Athens, 01-11-2022 Prot. No.: 2769 DECISION 61/2022 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via teleconference on 28-

06-2022, in order to examine the case referred to in the present history. Konstantinos Menudakos, President of the Authority and regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, Charalambos Anthopoulos as rapporteur, Christos Kalloniatis, Aikaterini Iliadou and Grigorios Tsolias were present. At the meeting, without the right to vote, the auditors Kalliopi Karveli, Fotini Karvela, expert legal scientists and George Rousopoulos, expert IT scientist, attended the meeting, as assistants to the rapporteur, and Georgia Palaiologou, an employee of the Department of Administrative Affairs, as secretary. The Authority took into account the following: The Authority, with decision 50/2021, examined, ex officio, the compliance of the Ministry of Education and Religious Affairs (hereafter Ministry of Education) with the recommendations of opinion 4/2020 on the compatibility of modern distance education in its school units primary and secondary education with the provisions of the legislation on the processing of personal data. In the context of the case, the updated Data Protection Impact Assessment (hereinafter DPA) was examined as well as the compliance actions of the Ministry of Health. The Authority found deficiencies in five points imposing a reprimand for each deficiency, while in regard to four of these points, instructed the Ministry to address the deficiencies in the manner detailed in the decision within a specific period of time (two months for the first three deficiencies and four months for the fourth) in order to eliminate the violations: In summary, the deficiencies that the Ministry had to address , were as follows: 1) No detailed investigation of the legality of processing purposes has been carried out by the Ministry, in particular in relation to consent to access information stored on a user's terminal equipment, when this is not necessary for the provision of the service requested by the user. 2) The information provided to the data subjects is less than that required by the GDPR, while this information is not in an understandable and easily accessible form with clear and simple wording, especially if it is information addressed to children. 3) The implemented security measures, although they are in the right direction, must be supplemented, 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 a minimum of information. 4) No proper assessment of data transfer to countries outside the EU has been carried out. especially if the decision of the CJEU in case C-311/18 (Schrems II) is taken into account. The Ministry informed the Authority of its actions with two memorandums, before the end of the two or four month period (G/EIS/312/14-01-2022 and G/EIS/4490/17-03-2022 respectively) while in the meantime he had provided information with his documents No. C/EIS/1658/02-02-2022 and C/EIS/2984/01-03-2022. Based on these documents, the responses of

the 2nd Ministry on the issues in which it had to comply with the Authority's decision are presented below. Issue 1: Analytical investigation of the legality of the processing purposes (paragraphs 11 to 16 of Decision 50/2021) The Ministry of Health provides evidence for the documentation of processing purposes 3, 4 and 5, which were deemed not to have been properly documented. Specifically, with regard to each of the three purposes of processing for which it was judged that an analytical investigation of legality had not been carried out, it states, in summary, the following: Regarding the 3rd purpose (drawing conclusions about distance education, as a statistical and research purpose , with YPAITH responsible for processing and CISCO performing the processing) YPAITH, in the capacity of "administrator", had access to all the metadata collected by CISCO during the provision of the service. This metadata included both data originating from users' terminal equipment and information generated during the use of the service. The aforementioned metadata was accessed on behalf of the Ministry of Education by authorized employees of the Institute of Computer Technology and Publications-"Diofantos" ("I.TY.E.-DIOFANTOS"), who had undertaken the publication of statistics in relation to distance education. The persons in question prepared a daily report in the form of an "xls" file, which contained the following statistics by level of education: a. Number of registered users. b. Number of conference calls held. c. Total video conference duration in minutes. d. Number of teachers who made at least one teleconference. e. Number of student connections in video conference. f. Average duration of teleconferences in minutes. 3 g. Average number of video conference participations. The above statistics were deemed necessary to draw conclusions regarding the provision of distance education in accordance with article 68 par. 2 of Law 4686/2020. The Ministry also provides an xls format file with the above statistics. Regarding the 4th purpose (improvement of the service provided by Cisco, for which it appears that Cisco may be the controller), the Ministry of Health states that "to clarify the roles, it has already been pointed out (...) that CISCO has contractually assumed the commitment not to process personal data for purposes beyond the performance of the contract, i.e. beyond the (technical) operation of the distance learning platform. In particular, in all the contracts concluded between the Ministry of Health and CISCO it is expressly provided that the second contracting party "...is not allowed to make any use of the personal data that will be made available for the implementation of this Agreement, which deviates from its purpose... Furthermore, however, to confirm the above, documentation requested by CISCO (see Ref. 2) is provided, from which it appears that the contractual prohibition in question supersedes any other terms that may be included in Privacy Policies or other documents of CISCO. In relation to the contracts concluded between the Ministry of Foreign Affairs and CISCO, it is provided that "...unless otherwise specified herein, the

provisions contained in the Personal Data Protection Annexes shall apply". This statement states that CISCO processes personal data in accordance with applicable laws and the contractual obligations provided for in the Master Data Protection Agreement dated March 13, 2020 and the agreement for the free trial of the Cisco Webex video conferencing platform for the implementation of the modern ex of distance education in the educational system dated November 9, 2020, as amended on December 4, 2020 ("we confirm that Cisco processes personal data in accordance with applicable statutory laws and contractual commitments made 4 in the Master Data Protection Agreement dated 13th March 20001 and the Agreement for the Free Trial of the Cisco Webex teleconferencing platform for the realization of modern distance learning in the educational system dated 9th November 2020, as amended 4th December 2020"). With regard to the 5th purpose (Cisco's compliance with financial and audit requirements, including the billing of services, with Cisco as the data controller), the Ministry of Health states: "the legal obligations to fulfill which it holds such data derive from the legislation of Netherlands. For confirmation, after the Decision, the Ministry of Health addressed CISCO requesting further clarifications in relation to the applicable provisions and the specific data that must be kept pursuant to them. With its reply of 13.01.2022 (see Ref. 2), CISCO confirms that the relevant financial / fiscal and audit requirements are provided for in paragraphs 1 to 4 of Article 52 of the Dutch General National Taxation Act ("Algemene wet inzake rijksbelastingen") and that the data retained in compliance with this legislation is limited to the following: 1) name and email address of the host (host), 2) URL of the video conference, 3) start/end time of the video conference, and 4) telephone number (where used).' Issue 2: Lack of information provided to data subjects - not understandable and easily accessible format, especially for children (paragraphs 17 and 21 of decision 50/2021) The Ministry of Health states, with its first memorandum, that it has taken the following actions to amend the procedure and the content of the information provided: "i. He drafted a new information text, which is structured in two chapters: a) to inform teachers and b) to inform students and their parents/guardians regarding the processing of personal data in the context of distance learning. Each chapter is structured in sections, so that 1 Obviously 2020 is meant 5 the information required according to article 13 GDPR is provided in a distinct manner. And the second chapter is written in a particularly simple and understandable language, so that it is understandable for students and their parents/guardians (see Ref. 3). The text in question has already been posted on the website with the domain name www.matainoumeasfaleis.gov.gr/tilekpedefsi, which has been developed and operates for the purpose of providing information about distance learning. In addition, it has been launched to post it on the official website of the Ministry of Education and Culture, as well as on the "webex.sch.gr" website of the Panhellenic School

Network. ii. A pop-up window was developed in collaboration with CISCO, which will appear when users log in to the e-learning platform. The window in question will include brief information about the processing of the personal data of the users of the distance learning platform and will refer to the above (under i) written information (see Ref. 4). iii. Audio-visual material (video) was created through which students will be briefly informed about the processing of their personal data during the provision of distance education (see Ref. 5). The material in question will be posted on the website www.matainoumeasfaleis.gov.gr and on the PSD. In relation to the above point iii, with the second memorandum, the Ministry of Health informs that an informative video for students has been posted on its channel on the YouTube application, while it is also accessible from the website https://matainoumeasfaleis.gov.gr/tilekpedefsi/. From the monitoring of the relevant websites, it appears that the video addressed to the students includes an information section in relation to the processing of personal data, although it focuses more on the safe use of distance education. In relation to point ii, it is pointed out that the pop-up was not finally implemented, but when students log in (through the URL is done through the proposed process 6 https://webex.sch.gr/students.php) there is an easily accessible hyperlink to information regarding the processing of personal data. Furthermore, it is observed that on the above website, during the time of the conference, an informative message appears in relation to cookies which states "We only use functional cookies to provide the services on our page. If you continue to use the page, we will assume that you are satisfied with this Learn more" and with the only possibility to select "Accept necessary cookies". The last two websites https://www.sch.gr/aboutcookies where words refer to the provision of detailed information in relation to the cookies used by the Panhellenic School Network (PSD) and the websites hosted on it. Question 3: Improvement in the applied security measures (paragraph 18 of decision 50/2021) The Ministry of Health, with its first memorandum, informed the Authority that in order to limit the risks related to identity verification and in particular to the use of personal devices, measures have been implemented / the following measures are being implemented: "a) I.TY.E.-"DIOFANTOS" provides the entire educational community with information regarding the use of personal devices for educational-service purposes within the framework of the operation of the Panhellenic School Network (PSD). b) As can be seen from the text of the 7.12.2020 updated EAPD Study of the YPAITH and all the relevant documents that have been submitted to the Authority, in each school unit a support group for teachers during distance education has been established, which consists of the Director and by at least one teacher with specialized digital skills (e.g. IT teacher PE86, ICT level B trainer, etc.). Furthermore, on a second level, a user support service ("Help Desk") of the PSD operates. 7 c) Already with the 7.12.2020 updated EAPD Study of the Ministry of Health, it was

proposed and approved as a measure to eliminate the risks from the use of personal devices for official purposes, the issuance of instructions in accordance with the Guidelines of the APDPH for the protection of data during telecommuting. In this regard, the Ministry of Education proceeded with the creation of audio-visual material for teachers, which will be posted on the website with the domain name www.matainoumeasfaleis.gov.gr and in the PSD (see Ref. 6)." In relation to the above point c, with the second memorandum the Ministry of Education and Culture informed that an informative video for teachers was posted on its YouTube channel, which is also accessible from the website https://matainoumeasfaleis.gov.gr/tilekpedefsi/. From the monitoring of the relevant web pages, it appears that the video focuses on the safe use of distance education. At the same time, with its initial memorandum, the Ministry of Education and Culture informed that on 10.01.2022 it submitted a request to the Institute of Educational Policy (IEP), in order to carry out awareness-raising actions for both teachers and students within the timetable of the program and with the following object: i) The full familiarization of the students and teachers / members of E.E.P. – E.V.P. with the tools of distance education. ii) The provision of basic information on the security of, as the case may be, personal or official electronic devices used by students and teachers/members of E.E.P. – E.V.P. during distance learning. iii) The provision of basic information and instructions for safe internet navigation and the use of the e-learning platform. iv) The provision of basic advice for the protection of privacy when using the e-learning platform and when implementing the online courses. As can be seen from the second memorandum of the Ministry of Health, the IEP approved the said request and on 20.01.2022 with a letter from G.G. Primary and 8 Secondary Education and Special Education were sent to the teachers (with a signed notification) a guide prepared by an IEP consultant on the subject: "Definition of the framework of action plans in school units of Pre-school and Special Education for the safe use and pedagogical utilization of digital distance learning tools and the Internet". Issue 4: Data transfers outside the EU (paragraph 20 of decision 50/2021) With its first memorandum, the Ministry of Health informed that it is in communication with CISCO and is monitoring the actions it has taken in compliance with its regulatory obligations in relation to cross-border transfers and in particular for the preparation study (in accordance with ESDP Recommendations 01/2020) on whether specific US legislation is applicable in the case of the data of users of the e-learning platform and whether an adequate level of protection of said data is ensured. At the same time, he stated that with the completion of the above study, the Ministry of Health and Welfare and CISCO will proceed to conclude a new contract, which will include the provisions contained in Executive Decision (EU) 2021/914 of the Commission of June 4, 2021. In this contract, attached as an Appendix a special and updated "privacy data

sheet", which will supersede the corresponding general documents of CISCO and will describe in detail the conditions of the processing carried out during the provision of distance education. updated according to contractual clauses Initially, the Ministry of Health, both in this memorandum and in its second one, raised an issue regarding its characterization as a "data exporter". It states that it transmits data exclusively to its counterparty "CISCO HELLAS SA" for the purpose of implementing the courses through the specially configured platform. Any onward transmission is carried out by this company "in-person" using the GDPR's transmission tools (standard contractual clauses, binding corporate rules and code of conduct). CISCO HELLAS SA, as a subsidiary of the CISCO group, transmits data to its parent company based in the USA. for the purpose of executing the 9 contracts it enters into, due to the technical operation of the distance learning platform and for invoicing reasons. The specific purposes and essential means are determined by the companies of the CICSO group, therefore they must be considered as controllers subject to the provisions of Chapter V of the GDPR. Reference is even made to a relevant example (with no. 13) of the Danish supervisory authority's guidance text2. Then, in relation to its obligations as derived from the "Schrems II" decision of the CJEU, the Ministry of Health states the following: It asked CISCO HELLAS for assistance in the preparation of a study for the assessment of the risk of the transfers carried out (Data Transfer Impact Assessment - hereinafter DTIA) so that on this basis a new contract can be concluded with the new standard contractual clauses. CISCO accepted the request and it was agreed that the process should be completed within the month of April 2022 (earlier than the deadline set by the EU Commission, which expires on 27/12/2022). On 11/3/2022 it was submitted by CISCO to the DTIA Ministry of Health according to a standard proposed by a member of the International Association of Privacy Professionals IAPP3. The content of the study was a product of collaboration withthe Ministry of Health

The study recognizes two processing purposes, a) the technical function

of the distance learning platform and b) the pricing. CISCO has its status

electronic communication service provider, therefore rated as

possible application of the provisions of Article 702 of FISA4. Therefore,

2

https://www.datatilsynet.dk/Media/637824108733754794/Guidance%20on%20the%20use%20of%2

0cloud.pdf

"Example 13 A Danish company uses a CSP based in the EU for hosting its CRM system. The CSP is a

subsidiary of a US parent company. According to the data processing agreement, the CSP processes certain types of metadata which are personally identifiable for its own purposes (such as capacity planning, security management and service improvements), including transfers the data to its US parent company. The CSP is considered a controller for its processing of the data for the above-mentioned purposes and is therefore itself responsible for complying with Chapter V of the GDPR in respect thereof transfer of the data to the US. Note that in this case, prior to engaging the CSP for the processing activity, the Danish company must assess on which legal basis it may disclose the relevant metadata to the CSP for the CSP's processing of the data for its own purposes".

3 https://iapp.org/resources/article/transfer-impact-assessment-templates/

4 Foreign Intelligence Surveillance Act US law

the effectiveness of (new) contractual clauses as a tool was evaluated

transmission. The Ministry of Health states that in the group's publicly accessible document

CISCO, which was posted following the above decision of the CJEU, is mentioned

that “Neither CISCO nor our Customers and Partners are personally managed

data that could be of interest to their intelligence services

USA. (eg information important to US national security). Not

we engage in processing activities or transmissions that display them

risks related to privacy and mass surveillance, which

engaged the CJEU in 'Schrems II' (eg consumer communications and

consumer behavior). The personal data submitted to

processing by CISCO does not actually involve a tracking risk

on behalf of the services of the U.S. and arbitrary interference with fundamentals

rights and freedoms of Subjects within the EU"5. To ensure

adequate level of protection of personal data during transmission to

parent company of the CISCO group in the USA. the following measures are taken:

a) Encryption is performed during end-to-end transmission.

b) Encryption is performed on storage.

c) A no backdoor policy has been established

policies).

d) It is possible to carry out checks or inspections of

of CISCO processing facilities by the exporters and, by extension, by

the Ministry of Health and its authorized advisors.

e) The Ministry of Health is informed of any access request submitted

by US public authorities

f) CISCO undertakes to review on a case-by-case basis, in accordance with law

of the United States, the legality of any order to disclose data.

5 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-faq-intl-

transfer-personal-data-post-schrems-II.pdf

g) Increased transparency is envisaged, as CISCO makes it available

Ministry of Health at least once every six (6) months reports on the requests that

submitted by the US authorities.

h) CISCO adopts the current best practices in relation to

cross-border transfers and access to the transferred data

(access controls and provision of training to executives are indicated as examples

of the Group companies).

The Ministry of the Interior and CISCO are in the process of negotiating a new one

contract, in which (in addition to the new standard contract clauses) it will

add conditions for the implementation of the above measures (which were judged not to

contradict the clauses and are sufficient to ensure the level

protection guaranteed by

GDPR). Furthermore, they have been proposed to

contracting companies with CISCO to take the following measures:

a) Encryption: It will be carried out in relation to all

them

teleconferences. The encryption algorithm and parameterization

of this will be strong against cryptanalysis performed by

the US Authorities. The encryption keys will be kept

solely under the control of CISCO.

b) Transparency: The prepared DTIA will be an appendix to the contract.

CISCO will submit a report to the Ministry of Health every six months (see above). In

case where the provision of specific information is contrary to

provisions of the legislation of the USA. CISCO will take into account the Ministry of Foreign Affairs

sufficient statistical data.

c) Regular evaluation of supplementary measures: The contracting parties

they will undertake to cooperate at least twice a year

for the evaluation of the measures. In case of changes in the relevant legislation

of the USA an extraordinary reassessment may take place.

Finally, the contract will provide a condition for the abolition of transfers to

third countries until July 2022. CISCO has assured that until then, all

the data processed during the operation of the platform

distance learning will be hosted on servers within the EU. and specifically in

Germany, as part of the company's "EU RESIDENCY" program.

With its second memorandum, the Ministry of Health also submitted the copy of the DTIA

which CISCO HELLAS SA forwarded to her. This includes, among others,

following:

Data exporter is CISCO HELLAS A.E.

Data importer is Cisco Systems Inc.

Context and purpose of transmission: Although the majority of personal

data is stored in the EU, for the provision of the "WebEx

Meetings" Cisco must transfer some personal data to the US.

as shown below.

of the host

Data categories: information

(Host) and

user information about the application's billing and operation;

They include: IP address, User Agent Identifier, network IP addresses,

MAC addresses of user devices, geographic region, information

participant (email, IP, username, phone), Host and user information

(name and email), session URL, session start and end time.

Technical implementation of the transfer: Standard contractual clauses with

additional measures.

and

Technically

are presented

https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1604543381171981

policy.

organizationally

meters:

in the

as

From the overall estimate, the total probability of occurrence is calculated

even a successful transfer of personal data to the authorities

of the USA in violation of data protection principles is 5.4% against

the considered period (until 31/7/2022). CISCO estimates that the residual

risk from the transfer is small and that the transfer is permitted, based on

data protection legislation.

13

The Authority proceeded with an investigation to establish in what way

addresses the issue of the application of Chapter V of the GDPR by companies

that provide similar/competing services to its Webex service

Cisco, which is basically a video conferencing service and which can

it is used in the context of various activities of many and different

nature of bodies. In particular, in the near future (17/03/2022) Zoom Video

Communications, Inc. introduced DTIA6 (and soon after EAPD) for services

of Meetings, Webinar, and Chat. For the purposes recognized in said

DTIA the estimate was as follows: Content (data center within EU) 0.0%,

Account (US) 0.05%, Support (US): 0.38%, Diagnostics (US):

0.65%, Trust & Safety Group (USA): 2.7% etc. The Government of the Netherlands together with

universities of the country conducted EAPD7 and DTIA8 (on 25/02/2022) for the

use of the company's applications Microsoft Teams, OneDrive and SharePoint

Online, in which six (6) sources of risk are identified in relation to the Fund

V of the GDPR, and measures are presented to limit the risks.

In these two organized DTIAs a similar methodology is followed and,

as in the case of CISCO, its legitimacy is assessed

processing in relation to the possible consequences for data subjects

from any cross-border data flow. The calculated probabilities

of transmission arise with qualitative criteria and assessments and are not easy

comparable. But a common feature is that for some purposes

processing (e.g. diagnostic data) the possibility of cross-border flow

data is not zero, although it is estimated to be very small. In all three DTIAs,

the acceptance that the processing is lawful is done on the basis of the admission that it is

safe to process as highly unlikely, but no

impossible, for there to be a cross-border flow of data which would cause

6 https://blog.zoom.us/surf-zoom-dpia/

7 https://www.privacycompany.eu/blogpost-en/new-dpia-for-the-dutch-government-and-

universities-on-microsoft-teams-onedrive-and-sharepoint-online

8 https://slmmicrosoftrijk.nl/?smd_process_download=1&download_id=5286

14 adverse consequences to any of the data subjects located in the EU. The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteurs after a thorough discussion, CONSIDERED ACCORDING TO THE LAW 1. The Authority ex officio examines the compliance of the Ministry of Health with regard to Decision 50/2021. Therefore, it examines its compliance based on points 1 – 9, 11 – 18 and 20 – 21 of the reasoning of the decision in question and the specific compliance orders of the operative part of the decision. 2. Based on the response of the Ministry of Health, the data used by ITI-DIOFANTOS for the 3rd purpose (extracting statistics by level of education) do not include data that comes from the users' terminal devices . Therefore, there is no question of applying the provision of article 4 par. 5 of Law 3471/2006. Therefore, as the export of statistical data is already provided for in article 63 par. 2 of Law 4686/2020, the processing in question has an appropriate legal basis based on article 6 par. 1 e' of the GDPR and is limited to data that is necessary for that purpose. It is pointed out that the processor (I.TY.E.-DIOFANTOS) also has access to data that comes from the users' terminal devices which, however, is allowed to be processed only for purposes that are necessary for the operation of the platform (i.e. the service requested by the user) and not for a different purpose. 3. In relation to the 4th purpose, based on the Ministry's response, taking into account the amended contracts and after the company's clarifications, it is accepted that CISCO is not entitled, from the contract, to use personal data derived from the use of service for the purpose of improving the service provided by the same. It is pointed out that any such use would be the subject of a separate investigation in relation to the legality of CISCO's activities. 4. In relation to the 5th purpose, of Cisco's compliance with financial and audit requirements,

including the billing of services, it appears that the Ministry of Health has now documented the legality of said processing. 5. In relation to the transparency obligations and in particular to the full provision of all the information provided for in Article 13 of the GDPR, the Authority finds that the information is now complete, as the new information text provides all the necessary categories of information. The information is structured in a way suitable for text reading, with each category of information highlighted. Regarding the specific method of presenting the information, a technique is followed that is often found on websites in Greece, in public and private bodies; the information is contained in a distinct text in "pdf" format which is referred to via a hyperlink. The Authority points out that this particular method is no longer suitable for presentation in online applications. The "pdf" format is suitable for presenting texts in a certain way, regardless of devices, but it requires, to a large extent, the use of additional software, inside or outside the web browser, while it is not always suitable for presenting long texts, especially on devices that have limited screen width (e.g. mobile devices). Furthermore, this approach is not suitable for an online environment, as taking into account the volume of information and the lengthy text, the likelihood of a data subject (especially a child) to be aware of at least the essential information is reduced. O.E. of Article 29 in the Guidelines on transparency under Regulation 2016/679 (WP260 rev.01)9 recommends the use of a multi-level approach when information is provided in a digital environment (see paragraphs 35 – 37). Authority 9 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/transparency_en 16 refers the Ministry of Health to a relevant announcement10 which it issued recently, in order to improve the information provided to data subjects through the website , which is the main means of providing information and on which the other material (e.g. audiovisual) has a complementary effect. 6. In relation to the above and the satisfaction of the principle of transparency, it is observed that on the website https://webex.sch.gr/students.php an informative message appears in relation to the use of cookies, which creates the impression on the website visitor that he is obliged to provide consent ("If you continue to use the page, we will assume that you are satisfied with this"). As, according to the Ministry of Health, the specific cookies are necessary for the operation of the website, the message in question should be modified accordingly. In this case, the purpose should only be to inform about the use of ("necessary") cookies as the website visitor has no option to refuse them. The Authority refers the Ministry of Health to the 25/02/2020 press release with "Recommendations for the compliance of data processors with the special legislation for electronic communications"11, which includes, in the form of points of caution, guidance for the lawful use of such technologies as well as practices to be avoided. 7. In relation to completing the measures necessary to limit the risks associated with

identity verification, and in particular with the use of personal devices, in such a way as to ensure that all teachers involved in the distance education process receive minimal information, the Authority considers that the Ministry of Education and Culture has taken appropriate actions, in order to initiate the improvement of the information provided and the awareness of teachers and students, as described in its memos. 10

https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia-polyepipedi-enimerosi-se-online-periballon 11

https://www.dpa.gr/el/enimerwtiko/deltia/systaseis-gia -ti-symmorfosi-ypeythynon-epexergasias- dedomenon-me-tin-eidiki 17 8. In relation to the application of Chapter V of the GDPR and the evaluation of personal data transfers to third countries, already with its first memorandum the Ministry of Health informed that with the completion of the DTIA study, the Ministry of Health and Welfare and CISCO will proceed to enter into a new contract, which will include updated contractual clauses in accordance with the Commission's Executive Decision (EU) 2021/914 of June 4, 2021, as follows to this end, the marking of point number 20 of the Authority's decision 50/2021. 9. Regarding the issue of the controller of the transmission, CISCO HELLAS SA collects, in principle, data as the processor for the Ministry of Health. As stated in decision 50/2021 "...only the standard contractual clauses included in the respective "MASTER DATA PROTECTION AGREEMENT" which is an integral part of the free concession contracts of the Webex platform may be applicable. Based on these clauses, it appears that data is being transferred from the Ministry of Health, as a data controller, to the US-based Cisco. The Ministry of Health has not clarified whether or not this specific contractual arrangement applies. CISCO itself in the public text FAQ: International Transfer of Personal Data post- Schrems II and Brexit12 does not include the processing purposes referred to in the above clauses among those for which it transfers data as a controller (it states on p. 5 "human resources data, administrative data, billing information, and customer relationship management"). In other words, it is clear that the (technical) operation of the e-learning platform is a purpose for which the Ministry of Health is responsible, while, as was mentioned in decision 50/2021, CISCO HELLAS is responsible for processing for invoicing purposes. Therefore, the claim of the Ministry of Health and Welfare that for the purpose of the execution of the contracts concluded by CISCO HELLAS the company itself is a data controller (for the technical operation of the distance learning platform and for invoicing reasons) is not confirmed. It is pointed out for completeness and information, that in any case, still 12

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-faq-intl-transfer-personal-data

-post-schrems-II.pdf 18 that is, even if it is considered that the transfer is made by CISCO HELLAS for its own purposes (as a

data controller and not in the context of the contract) it is clear that the Ministry of Health has the responsibility to check whether the transfer of data to CISCO HELLAS is legal, knowing that this data may be transferred to the USA, as the Danish Authority also points out in its text ("...the Danish company must assess on which legal basis it may disclose the relevant metadata to the CSP for the CSP's processing of the data for its own purposes..."). 10. The Ministry of Health, through CISCO, has followed the so-called "risk based approach" andhas estimated that as the possibility of access by the US authorities at data is too small, such processing is permissible. Specifically,

the evaluation of the Ministry of Health as a data controller comes to a conclusion

that the relevant legislation in the USA it is also problematic that what is transmitted

data and/or the data importer falls within its scope

this legislation. Then, as appears from the memorandum of the Ministry of Health and

the relevant analysis of CISCO13 was examined by the Ministry

additional measures applied so that the mechanism is selected

transmission (standard data protection clauses) to ensure

"substantially equivalent" level of protection to that of the E.U., ensuring that

any request by the law enforcement authorities of the third country (here

USA) is "necessary and proportionate". Further, after July 2022, the

The Ministry of Health reports that transfers to countries outside the EU are being abolished. and

data will be held within the EU. Therefore, after this date, the only

an issue that remains is the possibility of access by US authorities. at

held within the EU data. The consequences of calculated risk

are reduced, even more so in the case of the Ministry of Health, as from

transmitted data (and/or those that will be processed after

1/7/2022) contain largely fictitious elements, in terms of

students, and their identification, although it cannot be excluded, because of

13 See pp. 3-5 of the text FAQ: International Transfer of Personal. Data post-Schrems II and Brexit.

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-faq-intl-

presence of identifiers such as IP and MAC addresses, requires cross-referencing
(possibly multiple intersections) with other data sources. In
in the case of teachers, of course, the identification can be made simpler.
It must also be taken into account that from the purpose and nature of the procedure
distance education, it is highly improbable such data – which
refer to an educational process - be necessary for the enforcement authorities
of the law of the USA.. This approach, based on the risk, as seen and
from the corresponding studies on competitive products, a solution has been made that
appears to be followed or suggested by controllers in
similar applications. Therefore, from the method that the Ministry of Health worked on and based on
of which he documented the transfer of personal data to
countries outside the EU it can be accepted that the Ministry carried out
evaluation of the transmission in a manner described in paragraph 20 thereof
Decision 50/2021 of the Authority.
11. It is pointed out that the risk-based approach has not, to date, been
accepted by the supervisory authorities of the GDPR. Specifically, the wording of the article
44 of the GDPR does not provide for the size of the threatened risk as its criterion
transferability, but requires that the layer not be compromised
protection of natural persons guaranteed by the GDPR. Yes, on
cases where the legislator takes a risk-based approach to
GDPR, this is explicitly stated in the respective provision. Therefore, although the Authority
accepts that the possibility of access by US law enforcement authorities;
in the personal data of said processing, is very small,
it is questionable whether this finding makes transmission permissible (even

after 1/7/2022). The issue in question, however, does not only concern the Ministry of Health, but concerns every data controller who uses services teleconference of companies belonging to a group controlled by an entity subject to US law. As this matter has cross-border implications extensions, the Authority will examine the issue with the GDPR supervisory authorities through of the cooperation and/or coherence procedures provided for in GDPR, in order to achieve a coherent and comprehensive solution or approach.

20

FOR THOSE REASONS

The Authority considers that no new corrective measure is required in relation to the above case. At the same time, he calls on the Ministry of Education and Religious Affairs to proceed to the necessary amendments to improve transparency, as described in paragraphs 5 and 6 of the decision.

The president

Konstantinos Menudakos

The Secretary

Paleologo Georgia

21