the Ministry that from the initial evaluation carried out, in accordance with the relevant directives of the ESA, it emerged that the transfers referred to in particular 15 in standard contractual clauses and binding corporate rules are legal, as the implementation of the rights of subjects. The assessment carried out by the CISCO Group will be revised with the issuance of relevant instructions by the ESPD. For this evaluation, on the one hand, the already implemented personal data protection measures were taken into account, and on the other hand, the assurance that until today no request from the competent services for the provision/disclosure of data has ever been

submitted to the US-based companies of the Group. 7. Regarding the terms of the contract The Ministry states that on 04/12/2020 it was signed with "CISCO HELLAS S.A." act of amendment of the donation contract from 09/11/2020 in order to address the risks arising from the contractual conditions, as the Authority had pointed out with Opinion 4/2020 and for the content of the contract to fully meet the Authority's recommendations. Regarding the marking for data retention for seven years, it is clarified that, upon fulfillment of the purpose of the contracts, CISCO promptly deletes the personal data it processed on behalf of the Ministry, upon request, unless otherwise required by law. This deletion is included in the issues for which a special negotiation preceded and for which the general terms of the Group's policy do not apply, but the special agreement with "CISCO HELLAS A.E.". Also by means of an act of amendment to the contract, the references to data to be made available/made available were replaced in a way to cover, explicitly and with greater clarity to remove any doubts, the set of data, so as to reflect the will of the parties, which also interpretatively resulted from the content of the existing donation contracts. 8. Regarding processing subcontractors in particular those based outside the E.E. /EOX The Ministry states that in the Deed of Amendment of the donation contract from 04/12/2020 a list of subcontractors (Related 16 9) is attached as Appendix A which includes for each subcontractor: a) name b) categories of personal data processed at the request of processor (CISCO), c) description of the service provided by him, d) the country(ies) in which he operates, e) the conditions met for the cross-border transfer ("transfer mechanism"), where required. in this way, the Ministry can effectively control the legality of the cross-border transfers carried out and, in this regard, the compliance by the processor of its contractual commitments. 9. Regarding transparency and the implemented information and awareness activities The Ministry reports has provided the data subjects with detailed information about the implementation of the distance learning process, the as detailed in the EAPD (par. 45). The main methods used for the purpose of informing and raising the awareness of the subjects are: a) Circulars-announcements ("standard-service information"). The Ministry states that the use of statutory procedures, with which the educational community is sufficiently familiar, facilitates the satisfaction of the principle of accountability as the Ministry of Education and Culture is able to prove that the subjects were aware of the instructions and other information, as well as other fundamental principles that govern the action of the Public Administration. b) Websites: The Ministry of Education has developed two (2) websites with user-friendly (minor) users and fully updated content in order to inform and raise awareness among students and their families. c) Training Activities / Programs: The Ministry of Education and Culture has organized the activities mentioned earlier. 10. Regarding securing the requirements of art. 38 GDPR on the independence and the provision

of the necessary resources to the Ministry's DPO 17 According to the Ministry, the participation of the DPO in the planning and implementation of the distance education process results from the text of the EAPD itself, as in paragraph 84 it is stated that provided on 7/12/2020 the advice of the Ministry of Foreign Affairs (art. 35§2 GDPR) before the finalization and acceptance of the study. The Ministry considers that any further analysis regarding the formulation of its opinion and the exercise of its powers in the context of the specific processing activity is unnecessary. Regarding the issue of independence, it is pointed out that the DPO is not subject to orders regarding the exercise of its duties nor is it controlled in any way, it does not take decisions or hold a position from which it can determine the purposes and/or means of any processing of personnel data character. He argues that the DPO took on this role because of its expertise and ability to fulfill the relevant tasks. He also adds that given the nature of the processing activities as well as the size of the Ministry, as of September 2020 a plan is being considered for the assignment of DPO tasks at the level of regional directorates, which will take on the specific role, will be selected on the basis of their professional skills and will exercise the responsibilities that will be assigned to them under the supervision of the YPD of the Ministry. In this way, the Ministry had responded in a related case (after a report by a Member of Parliament, see the document with reference no. G/EIS/4109/15-06-2020). The Ministry of Foreign Affairs cooperates with all departments of the Ministry and is supported by senior officials of the Directorates of the Ministry. The contact information of the DPO is available both to the Authority and to the data subjects. Finally, the Citizen's Advocate with his document No. 296136/20507/10-04-2021 (Authority No. C/EIS/2512/12-04-2021) informed the Authority that he received and is examining from the side of his responsibilities, a large number of reports from parents and teachers regarding the protection of the personal data of the subjects who use the WEBEX platform in the context of distance education, and asks for the sending of the Authority's conclusion. 18 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 THINKS ACCORDING TO LAW 1. In accordance with the provisions of Articles 51, 55 and 57 of the General Data Protection Regulation (EU) 2016/679 (hereinafter GDPR) and Articles 9 and 13 of Law 4624/2019 (Official Gazette A

137), the Authority has the authority to supervises the implementation of the provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. 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 the 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.cit. para. 59 and CJEU 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). 19 The processing of personal data in a transparent manner is a manifestation of the principle of legitimate processing and is linked to the principle of accountability, giving the subjects the right to exercise control over their data by holding the controllers accountable1. 3. With the GDPR, a new model of compliance was adopted, a central element of which is the principle of accountability, in the context of which the data controller is obliged to plan, implement and generally take the necessary measures and policies in order for the data processing to be compliant with the relevant legislative provisions. In addition, the data controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. It is no coincidence that the GDPR includes accountability (Article 5 para. 2 GDPR) in the regulation of the principles (Article 5 para. 1 GDPR) governing the processing, giving it the function of a compliance mechanism, essentially reversing the "burden of proof" as to the legality of the processing (and in general compliance with the principles of article 5 par. 1 GDPR), shifting it to the data controller, so that it can be validly argued that he bears the burden of invoking and proving the legality of the processing. Thus, it constitutes the obligation of the data controller, on the one hand, to take the necessary measures on his own in order to comply with the requirements of the GDPR, and on the other hand, to demonstrate his compliance at all times, without even requiring the Authority, in the context of research - of its audit powers, to submit individual - specialized questions and requests to ascertain compliance. The data controller must, in the context of the Authority's audits and investigations, present on his own and without relevant questions and requests from the Authority the measures and policies he adopted in the context of his internal compliance organization, as he is aware of them after planning and implementing the relevant internal organization. 1 See O.E. of article 29 as adopted

by the GDPR - Guidelines on transparency under Regulation 2016/679 of 11-4-2018 (WP 260 rev.1), pp. 4 and 5 20 4. In in relation to the principle of transparency, the GDPR Guidelines2 state that the concept of transparency in the GDPR is user-centered and non-formalistic, while it is realized through specific practical requirements for controllers and processors provided for in various articles of the Regulation. The practical (information) requirements are described in Articles 12 to 14 of the GDPR. However, the quality, accessibility and clarity of understanding of the information are just as important as the actual content of the transparency information to be provided to data subjects. Article 12 of the GDPR requires the information provided to comply with specific rules which include the following obligations: to be concise, transparent, understandable and easily accessible (Article 12(1)), to use simple and clear wording (Article 12(1)), and the requirement for clear and simple wording is of particular importance when providing information to children (Article 12 paragraph 1). Furthermore, in article 13 par. 1 and 2 of the GDPR, a specific set of information is defined that the data controller must provide to the data subject at the time of receiving the personal data. 5. In accordance with the provisions of article 6 par. 1 of the GDPR, the processing is lawful only if and as long as at least one of the following conditions applies: ...c) the processing is necessary to comply with a legal obligation of the controller,.... .e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of a public authority delegated to the controller. 6. Especially with regard to access to information stored on a user's terminal equipment, the more specific legislation for the protection of personal data and privacy in the field of electronic communications3 (ePrivacy) applies, specifically article 4 paragraph 5 of 2 For full analysis see paragraphs 4,7,8,9,11, 12, 14, 15 and 16 in the aforementioned document WP 260 rev.1 3 See and recital 173 of GDPR 21 Law 3471/2006 in which it is provided that the storage of information or the gaining access to information already stored in the terminal equipment of the subscriber or user is only allowed if the specific subscriber or user has given his consent after clear and extensive information according to par. 1 of article 11 of Law 2472/19974, as applicable. Subscriber or user consent may be given through appropriate settings in the web browser or through another application. The above does not prevent storage or access of any technical nature, the sole purpose of which is to carry out the transmission of a communication via an electronic communications network or which is necessary for the provision of an information society service, which has been expressly requested by the user or the subscriber. Now, for the concept of consent as well as for the other definitions of Law 2472/1997 which are used in the ePrivacy legislation (which where applied prevails as lex specialis), the GDPR definitions are applied. 7. The concept of DPA is defined in article 35 of the GDPR. Based on the GDPR, controllers must implement appropriate

measures to ensure and be able to demonstrate their compliance, taking into account, among other things, "risks of varying probability of occurrence and severity to the rights and freedoms of natural persons" (article 24 par. 1). As pointed out by O.E. of article 29 in the relevant guidelines adopted by the GDPR5, the obligation of data controllers to carry out DPA in certain circumstances should be understood in relation to their general obligation to appropriately manage the risks involved in data processing of a personal nature. Furthermore, the GDPR is a key tool for satisfying the principle of data protection by design, as defined in article 25 par. 1 of the GDPR, according to 4 See article 94 par. 2 GDPR. Now every reference to Law 2472/1997 is considered a reference to the GDPR. 5 Guidelines for Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to entail a high risk" for the purposes of Regulation 2016/679. (WP 248 rev. 01) 22 which the controller, taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and the freedoms of natural persons from processing, effectively implements, both at the time of determining the means of processing and at the time of processing, appropriate technical and organizational measures, such as pseudonymization, designed to implement data protection principles such as the minimization of the data, and the incorporation of the necessary guarantees in the processing in such a way as to meet the requirements of the GDPR and to protect the rights of the data subjects. It should be noted that in paragraph 9 of the said article 35 it is defined that "Where appropriate, the data controller shall seek the opinion of the data subjects or their representatives on the planned processing, without prejudice to the protection of commercial or public interests or the security of transactions processing." 8. With its opinion 4/2020, the Authority already examined the legality of the processing of personal data during the implementation of modern distance education procedures by primary and secondary school units, which was implemented following the no. 57233/Y1 of Ministerial Decision. Before the aforementioned Y.A. the Ministry of Education and Religious Affairs conducted an EAPD, based on article 35 of the GDPR and following a provision in article 63 of law 4686/20. The Authority deemed the modern distance education process to be legal, however, finding that the conducted EAPD has not fully examined a number of factors and risks in relation to the rights and freedoms of the data subjects. Recognizing the necessity of modern distance education, especially in cases of a pandemic, the Authority provided an opinion to the Ministry in order to address the above shortcomings and called on it, within an exclusive period of three months, to take the necessary actions to amend and supplement the EAPD and the received meters. 9. Article 37 of the GDPR introduces the obligation of public authorities to appoint a data protection officer (DPO). Based on paras 5 and 7, the

appointment 23 is made on the basis of professional qualifications and in particular on the basis of expertise in the field of data protection law and practices, as well as on the basis of the ability to fulfill the duties referred to in article 39, while the his contact details are published and communicated to the supervisory authority. In accordance with Article 38 para. 2 GDPR, the organization supports its data protection officer by providing necessary resources for the exercise of his duties and access to personal data and processing operations, as well as resources necessary to maintain his expertise. The EDPS has specified the elements that a data controller must take into account in order to be able to claim that it supports the DPO in practice6 but also to respect its independence. 10. OIELE and IOE submitted reports - complaints to the Authority, against the distance education process, arguing that it is carried out in violation of the legislation on the processing of personal data and presenting a series of arguments which are presented briefly in the history of the present case. Article 77 para. 1 of the GDPR states that "Without prejudice to any other administrative or judicial appeals, each data subject has the right to submit a complaint to a supervisory authority, in particular in the Member State in which he has his habitual residence or place of work of or the place of the alleged infringement, if the data subject considers that the processing of personal data concerning him infringes this Regulation.' At the same time, article 80 par. 1 and 2 stipulates that "1. The data subject has the right to entrust a non-profit body, organization or association (…) to submit the complaint on his behalf (…) if provided for by the law of the member state. 2. Member States may provide that any body, organization or association referred to in paragraph 1 of this article has the right, regardless of any delegation of the data subject, to submit a complaint to the competent supervisory authority in that Member State by virtue of 6 See O.E. article 29 "Guidelines on Data Protection Officers" adopted by the EDPS - section 3.2 - WP 243 rev.01 24 article 77 (…) if it considers that the data subject's rights under this regulation have been violated as a result of processing." Article 41 of Law 4624/2019 provided that a data subject may entrust the submission of a complaint on his behalf to a non-profit entity, organization, organization or association or association of persons without legal personality of a non-profit nature, but the possibility of submitting a complaint without assignment by data subject. Therefore, the documents of OIELE and IOE cannot be considered as complaints under Article 77 of the GDPR. The Authority, however, has the possibility to carry out ex officio investigations or audits for the implementation of the regulations regarding the protection of the individual against the processing of personal data (see GDPR article 57 par. 1 para. h' and kv' as well as article 13 par. 1 circular n. 4624/2019). In this case, the Authority takes into account the reports of the two federations and examines the case ex officio, to the extent it deems necessary. 11. During the 2020-2021 school year, the Covid-19 pandemic continued, while for long periods of time the

school units did not function for life, either as a whole due to a decision of their universal non-operation for reasons of public health protection, or individual school units units or departments, in accordance with sanitary protocols. In these cases, it is clear that the provision of education, which is an obligation of the state, must continue remotely, through synchronous or asynchronous education processes. Distance education delivery methods can, overall, be distinguished into asynchronous distance education and modern distance education methods. As documented by the memorandum of the Ministry of Education and Culture and the studies attached to it, the provision of modern distance education is judged to be a necessary tool for the educational process to be effective, let alone for long periods of non-operation of life education for reasons protection of public health, as the purpose of providing education does not can be effectively met by providing only asynchronous distance education. As modern distance education can only be done with electronic means that ensure two-way communication between teacher and students, which in fact requires the processing of personal data of the participants in the educational process, said processing is necessary. For the legality of the processing, compliance with the principles governing the processing of personal data must of course be ensured (Article 5 GDPR). 12. From the updated EAPD and the details of the case file (including the activities file), the following emerges in relation to the personal data processing operations carried out, through the Webex system. Specifically, from the analysis of Cisco's "privacy data sheets" and from section 2.3 of the GDPR, it follows that the following categories of data are collected during processing: A) User information data: name, email address, password, browser software (browser), phone number (optional), mail address (optional), avatar icon (optional), user information included in their folder (if synced), unique user identifier (UUID). B) Computer and usage data: IP address, User Agent identifier, hardware type, operating system type and version, client program version, network path IP addresses, user MAC address (where applicable), service version, actions taken, geographic region, meeting session information (Session Information eg day and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity), number of meetings, number of sessions with and without screen sharing, number of participants, screen resolution, connection method, performance, diagnostic and troubleshooting information, meeting host information for billing purposes (host name and ID, meeting URL, meeting start/end time), meeting title, participant information including email addresses, addresses IP, usernames, phone numbers, room device information). 26 C) User Generated Information: meeting recordings (if enabled), meeting recording transcripts (optional, only if enabled), uploaded files (for Webex Events and Training only). The compliance times are as follows for each category: a. for active subscriptions: while the subscription is active. For

expired subscriptions: Data is deleted except for Name and UUID, which is retained for 7 years as part of Cisco's business records and is retained for the company to comply with financial and audit requirements (as well as billing data). b. They are kept for 3 years, for the record related to the delivery of Cisco services. This information is used to derive analytics and to measure performance statistically but is pseudonymised. Billing information kept for 7 years.) c. This information is retained for up to 60 days after termination of service. In terms of security measures, category a and c data is encrypted during transmission and storage, while category b data is encrypted only during storage. From the information provided by Cisco, the above data is used for the following purposes: a and c. Depending on the purposes of the Cisco customer (in this case the Ministry of Health) to manage the teleconferences and to support the provision of the service by Cisco. b. The purposes are similar, except that the purpose is to improve the service provided by Cisco. Therefore, in conjunction with what is mentioned in section 2.4 of the GDPR, the following purposes and data controllers arise: Purpose 1: The provision of modern distance education, to satisfy the state's obligation to provide education, with the Ministry of Data Protection responsible for data processing and performing the edited by CISCO and ITYE Diofantos. Purpose 2: to support the provision of modern distance education, with the Ministry of Health responsible for processing and CISCO and ITYE Diofantos executors. This purpose can be considered as a sub-purpose of the 1st. Purpose 3rd: The drawing of conclusions regarding distance education, as a statistical and research purpose, with the Ministry of Health responsible for the processing and the processing carried out by 27 CISCO. Purpose 4: To improve the service provided by Cisco, for which it appears that Cisco may be the controller. Purpose 5: Cisco's compliance with financial and audit requirements, including billing for services, with a Cisco controller. 13. The main aspects of the legality of the processing in relation to the 1st and 2nd purpose, as described above, have already been examined with the opinion 4/2020 of the Authority. The legality of the processing is based on par. 1 c) (in particular with regard to the 1st purpose) and 1 e) (in particular with regard to the 2nd purpose) of article 6 of the GDPR. It is pointed out that in order to serve the purposes in question, access is made to information stored on a user's terminal equipment, which is necessary for the provision of the distance education service, which the user of the service has expressly requested. 14. In relation to the 3rd purpose, according to the Ministry of Health, the specific procedure does not include personal data processing operations excluding the initial application of the "anonymization method" and is complementary and outside the scope of the GDPR. In order to assess the legality of this activity, it is crucial to examine the applicable law. Based on the information provided by the Data Protection Authority, processing activity files and privacy data sheets, data from the user's

terminal device (e.g. browser software, IP address, User Agent ID, hardware type) are used to extract statistics , operating system type and version, client program version, network path IP addresses, user MAC address) as well as data generated during the use of the service (eg actions taken, meeting session information). As the drawing of statistical and research conclusions in relation to the distance education process is not necessary for the provision of the information society service (distance education), which is expressly requested by a user, access to the information originating from the terminal device of the respective user can only be done based on the consent of the 28 user in question. For other data, which are generated during the use of the service and collected for a different purpose than the original one, without consent or provision to ensure the purposes referred to in article 23 par. 1 of the GDPR, the legality of the processing can be established if examine the conditions of article 6 par. 4 of the Regulation. From the memorandum of the Ministry of Health, it does not appear that a detailed investigation of the legality of the purpose in question has been carried out. After all, the reference to an anonymization method is not supported by findings or data collected by Cisco. In contrast, Cisco's privacy data sheets directly refer to pseudonymization for extracting analytics and for statistical performance measurement. 15. In relation to the 4th purpose, it is clear the intention of the Ministry, especially with the contract amendments, to limit the processing in a way that leaves no room for further use. In particular, as stated by the Ministry of Health, the metadata, as well as all personal data processed in the context of distance education, excluding the data that CISCO must, according to the law, keep further, are deleted immediately as soon as the purpose is fulfilled of the contract. In this case, the special condition of the concluded contract of Cisco's general condition prevails. The Ministry of Health, as the controller, should have ensured that even during the period of operation of the distance education, no processing will be carried out with Cisco responsible, or if it is carried out, this will happen with the assurance of legality (e.g. with discrete consent, especially if taking into account that a significant part of the metadata comes from the end users' devices). Although the Ministry of Health has no influence on how Cisco uses this data, it is aware that by choosing to use the Webex Meetings application it allows the transmission of personal data of users to Cisco for company purposes. Therefore, in terms of the specific activity you should considered at least a joint controller with Cisco7.The Authority 7 See and CJEU decision in case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV 29 points out that the risk from such activity appears to be limited by the fact that the data is pseudonymised and possibly of low "risk" as it is doubtful (but not impossible) that it could be used in a way that would adverse consequences for data subjects. Based on the principle of accountability, it is up to the controller, in this case the Ministry of Health, to actively and

thoroughly examine all aspects of the processing (of transmission to Cisco and use for its own purposes) and to ensure its legality8, which it has not happened for the specific purpose. Further, individual components of the processing need clarification, such as the deletion of data at the request of the Ministry instead of automatically, after the fulfillment of the purpose of the contracts. 16. The above reasoning is applied accordingly and with regard to the 5th purpose. The reference "unless otherwise required by law" does not clarify what the applicable law is in this case. Cisco, as it appears from the privacy data sheets, states that it keeps data for billing purposes for up to 7 years, to satisfy its legal obligations. In the case of the contract with the Ministry, as the billing is not based on usage, the billing data and those related to financial and audit requirements does not appear whether or not they include application user data. Based on the principle of accountability, it is the responsibility of the Ministry of Health to actively monitor and ensure that no data is transmitted to Cisco that is not necessary for the purpose in question. 17. In relation to the principle of transparency and the provision of the required information for the processing, it is established that the Ministry has taken actions for the purpose of information but it is doubtful whether this information meets the criteria of the GDPR. The role of educational and information activities is not limited to satisfying the principle of transparency but also to a proper understanding of the risks and consequences of possible data processing during the distance learning process. An approach is therefore required 8 For the role of data controllers in relation to the principle of accountability see paragraph 3 of the recommendations 01/2020 of the EDPS in relation to the additional measures for transfers in order to ensure compliance with the level of data protection of the E.U. 30 in accordance with the OE guidelines of article 29 adopted by the EDPS in order to ensure that the information addressed to the different categories of data subjects is concise, transparent, understandable and easily accessible, with simple wording especially with regard to children. In particular, in relation to the applied methods, the following are highlighted a) The Ministry of Education correctly states that the circulars and announcements reach all teachers. However, it is common experience that an educator receives several announcements and circulars every week, therefore, informing through circulars regarding the specific group of data subjects is initially correct, but must be supplemented by providing the information during the receiving stage of data to ensure maximum efficiency. It is pointed out that the specific method of information, which does not concern other categories of data subjects besides teachers, does not seem to contain the information required by Article 13. b) The websites used provide a basic information regarding the processing, but basic information of Article 13 of the GDPR is absent. The information is structured with frequently asked questions while there is no specific link specific to personal data (which could be

differentiated appropriately for the categories of data subjects). For example, the information text9 which concerns students and parents is as follows: "In application of the New European Regulation on the Protection of Personal Data 2016/679 and Law 4624/2019), we inform you about the processing of your personal data by the Hellenic Public as represented by the Ministry of Education and Religion, as controller. Your personal data (e-mail) is subject to processing by the school unit due to your status as students and/or parents or guardians and your relationship with the Greek State, and it is necessary 9 Check on the date of the meeting - https:/ /matainoumestospiti.gov.gr/sychnes-erotiseis/ 31 for the fulfillment of the purposes and obligations of the Greek State, according to the provisions, to ensure the smooth operation of the educational activity during the period of application of the emergency measures to deal with the Covid coronavirus -19 and the ban on teaching in person. In addition, during their participation in distance education, students communicate to IT and internet service providers cooperating with the Ministry of Education and Religion, at their choice, a name or a username, exclusively in order to make modern distance teaching technically possible, through the relevant teleconferencing platform, and exclusively for as long as the above ban is in effect, and then they will be deleted by the providers in question. It is recommended that students log in via a browser (and not via an application). You have the right to receive confirmation as to whether or not personal data concerning you is being processed. In the event that your personal data is being processed, you have the right to access your personal data, obtain a copy of it, correct inaccuracies, fill in incomplete personal data, delete personal data, stop processing it, download it in a structured, commonly used and recognizable form machinery form, transferring them to another controller, without objection from the Greek State, transferring them from the Greek State to another controller, if this is technically possible, submitting a complaint to the Personal Data Protection Authority, objecting at any time to their processing for marketing purposes. For any question you have in relation to the processing of your personal data by the Greek State and/or your related rights, we remain at your disposal (e-mail contact cst@minedu.gov.gr). Therefore, the following is established: a) The contact details of the data protection officer are missing 32 b) The recipients/categories of recipients are generally described as "IT and internet service providers" without specifying their role c) There is no clarification in relation to retention of metadata, therefore the information is incomplete regarding the categories of data, purposes and retention times related to the processing of this data. d) The text is written in an unstructured way, so that the provision of the information of Article 13 of the GDPR is not clearly visible. e) The text is not easily accessible, as it is contained within frequently asked questions. Furthermore, the provision of the information prior to processing is not guaranteed. f) The text is not suitable for providing

information to children of various ages and cognitive levels. g) it is doubtful whether many parents and students visit the two websites mentioned by the Ministry. For example, the content of informational websites could be enriched with missing elements, designed to appeal to different age groups, include more detailed information, appropriate information on the student login page for the webex meetings application, informational actions within school, creating a detailed presentation in a format suitable for children but also for parents and teachers. 18. The Ministry of Health, with its memos, its actions and the updated EAPD, attempts to address a series of risks involved in the processing of personal data. The Authority, after the initial study of these elements, raised specific questions to the Ministry, in order to investigate whether specific risks have been adequately addressed, in order to minimize the possibility of their occurrence. According to the case file, identity verification is a key security measure to limit third-party access to "digital classrooms". The Ministry of Health, although it accepts its usefulness, does not appear to have provided appropriate instructions and training to its staff (the teachers), so that the control is applied in every case. The Ministry mentions specific actions (support group, education) which are correct, but do not ensure that all (or the vast majority) of teachers are properly informed about the their responsibilities. It is reasonable to argue that the majority of teachers were proceeding with some form of identity verification, but this, although it indicates that the consequences of not applying an appropriate measure are small, does not negate the obligation of the controller to provide his staff with appropriate instructions. Also, the Ministry of Health already describes the use of personal devices (by students or teachers) as a "main threat" and accepts that this risk exists. As above, the risk reduction measures, which due to the nature of the activity, must mainly include organizational measures and information and awareness actions (as Professor A rightly points out in his opinion). The Ministry of Education and Culture, as the controller, did not provide any evidence to show that such actions have been implemented in a systematic way, appropriately adapted for the groups of teachers and students. From the response of the Ministry of Health to the Authority's 1st question, it appears that the data controller failed in the issues of information and awareness. Specifically: a) No specific evidence was provided from which it follows that "identification of special measures and techniques (including training methods) to minimize the impact on the rights of data subjects" has occurred. On the platform https://t4e.sch.gr/ the program of the action "Rapid training of teachers in the implementation of distance education (holistic approach)" has been posted, which does not seem to contain issues related to the processing of 34 personal data or the above special measures. Furthermore, there is no such reference in the relevant invitation10 NSRF. b) A particularly late implementation of fast-track training, which started after January 2021, as shown by the platform, was found.

c) Voluntary implementation of training. From the statistics of the above platform11 it appears that less than 85,000 teachers of Primary and Secondary education participated in the programs, therefore the program did not cover all the teachers of these two levels12. It should be noted, however, that the implementation of the activity in question is judged to be particularly positive, as it ensures, to a satisfactory degree, the familiarization of the participating teachers with the distance education procedures and the provision of education adapted to each level. Furthermore, for the same purpose and in relation to the information and awareness actions that concern not only teachers, but also students, the Ministry had the possibility to organize informational actions, possibly also within the timetable, to enrich the timetable of the students with activities aimed at better (safer, with respect for third party personal data, actions to understand the risks, etc.) use of the new tools. Such actions would lead not only to increased transparency, but also to a reduction in the risks of the illegitimate use of personal data, which students (but also third parties) may become aware of in the context of the operation of a distance digital class. Consequently, it follows that the Ministry of Health, as the data controller, for the above reasons, does not apply, at the time of processing, appropriate technical and organizational measures for the application of data protection principles and the integration of the necessary guarantees. The applied measures are found 10 https://www.espa.gr/el/Pages/ProclamationsFS.aspx?item=4901 11 At the time of the conference 12 See https://www.alfavita.gr/ekpaideysi/335358_ekpaideytikoi-analytika-stoiheia-gia-synolo-ton-ypiretoynton-stin-protobathmia from which it follows that the number of teachers in the Primary level alone is now 88,000. 35 but in the right direction and must be completed, in a way that is available to every teacher, while it must be ensured that all teachers involved in the distance education process have received minimal information to ensure the reduction of risks. 19. In relation to the involvement of the data subjects provided for in article 35 para. 9 of the GDPR, the EDPS considers that the opinions in question could be requested by various means, depending on the context (e.g. with a general study that related to the purpose and means of the processing operation, by querying employee representatives or by routine inquiries sent to the controller's future clients) ensuring that the controller has a lawful basis for processing the personal data at stake when the requested due opinions. It should be noted that consent to processing is obviously not a means of seeking the opinion of data subjects. The Ministry of Health maintains that the opinion was formulated during the implementation of statutory procedures and that it was decided to carry out an investigation in collaboration with the IEP, which is ongoing. In the above provision of the GDPR reference is made to "...opinion of the data subjects or their representatives on the planned processing...". Therefore, the expression of

opinion is, primarily, meaningful in the initial stages of the GDPR and after the basic characteristics of the processing, the possible risks, the relevant consequences and the corresponding reduction measures have been made known to the affected persons. The GDPR does not define the process of obtaining an opinion, but leaves the controller free to organize it as he deems most efficient. In this particular case, however, the formal meetings cannot be considered as part of the process of expressing the opinion of the subjects. And this as the characteristics of the processing and the identified risks had not been made known in the meetings for a sufficient period of time, nor was it proven that there was a discussion, presentation or explanation of the risks during the meetings. Furthermore, no relevant procedure was implemented during the review process of the EAPD. The reference to a research in collaboration with the IEP, is based on a decision of the Board of the IEP during its meeting on 18/03/2021 (more than three months after the completion of the 36 EAPD) for the approval of a research entitled "Investigation of the effects of removal from live teaching and the application of distance education, to students and teachers, of primary and secondary education, due to the COVID-19 pandemic". The purpose of the investigation, as well as its object, does not appear to concern issues of dealing with risks related to the processing of personal data, while, even if it were accepted that the investigation, even incidentally, has included the issues of the EAPD, the date meeting proves that it does not meet the requirement to identify risks in the early stages, nor is there any evidence linking the EPPO to the conduct of the investigation. As the Authority had already pointed out with opinion 4/202013, the involvement of the data subjects, who are directly or indirectly affected, is necessary, it results in increased transparency and ultimately, it can lead to increased trust of the data subjects in the operations processing. As it is established that no actions were taken in this direction14, it follows that the data controller violated the obligation of article 35 par. 9 of the GDPR. 20. Article 46 of the GDPR states that "1. In the absence of a decision pursuant to Article 45(3), the controller or processor may transfer personal data to a third country or international organization only if the controller or processor has provided appropriate safeguards and provided that they are enforceable rights and effective remedies for data subjects. 2. The appropriate guarantees referred to in paragraph 1 may be provided for, without requiring a specific authorization from a supervisory authority, by means of: (…) b) binding corporate rules in accordance with Article 47, c) standard data protection clauses issued by the Commission in accordance with with the examination procedure provided for in Article 93 paragraph 2, (…)". 13 See section 2.2 section B of opinion 4/2020 (pp. 18-20) 14 On the contrary, it appears that there was involvement of experienced entities and experts 37 In the recent decision of C-311/18 (Schrems II), the CJEU pointed out that the above provision must to be interpreted in conjunction with Article 44 of

the GDPR, which aims to ensure that the level of protection of personal data guaranteed by the GDPR is not undermined, regardless of the country to which it is transferred and regardless of the provision based on which the transmission15. The Court clarified that the level of protection in third countries does not it needs to be identical to that within the EEA but substantially equivalent16. Standard contractual clauses, as a transfer tool, are intended to provide EU-based data exporters with contractualguarantees applied uniformly in all third countries17. However, as pointed out by the Court18, due to their inherent contractual nature, standard contractual clauses bind the contracting parties and not the third country authorities and, therefore, additional measures may be required to ensure that the required by EU law level of protection. The Court further states19 that data exporters (controllers or processors) are responsible for checking, on a case-by-case basis and, where necessary, in cooperation with the importer in the third country, whether the legislation of the third country affects the effectiveness of the appropriate safeguards that provided by the transmission tools of article 46 GDPR. In cases where third country legislation does not ensure the protection of personal data transferred as required by EU law, the Court leaves open the possibility for data exporters to implement additional measures which ensure the level of protection required by EU law EU. Exporters should specify these measures on a case-by-case basis. This is consistent with the principle of accountability of article 5 par. 2 GDPR20. 15 See Decision C-311/18 (Schrems II), Sk. 92, 93 16 Ibid. sc. 94. 17 Ibid., sk. 133 18 Ibid., sk. 133, 125. 19 Ibid., sk. 134, 135 20 See Supplementary Measures Recommendations 1/2020, p. 9. 38 Looking at the processing activities in this particular case and in relation to the issue of data transfer outside the EEA, from Cisco's Privacy Data Sheets for Webex Meetings (section 3, version 4.6 – Apr 2021) it appears that "user generated information" is kept only in Europe. However, Class A and Class B information (user information data including billing data and computer and usage data) is held in the US. The Ministry states that Cisco uses various mechanisms to secure data transfers to countries outside the EU. and refers specifically to binding corporate rules (which, according to the Authority's investigation, have been approved by the Dutch supervisory authority, but do not relate to the data processing activities in question, nor can they be applied to the Ministry of Health, but only to data transfers between companies belonging to the Cisco group) and standard data protection clauses issued by the European Commission. In this case, although the Ministry of Health does not point it out in its memorandum, only the standard contractual clauses included in the respective "MASTER DATA PROTECTION AGREEMENT" which is an integral part of the contracts for free concession of the Webex platform may be applicable. Based on these clauses, it appears that data is being transmitted from the Ministry of Health, as a controller, to the US-based Cisco.

The processing activities are specified in the annex to the clauses in the following sub-purposes: registering the customer to the service, displaying a user's avatar image to other users, providing support, understanding how it works, diagnosing technical issues, improving the service by analyzing aggregated data, responding to customer requests, provision of optional components of the service, quality monitoring of the service, analysis of the service. It is clear that the Cisco company (in this case the group and its companies) is subject to US law, therefore, in principle, an adequate level of personal data protection is not ensured. Therefore, each transmission must be considered individually for its legality. In the EDPB's recommendations on the 39 additional measures for international transfers to ensure compliance with the EU21 data protection level, para 43.3 states that the controller's assessment may reveal that the relevant legislation in the third country is problematic22 and that the transmitted data and/or the data importer falls or may fall within the scope of this legislation. In view of the uncertainty regarding the potential application of the legislation in question, the exporter may then decide to: Suspend the transfer or implement additional measures to prevent the risk of the potential application to the importer of the data or the transferred data of legislation or practices in country of the importer, which may affect the contractual guarantees of the instrument of transmission which attempt to ensure an equivalent level of protection to that of the EEA. Alternatively, the exporter may decide to proceed with the transfer without implementing additional measures if it considers that there is no reason to believe that the legislation in question will in practice be applied to the transferred data or the importer. The exporter is required to be able to demonstrate and document through its assessment, where appropriate in cooperation with the importer, that the third country law in question is not interpreted and/or applied in practice in a way that captures the transmitted data and the importer, also taking into account the experience of other entities operating in the same field and/or related to similar transmitted personal data and the additional sources of information described in paragraphs 45 – 47 of the text of the EDPS recommendations. 21 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – version 2.0 – 18/6/2021 22 Based on the guidelines of the EDPS, problematic legislation is that which 1) imposes on recipient of the personal data obligations and/or affects the data transmitted, in such a way that it can affect the contractual guarantees of the transmission tools which ensure a substantially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognized by the Charter of Fundamental Rights of the EU or goes beyond what is necessary and proportionate in a democratic society to ensure one of the important objectives also recognized in the law of the Union or the Member States, such as those referred to in Article 23

para. 1 of GDPR. 40 In this particular case, such an in-depth study is absent. The reference that "CISCO HELLAS A.E." contractually undertook not to transmit outside EE/EOX the personal data it processes on behalf of the Ministry without prior notification, it simply repeats the obligation of the law, without providing evidence for the non-application of US legislation23. Reference is made to an assessment by the CISCO Group (based in particular on standard contractual clauses and binding corporate rules transfers which ensure the application of the rights of the subjects and in which the protection measures and the assurance that to date never a request for the provision/disclosure of data has been submitted to the US-based companies of the Group) but which has not been provided, while it is clear that the binding corporate rules are not applicable in the case under consideration. The reference to an assurance that to date no request for the provision/disclosure of data has ever been submitted to the US-based companies of the Group is insufficient24, while it is not substantiated by information that is available, publicly or in another verifiable way. Therefore, the Ministry must demonstrate and document with a detailed report that the legislation in question will not be applied in practice to the transferred data and/or to the importer and, consequently, that this legislation will not prevent the importer from fulfilling its obligations which derive from article 46 of the GDPR. Furthermore, during this study the Ministry must also examine the manner in which data transfers outside the EEA are ensured following the adoption of Executive Decision (EU) 2021/914 of the Commission of June 4, 2021 "regarding standard contractual clauses for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council". It is pointed out that based on Article 4 of the decision in question, Decisions 2001/497/EC and 2010/87/EU are repealed from 23 The CJEU in the Schrems II decision has already expressed concern about Article 702 of the Foreign Intelligence Surveillance Act) and Executive Order 12333, see sc. 184, 192, 195 ff. 24 See Recommendations 1/2020 on Supplementary Measures, p. 19, para. 47. 41 27 September 2021 and contracts concluded before 27 September 2021 based on these decisions are considered to provide adequate guarantees until 27 December 2022, under condition that the processing operations that are the subject of the contract remain unchanged and that the invocation of these clauses ensures that the transfer of personal data is subject to appropriate safeguards. 21. The issue of the independence and the adequacy of resources of the Ministry's DPA does not concern only this specific case. In order for the Authority to judge whether there is a question of independence, a more specific audit is required, which is not related to the legality of processing during distance education. With regard to the resources of the Ministry of Foreign Affairs, in principle it must be accepted that one person as Minister of Foreign Affairs is not sufficient for the Ministry of Health. This has already

been accepted by the Ministry, which as of September 2020 has prescribed a new operating model of the Ministry of Education, through links to the regional directorates of education. This model seems to be more efficient and although it is not examined in this paper, it is advisable to speed up the actions to strengthen the role of the Ministry of Foreign Affairs. Consequently, as the issues of personal data processing during modern distance education are primarily examined in this particular case, the examination of the issues of independence and adequacy of resources of the DPO must be separated. And this as a more specific control is required that takes into account the organizational structure of the Ministry, the number of employees and data subjects, the services and electronic applications it offers to natural persons, the resources it provides to the Ministry of Foreign Affairs for the supervision of its activities, the way , with which the responsibilities of the Ministry of Foreign Affairs are exercised in practice. With regard to the declaration of the Ministry of Foreign Affairs to the Authority, it was made late (with document no. prot. C/EIS/1821/14-03-2021), the delay, however, is only a formal omission, as it is clear from the data of the assumption that the specific DPO was appointed from May 2020, to replace the initially designated DPO, while there have been communications of the DPO with the Authority for different cases (indicatively, as a point of contact in the context of data breach notifications). However, as has already been pointed out above in paragraph 17 during the examination of the 42 requirements to satisfy the principle of transparency, on the website of the Ministry there is an essential omission consisting in the lack of specific information in relation to personal data (policy) and reference to contact details of the Ministry of Foreign Affairs. Such reports exist in relation to more specific applications or websites of the Ministry25, which, however, do not cover the obligation arising from article 37 paragraph 7 of the GDPR. 22. In view of the above considerations, the Authority considers the following: a) in relation to the issues of legality of the processing of personal data, as set out in particular in paragraphs 11 to 16 hereof, it is established that the Ministry has violated the provisions of the article 6 of the GDPR, in conjunction with article 4 par. 5 of Law 3471/2006, as applicable. Specifically, in relation to the purposes 3, 4 and 5 referred to in the said paragraphs, it finds access to information stored on a user's terminal equipment in violation of article 4 par. 5 of Law 3471/2006, and that it has not been carried out detailed investigation of the legality of said purposes, so that its legality can be documented based on Article 6 of the GDPR. With regard to the violation in question, the Authority considers that, at this stage, the effective, proportionate and deterrent measure to deal with the violation in question is, based on Article 58 para. 2 b GDPR, to issue a reprimand to the Ministry of Health and at the same time instruct it, based on Article 58 para. 2 d of the GDPR, to make the processing operations compliant with the provisions of the GDPR, dealing with the violations analyzed in

paragraphs 11 to 16 of this within a period of two months from the delivery of the decision. After this period, the Ministry of Health must have ensured that it obtains consent for access to information stored on a user's terminal equipment, when this is not necessary for the provision of the service requested by the user, and has documented in detail the legality of processing purposes numbered 3 to 5. 25 For examples, see https://smsresults.minedu.gov.gr/panelladikes_sms_2021_proswpika_dedomena.pdf, https://edutv.minedu.gov.gr/index.php/profil-menu/videos/pnevmatika-prosopika, https://www.minedu. gov.gr/publications/docs2019/5. Processing_Data_of_Personal_Character.pdf, 43 b) in relation to the issues of transparency, as analyzed in paragraph 17 of this document and with regard to the announcement of PYD data, in paragraph 21 of this document, it is established that the Ministry has violated the provisions of article 13, in combination with article 5 para. 1 a GDPR, article 12 and article 37 para. 7 GDPR. In particular, it is found that the information provided is less than what is required by the GDPR, that the information is not in an understandable and easily accessible format and that clear and simple wording is not used, especially taking into account that this is information also addressed to children. With regard to the violation in question, the Authority considers that at this stage, the effective, proportional and deterrent measure to deal with the violation in question is, based on Article 58 para. 2 b GDPR, to issue a reprimand to the Ministry of Health and at the same time instruct him, based on Article 58 para. 2 d GDPR, to make the processing operations compliant with the provisions of the GDPR, dealing with the violations analyzed in paragraph 17 hereof and modifying the procedure and the content of the provided information within a period of two months from the service of the decision. c) In relation to the risks involved in the specific processing of personal data as analyzed in paragraph 18 hereof, it is established that the Ministry has violated the provisions of article 25 paragraph 1 of the GDPR, as the technical and organizational measures taken do not adequately protect the rights of data subjects. With regard to the violation in question, the Authority considers that, at this stage, the effective, proportionate and deterrent measure to deal with the violation in question is, based on Article 58 para. 2 b GDPR, to issue a reprimand to the Ministry of Health and at the same time instruct it, based on Article 58 para. 2 d GDPR, to make the processing operations compliant with the provisions of the GDPR in the manner analyzed in paragraph 18 of this within a period of two months from the service of the decision . d) In relation to the expression of opinion of the data subjects or their representatives on the planned processing, it is established that the Ministry of Health violated the obligation of article 35 paragraph 9 of the GDPR. Regarding the said 44 violation, the Authority considers that, at this stage, the effective,

proportionate and deterrent measure to deal with the said violation is, based on Article 58 para. 2 b GDPR, to address a reprimand to the Ministry of Health e) In relation to the issue of data transfer outside the EU, as analyzed in paragraph 20 hereof, it is established that the Ministry of Health has violated the obligations of Article 46 of the GDPR, as no assessment of the transfer has been carried out in the manner described in said thought. With regard to the violation in question and taking into account the very recent relevant guidance of the EDPS, the Authority considers that, at this stage, the effective, proportionate and deterrent measure to deal with the violation in question is, based on Article 58 par. 2 b GDPR, to address a reprimand to the Ministry of Health and at the same time instruct it, based on article 58 par. 2 d GDPR, to make the processing operations compliant with the provisions of the GDPR, dealing with violations in the manner analyzed in paragraph 20 hereof, within a period of four months from the service of the decision. The Authority: FOR THESE REASONS A. Addresses the Ministry of Education and Religious Affairs: a) Reprimand for violations of the provisions of article 6 of the GDPR, in conjunction with article 4 paragraph 5 of Law 3471/2006. b) Reprimand for violations of the provisions of article 13, in conjunction with article 5 para. 1 a of the GDPR, article 12 and article 37 para. 7 GDPR. c) Reprimand for violations of the provisions of article 25 par. 1 of the GDPR. d) Reprimand for the violation of article 35 par. 9 of the GDPR. e) Reprimand for violations of the provisions of article 46 of the GDPR. 45 B. Instructs the Ministry of Education and Religious Affairs, as controller, to make the processing operations in accordance with the provisions of the regulation and specifically as follows: 1) within two (2) months from the receipt of this: a) Deal with the violations of provisions of article 6 of the GDPR, in combination with article 4 par. 5 of Law 3471/2006 in the manner analyzed in paragraphs 11 to 16 hereof. b) Deal with violations of the provisions of article 13, in conjunction with article 5 par. 1 a GDPR, article 12 and article 37 par. 7 GDPR, as analyzed in paragraphs 17 and 21 of present, modifying its procedure and content

information provided

c) Deal with violations of the provisions of article 25 paragraph 1

of the GDPR in the manner analyzed in paragraph 18 hereof.

2) within four (4) months of receipt of this address

the violations of the provisions of article 46 of the GDPR in the manner that

is analyzed in paragraph 20 hereof.

After the expiry of the respective deadline, the Ministry must inform

the Authority for its compliance.

The president

The Secretary

Konstantinos Menudakos

Irini Papageorgopoulou