Athens, 05-07-2019

PRINCIPLE FOR DATA PRIVACY

Prot. No.: G/EX/3254/07-05-2019

FOR OPIC CHARACTER

A P O F A S H A . 10 / 2019

The Personal Data Protection Authority met, after

invitation of its President, to a regular meeting at its headquarters on 4/24/2018,

following the meetings of 16/3/2017, 20/6/2017 and 21/9/2017,

in order to examine the case referred to in the present history.

The President of the Authority, Konstantinos Menudakos, and the regular members were present

of the Authority Konstantinos Christodoulou, Antonios ymbonis, as rapporteur,

pyridon Vlachopoulos, also as rapporteur, Konstantinos Lambrinoudakis,

Charalambos Anthopoulos as well

the alternate member Emmanuel

Demogerontakis in replacement of regular member Eleni Martsoukos, n

which, although legally summoned in writing, did not attend due to obstruction. the

meeting, without the right to vote, also attended by order of the President,

Maria Alikakou and Efrosyne Yougle, special scientists - auditors, as

assistant rapporteurs, who withdrew after the debate and before the conference

and making a decision, and Irini Papageorgopoulou, his employee

Department of Administrative Affairs, as secretary.

The Authority took into account the following:

It was submitted to the Authority under no. prot. G/EI /7646/23.11.2016 his complaint

of the Association of Private Colleges (hereinafter I) regarding imposed by

Ministry of Education, Research and Religions (hereafter Ministry of Education) obligation

registration of "simple" data and data of special categories of students,

parents/guardians and teachers of private schools in the single central

database of the Ministry of Education and Culture under the name "mySchool" (hereinafter "mySchool").

specifically, with no. prot. Φ8/145/97610/Δ2/14.6.2016 document of

G.G. of the Ministry of Health, I was informed that from the 2016-2017 school year all

private primary and secondary schools had to register

in the above "mySchool" database data regarding the student potential, the

school unit and the register of teaching staff, so that

the digital display of the operating elements of all private is completed

school units. on 22.9.2016, the Ministry of Health with the no. first

154892/E1.22.09.2016 his document returned to the above issue and, among other things,

as stated in the present complaint, it was imposed on private schools n

obligation to register the weekly program in "mySchool".

of teaching, the data of teachers and students of each class and

department corresponding to public schools. Regarding the add-ons

optional school actions, it is specified in the above document that for them

the existing procedure of mandatory notification of the concerned is followed

education directorate. then, on 07.10.2016, according to the judgment

complaint, all private schools received from the Head of Department B

of Private Primary Education of the Ministry of Education and Culture e-mail, with which

were invited to register their operating data for the school year 2016-

2017 in a free software electronic form (Google Forms), below

part of which was marked not to complete the code.

then I with no. prot. 260/24.10.2016 document to

the Head of the Department of Private Education of the Ministry of Education and Culture asked to

be informed, if the Ministry of Health and Welfare has complied with the recommendations it had addressed

the APDPH with decision 139/2014, as well as for its communication methods
Ministry of Health with the schools so that the private schools can inform
safely the Ministry of Health in accordance with the legislation that governs the safe
electronic transactions. e response of the above document regarding the
legality of the processing in question, the Ministry of Health informed I that it

depends on the p.d. 114/2014 (Ministry of Health Organization Chart) and the no. first
Φ8/145/97610/Δ2/14.6.2016 document of the Ministry of Health (see above).
O I, considering that the above response of the Ministry of Health regarding its legality
under processing is not correct, as, according to his claims, "no
here the smallest thing is against the law and at the same time carries great risks
in terms of data security" and "the Ministry of Health has not complied with them
as addressed to him by the Authority with letter no. 139/2014 decision of
appealed with the present complaint to the Authority.
the context of examining the said complaint, the Authority sent it with no. first
C/EX/7646-1/01.12.2016 document, with which he notified both the Ministry of Health, as
controller, as well as at the Institute of Computer Technology and
"Diofantos" Publications (hereinafter ITYE-Diofantos) as processing,
the above complaint and invited them to submit their opinions in writing
and clarify, in particular, a) the provisions in which the obligation is provided
registration
personal
data
of
students/parents-
guardians/teachers of private schools in the "mySchool" system, b)

issues related to the security of the above processing, including

of the security issue of the website's SSL certificate

sso.sch.gr, of private schools' access to the above system without IP

addresses of the Panhellenic Cholic Network (P D), as well as the application

of recommendations b, c, d, f, h, i of point 6 of decision 139/2014 in combination

with the "mySchool" portal user manual, which is posted on the main page

page of the system in question dated 01.9.2014.

then the Ministry of Health notified the Authority with no. first

C/EI /8365/19.12.2016 document, with which it called on ITYE-Diofantos to

respond to b) question of the above document of the Authority. With no. first

G/EI /8494/23.12.2016 electronic message of the Secretariat of Electronics

Address, it was forwarded with no. prot. 219178/A3/21.12.2016 his document

Department A' – Digital Design and Development of A/T Applications and

of Higher Education of the Ministry of Education, in which it was stated that the address in question

"has no involvement in its design, development and operation

"mySchool" information section.

3

Subsequently, and given that the Authority did not receive a response to the above

her document, resent it with no. prot. C/EX/1060/10.2.2017 document, with

which pointed out both to the HYPETH and to the ITYE-Diofantos, that in

in the event that he did not receive an answer, he would proceed with the exercise of his powers

law of its competences.

in response to the last above-mentioned document of the Authority, ITYE-Diofantos

sent it with no. prot. G/EI /1074/10.2.2017 electronic message, with

which forwarded to the Authority his document to the Ministry of Health, which contained

answers to the original with no. prot. G/EI /7646/23.11.2016 document of the Authority

and which, according to ITYE-Diofantos, the Ministry of Health should have

incorporate in its own response to the Authority.

Following these, and mainly for the reason that the Authority did not accept reasonable

period of time some response from the Ministry of Health to the above documents, he called

the Ministry of Health, as the controller, the ITIE-Diofantos, as the executor

processing as well as the complainant I, to attend its meeting

Plenary of the Authority on Thursday 16-3-2017, for the discussion of the matter under review

of I's complaint (corresponding call number C/EX/1721/02.3.2017,

C/EX/1722/02.3.2017, C/EX/1725/02.3.2017).

then, Department B of Private Secondary Education and

of Primary Education of the Ministry of Education and Culture sent to the Authority the no. first

40496/GD4/09.3.2017 (prot. no. of the Authority G/EI /1964/10.3.2017) answer

document referring to the Authority's first clarifying document, without doing so

mentioned in the Authority's second and last document. With the above document, the

Ministry of Health gave the following clarifications: a) private schools cannot

are treated as businesses operating in free economy terms,

but are subject to the supervision of the Ministry of Health according to article 16 thereof

of the Constitution and Law 682/1977 which refers to private education, b) the

provisions of Law 1566/1985, in accordance with article 62 par. 7 thereof, apply

proportionally also in private schools in order to have harmonization between them

of two forms of education (public and private), c) from the existing provisions

there is no exception to the registration of students' details and

of educational private schools of first grade and second grade education. the

document

this

incorporated

the

answer

of

ITYE-Diofantos

4

(G/EI /1074/10.2.2017) regarding the issues concerning the safety of

processing through the "mySchool" system.

they attended the Authority's Plenary meeting from 16-3-2017

legally, they presented their views and answered questions from its members

At the beginning the representatives of the Ministry of Health, the Head of the General Directorate of

B, General Director of Primary and Secondary Personnel

of Education and C, Head of the Department of Private Primary Schools

of Education, the representatives of I, D, member of the board of directors, E,

I's advisor and partner in IT matters and Grigorios

Lazarakos, attorney-at-law, as well as the representatives of ITYE-Diofantos

T, technician, responsible for the "mySchool" system and Z, supervisor

of department T1 of the Directorate of Educational Technology. In addition, the Ministry of Health and

I submitted the no. prot. G/EI /2664/29-3-2017 and G/EI /2665/29-3-2017

reminders, respectively.

subsequently, the Authority, with the electronic message dated 4/27/2017, invited

the ITYE-Diofantos in a meeting at its headquarters for the purpose of its presentation

operation of the "mySchool" system to the assistant lecturers. The ITU-

Diophantos accepted this invitation (prot. no. G/EI /3504/28-04-2017)

and at the meeting, which took place on 3-5-2017, it was presented

of the "mySchool" system in a test environment by its representatives

ITYE-Diofantos T and Z, who provided clarifications to their questions

assistant presenters submitted during the presentation. Further
clarifications regarding the security measures of the "mySchool" system
were presented to the Authority by ITYE-Diofantos with the date of 02/5/2017
electronic message (prot. no. G/EI /3511/02-05-2017). Also, with the from 04-5-
2017 e-mail was requested by ITYE-Diofantos to send to the Authority
the "screens" and the data registered in the "mySchool" system for them
panhellenic exams before and after the change in the way they are conducted, as well
and the "screens" concerning the data of private teachers
schools. ITYE-Diofantos provided the above data with the from 04-5-
2017 electronic message (prot. no. G/EI /3637/05-5-2017).
The Authority met on 20/6/2017 to discuss the said case and
deemed it necessary to provide additional information regarding the collection

data of students-parents/guardians and teachers of private schools.
Following this, the Authority requested from ITYE-Diofantos, with the 20/6/2017
email, to provide status with the type of all data
which are kept in the "mySchool" system and concern students-parents/guardians and
teachers. ITYE-Diofantos provided the requested data to the Authority
with the e-mail from 21/6/2017. then, the Authority sent it with no.
prot. C/EX/4865/23-6-2017 document, with which he requested from the Ministry of Health and
to submit two completed statements (excel file with two sheets), the
which included the type of data (column A), one of the students-
of parents/guardians (on the first sheet of the excel file) and the other of them
teachers (on the second sheet of the excel file). For each of the data
of students-parents/guardians and teachers were asked to complete
four columns (B-E). In particular, in the fields of column B it was requested to

fill in "YES", if the corresponding data in column A was transmitted to

Ministry of Education from private schools before the "mySchool" system and "NO" to

otherwise. the fields of column C were requested to be completed "YES", if

had been requested by the Ministry of Education and Culture to be registered in the "mySchool" system by

private schools the corresponding data in column A and "OXI" in the opposite

case. the fields of column D asked to fill in which data

they considered on the one hand the HYPETH and on the other I , necessarily, according to their judgment,

for the exercise of the supervisory authority of the Ministry of Health, as provided in

current legislation (especially n. 682/1977, n. 4452/2017, p.d. 114/2014), in relation to

the performance of a single student number and the conduct of the Panhellenic exams.

the fields in column E were asked to justify, in their judgment, which

data they consider not necessary for his supervisory competence

Ministry of Health, as provided for in the current legislation, in relation to performance

uniform student number and the conduct of the pan-Hellenic exams. The Ministry of

replied to the Authority with no. prot. G/EI /5232/10-07-2017 document and o

I with the no. prot. G/EI /5212/07-07-2017 document.

Subsequently, the Authority sent the no. prot. G/EX/5399/14-07-2017

document, with which he requested the Ministry of Health and Welfare to document specifically, by invocation

of any existing relevant provisions of the current legislation, the necessity

of registration in the "mySchool" system (as well as its necessity

access by the relevant Director of Education) for each of the personal

student and teacher data (as listed in the corresponding column A

of the excel file), which he deems to be convenient and necessary for him

intended purpose of the supervisory authority of private schools, such as

each time he is specialized (e.g. for the validation of study titles of

of private schools, to check its pedagogical suitability

timetable, for the conduct of the Panhellenic exams, the control

of teaching hours, etc.) and, in general, for the exercise of

responsibilities of the relevant Director of Education. The Ministry of Health responded to the Authority

with the no. prot. G/EI /5845/01-08-2017 document.

then, the issues related to the measures are listed in more detail

security of the "mySchool" system based on the above documents of the Ministry of Health,

ITYE-Diofantos and I.

in the present complaint, I reported that the Ministry of Health and Welfare has not complied

with the recommendations under items 6a and 6g addressed to him by the Authority with no.

prot. 139/2014 Decision regarding the security measures of the system

"mySchool".

specifically, I raised the issue of non-compliance with recommendation 6a

of the above decision, according to which the Ministry of Health must "(...) a) To proceed

encryption, according to internationally accepted standards, at least, of

identification data of students and their parents-guardians (as well as

of the identification data of all categories of subjects) that are kept on

data base of the said department (…)". I claimed not to know,

whether said encryption has been completed and raised the issue of security

of the TLS certificate used to encrypt them

of transmitted data between his computer/browser

user and the central server of the "mySchool" system. according to

reportedly, the TLS certificate of the system in question is low

security, compared to the corresponding certificates of the application of one

of a private organization with a high level of security (such as the relevant application

of a Bank). I provided indicatively two copies of reviews

security overviews, as generated by the web browser

Chrome, one of which concerns the central website of the system

7

"mySchool" and the other the website of Eurobank AE. her

provided security overview of the banking website

the designation "strong cipher" ("strong cipher") was mentioned, while

they were referring to the equivalent of the "mySchool" system website

"obsolete connection service" and "older

encryption" ("obsolete cipher"). I also mentioned that taxisnet,

according to press information, has decided to implement an upgrade of

communication protocols, with the result that they are no longer supported

operating systems, such as Windows XP which are still used by

services – centralized and decentralized – of the Ministry of Health, (but they are not supported with

new updates, which makes them unprotected and insecure).

In addition, according to the present complaint, although the Authority with sub

items 6g recommendation of Decision 139/2014 requested from the Ministry of Health "(...) g) To

ensure that the system excludes the flow of money originating from

from an IP address outside the Panhellenic School Network given that the

application allows access only to users who are authenticated by

the Central Accreditation Service of the Panhellenic School Network and the

YPAITH does not document at all why the trial is allowed from all of them

Greek IP addresses, which increases the risk of online attacks.

(…)", in no private school has been installed, by the competent authority,

IP address of P D, with the result that the above recommendation is not respected

Principle.

The Ministry of Health, as controller and the ITYE-Diofantos, as executor

the processing, they informed the Authority about the issues raised by I for

the security measures of the "mySchool" system, as follows:

the Authority's Decision 139/2014, its "security gaps" were not highlighted

central database of the "mySchool" system. The beginning from the institution

in its role made recommendations, mainly regarding the strengthening of the safe

use of the application so that only authorized users have access

in the name, register, class and details of parents/guardians of the students,

and the confirmation of the non-access of users outside the school to these details,

while in addition recommendations were made for the adoption of controlled procedures

access.

8

Regarding the issue of the security of the TLS certificate, the Ministry of Health reported

that access to the "mySchool" system is done by authenticating it

user through the interface of entering the code in the central system

certification/authorization (https://sso.sch.gr) and its change system

password (https://register.sch.gr/password). directly with the Management and

Account Security instructions are available on the website https://sso.sch.gr

of safe use (https://sso.sch.gr/safetyInfo.jsp). With a frequency of at least two

times a year, there is an update to the users from the service "Single Sign

On" - SSO of P D in relation to the password and its security.

The TLS certificate of the website https://sso.sch.gr is RSA

2048 bits (signature algorithm SHA256withRSA) and has been issued by TERENA

Certificate Authority. Some applications are required to serve and

older browsers, which are built into old operating systems

systems and for this reason the corresponding ciphers or

older protocols. this is why the designation "obsolete cipher"

in the security options of the Chrome browser, while

there was a problem, an incomplete or reduced security message would be displayed.

The corresponding TLS certificates of the online banking sites

organizations

such as

www.nbg.gr,

www.alpha.gr/e-banking/en

and

www.winbank.gr/sites/idiwtes/el/Pages/default.aspx is RSA 2048 bits (signature

algorithm SHA256withRSA) similar to sso.sch.gr. In addition, the TLS certificate

of the "mySchool" system after user authentication is also this

RSA 2048 bits (signature algorithm SHA256withRSA) and is categorized as A',

from acquaintances

server security rating sites

web applications. The ones characterized by its latest editions

chrome of TLS certificates as obsolete ciphers under no circumstances

means they are weak or create issues of insufficient security. They just have

implemented newer cipher creation methods (called "modern").

The Ministry of Health and the ITU-Diofantos presented with the no. first

C/EI /1964/10-3-2017

document copies

of

security reviews

online

places

e-banking

banking

organizations

(e.g.

https://ibankretail.nbg.gr

(National),

www.alpha.gr/e-banking

(Alpha),

https://www.winbank.gr/sites/idiwtes/el/Pages/default.aspx (Piraeus)), as well as

9

of the GSIS (https://login.gsis.gr/mylogin/pages/login.jsp), from which it appears that

the websites in question were rated the same by the browser

chrome (with that of the "mySchool" system) to use "obsolete ciphers".

In view of the above, according to the Ministry of Health and the ITYE-Diofantos, the

allegation referred to in I's complaint about his lack of security

"mySchool" system does not correspond to reality.

Regarding the issue of accessing the "mySchool" system outside of IP

Directorates of the Ministry of Health, the Ministry of Health and the ITU-Diofantos reported the following:

Access exclusively within P D cannot be a realistic option

for the "mySchool" system. All users utilize the tool, often

and in non-working hours. In addition, users of its Central Service

Ministry of Education, the users of the Institute of Educational Policy (IEP), as well as all

private schools do not have access to P D.

The system infrastructure remains safe from malicious attacks with the

help with certificates, monitoring systems and preventing attacks

as well as firewall systems, and access to it

allowed only to Greek IP addresses.

All units of the standard have access to the "mySchool" system

Primary and Secondary education and all its administrative structures

education. In addition, individual access accounts have also been attributed to

users of the central service of the Ministry of Health, as well as at the Institute

Educational Policy. Non-formal schools will also have access

training of the Ministry of Health for the utilization of the system as a computerized one

daily operation tool. Also, taking advantage of the role of the person in charge

approximately 30,000 teachers and individuals have access to the department

accounts, as issued and maintained by P D. Its users

of the "mySchool" system have an account at Π D, which has the

management of these accounts. The codes for users to access the

system are encrypted by P D.

The use of the "mySchool" system by private schools, according to

examination of the case in question, is analyzed as follows:

10

Type

Usage rate

system (students)

System utilization rate

(educators)

Primary school

Private High School

Private High School with

High school classes

Private

bile

Private

High School

Private

EPAL

Private High School

Private Kindergarten

Daily

Vespers

80.5%

100.0%

80.8%

100.0%

100.0%

98.9%

68.6%

61%

100%

54%

100%

100%

74%

47%

Also, the "mySchool" system integrates computer functions

for the support of the panhellenic examinations at the level of school units and

MINISTRY OF It still receives data from the National OP ED system

(Ministry of Public Health) based on KYA 1493/2016 as a result of the repeal

the paper presentation of the students' birth certificates. Also,

provides the statistical data requested by EL TAT for each school

year.

The "mySchool" system can also be used outside standard hours,

as well as the possibilities provided by the system for the computerized support of

structures are such that make its acceptance and utilization universal.

it is often not possible to complete the administrative work within the standard

teachers' hours. In addition, a factor that does not allow the

completion of all computer work during the standard

hours is the fact that there are not the necessary workstations in

professors' office (e.g. for each head of department) and in many

cases not even a computer. In view of this, in every newsletter

meeting of teachers, attended by ITYE-Diofantos, the request

access to the system outside working hours was universal. The requests

arose during the system presentation days in 2014 in all

Regions of the country in the presence of all the directors of school units, while

are also recorded in electronic bulletins of the same period. The reasons are summarized

in the partial inadequacy of the infrastructure of P D in some cases to

respond to the effective coverage of school network needs

units.

With the no. prot. G/EI /2665/29-3-2017 his memorandum, which

submitted to the Authority following the 16-3-2017 hearing summons, I

raised, in addition to the issues mentioned above, the following related issues

with the security of the "mySchool" system. Particularly:

1) regarding the authentication of users, the following are mentioned, in summary

quotes:

The authentication level of the "mySchool" system is not so

as strong as his confidence level warrants. Its online services

system process "simple" data and data of special categories and,

therefore, they are included in the highest level of trust, level 3.

The authentication of the "mySchool" system is low or moderate

certainty about the correctness of the user's digital identity. The system

uses a password for authentication, a fact that

ranks at authentication level 1 (low or moderate certainty about

correctness of a user's digital identity). International safety standards

define that for the systems, which process "simple" and expert data

categories and in which only authorized persons have the possibility

access to the services offered, a high degree of certainty is required

correctness of the user's digital identity. This means that the mechanism

authentication should use two-factor technology

authentication) and specifically digital certificates or utilization

loose or hard storage tokens instead of using authentication with

a simple password chosen for the 'mySchool' system.

The fact that it is registered in the "mySchool" system is very important

number of personal data and that many thousands are allowed access

civil servants, who are geographically dispersed and have

access even from an internet cafe or their home, and this access

allowed by potentially vulnerable endpoints, renders

absolutely necessary to have a second level of security (2nd factor

authentication).

Also, reference is made to recommendation 6b of its decision 139/2014
APDPH, according to which the Ministry of Health must "(...) take care, so that
including the possibility of creating individual user accounts
to be assigned by appropriately authorized teachers of each college
unit and employees of each administrative structure such as the directorate or regional
address, in order to avoid any sharing of my unique account
attributed to the director of the college unit or the administrative structure for it
carrying out all the tasks required by the service side
"mySchool" (…)". For this recommendation it is stated by I that it is known
throughout the educational community that "mySchool" is used by
at least three (3) employees of each Education Directorate or each
of the Regional Directorate, except for the responsible Director. The result is
that all the above employees can share the username and password
of the Director having, indeed, the possibility of access from their home and
from possibly infected PCs.
Additionally, it is reported that the 'mySchool' login interface is vulnerable
to attacks, because CAPTCHA is not applied when entering the codes,
it is allowed to copy-paste (copy-paste) the codes in the respective ones
fields, the browser is allowed to save the password, while
it is simply given as advice to users "Avoid storing it
password from the browser and prefer to retype it
every time" and no encryption is applied to passwords.
2) regarding the Security Policy of the "mySchool" system, the
below, summarized:
The "mySchool" system is not properly designed to prevent
threats during the user registration process, because a) the creation of a new

account is vulnerable to threats and is not secure since it does not

verifies the user's identity (page 26 of the Security Policy), b) h

retrieving account credentials is not secure (page 30 of

Security Policy), c) the process of removing user access is wrong

designed and involves many security risks (page 31 of the Policy

Security).

13

Also, the "mySchool" system appears to be vulnerable to a crowd

attacks, as these have not been provided for by the Security Policy. THE

Security Policy does not correspond to the level required by the system

'mySchool', does not appear to be revised regularly, is not known to users,

no compliance checks are carried out, no procedure has been provided

risk management and periodic vulnerability checks are not foreseen and

incident and has basic deficiencies in content.

3) regarding additional issues for the 6g recommendation of Decision 139/2014 of

The following, briefly listed, are mentioned in the APDPH:

The use of a PC outside a closed network (P D) and, indeed, from places outside

of the office carries many risks for the interception of codes and

data, particularly on a system that is not protected by a strong

authentication. Indicatively, it is stated that the system is not protected by

"viruses", "Trojan horses" and "worms" (virus, trojan horses, worms) in

local computers from which it is accessed and which it can

for the whole family to use. It can also be accessed from the internet

cafe or a friend's PC, where the user fails to log out or

whose network is monitored, by free wifi, by mobile phone and

tablets or from PCs with old operating systems windows XP, vista, which

are not supported with new security releases from Microsoft. The mentioned
from ITYE-Diophanto security measures, according to I, cannot
cover the interception of the identifiers and passwords of the above
cases resulting in the malicious user gaining access to
student and teacher data.
Regarding the use of the "mySchool" system during non-working hours
and outside standard hours, I reported that the above practice is contrary
in the labor legislation, as it implies a direct violation of the legislation
provisions that have been established for the defense of the rights of
workers and, above all, the exclusion of labor exploitation phenomena
potential. He also stated that it goes without saying that private schools do not
willing to adopt delinquent behavior against teachers
and the employees of the schools, who have been hired to provide the services
in a given way and at a given time and place.

4) regarding other security measures of the "mySchool" system, refer to
following, summarized:
System users are not trained in security issues. The
diaries and the electronic messages sent twice a year to
users of the P D SSO service in relation to the password and the
his safety, are a formal and not an essential training process of
users. Users are easy, due to lack of training, to fall victim
fraud ("phishing") to intercept codes.
The "mySchool" system presents availability problems, because from
at 23.30 on 16-3-2017 and until the morning of the next day it was not working.
It is not possible to enter mass data from

information systems of private schools in the "mySchool" system with

xml files, although, according to I, during the hearing process

it was mentioned before the Authority that this possibility exists. I sent

to the Authority, to prove, as he states, his claim, from 16.3.2017

Email message with attached screenshots and the manual

of use of the "mySchool" system, according to which the mass introduction of

data of the students is done from an excel file.

according to I, questions regarding the security of the system

creates the ability to search and find all private elements

teacher, including this AKMA, alone

registration of the teacher's tax identification number in this system. This is provided for in

"mySchool" user manual and the screenshots contained therein.

To refute the claim that AMKA exists as an image in the manual but

does not work, the representative of I sent the Authority from 16.3.2017

Email message with screenshots of the application attached

and with details of a specific teacher, according to which it also appears

his AMKA.

Also, according to I, security questions and

protection of personal data is created by the interconnection of the base

data from the "mySchool" system based on the National Census and,

mainly, the fact that users of the "mySchool" system can

search for the student's data in the National Census database. In addition, the

I reported that he was informed that the codes of the database and of

encryption of the "mySchool" system has only one person.

Furthermore, in his above memorandum, I argues that the Authority should

to ask the data controller to carry out a study

impact assessment for the protection of his personal data

of the "mySchool" system as defined in article 35 of the General Regulation

on Data Protection (EU) 2016/679.

The Authority, after examining all the elements of the file, as well as the

of what was mentioned during the hearing, after hearing the speakers

and the assistant rapporteurs, who then left before the

conference and decision-making, and after thorough discussion,

THOUGHT ACCORDING TO THE LAW

1. Private education is under the supervision of the State according to the constitution,

in article 16 par. 2 and 8 which states that "[…] 2. Education is basic

mission of the State and aims at the moral, spiritual, professional and

physical education of the Greeks, the development of the national and religious

conscience and their development into free and responsible citizens.[…] 8.

Law defines the conditions and conditions for granting a license for the establishment

and operation of schools that do not belong to the State, the related

supervision exercised over them, as well as his official status

their teaching staff."

2. Article 4 par. 1 of the applicable to the case under consideration L.2472/1997 (A'

50) states that "Personal data to be lawful

processing must: a) Be collected in a legitimate and legal way for

defined, clear and legitimate purposes and exist legitimately and

lawful processing in view of these purposes. b) Be relevant, convenient,

and no more than is required in each case in view of its purposes

processing. c) To be accurate and, if necessary, to be submitted to

update. d) [...]'.

3. Article 10 par. 3 of Law 2472/1997 stipulates that "the data controller
must take the appropriate organizational and technical measures for it
security of data and its protection from accidental or unlawful
destruction, accidental loss, alteration, prohibited dissemination or access and
any other form of unfair processing. These measures must ensure
level of security commensurate with the risks involved in the processing
and the nature of the data that is the object of the processing.[…].” THE
this obligation falls accordingly on each processor,
in accordance with par. 4 of the same article.

4. Article 1 of Law 682/1977 "On Private Schools of General Education
and Boarding Schools" (A' 244), as applicable, stipulates that "Private general schools
of education, according to the meaning of this law, are the corresponding to
public schools of general primary or secondary education that do not belong to the
State, but established and maintained by natural or legal persons,
according to the specific provisions of this law." Further, in article 2
par. 1 and 5 it is defined that "1. The Private schools of general education
fall under the competence of the Ministry of National Education and
Religions, exercising supervision over them through the regional ones
supervisory bodies. [...] 5. For disciplinary responsibility and in general
procedure and any other relevant matter concerning disciplinary proceedings and
penalties for teachers of private general education schools
the provisions of Law 3528/2007 shall be applied proportionally."1.

5. Article 62 par. 7 of Law 1566/1985 "Structure and operation of the primary
and secondary education and other provisions" (A´ 167) provides that
"Without prejudice to paragraph 4 of article 52, the provisions thereof

of law are applied accordingly to private primary school units

and secondary education and to their educational staff, except

from the provisions of cases A', B' and C' of article 11."2.

1 Paragraph 5 was added by article 41 of Law 4301/2014.

2 Article 52 was repealed by Article 3 of Y. A. T. 5/26 (Domestic Household National Education) of 4/5.10.88,

B´732. In addition, according to article 110 par. 1b of Law 4547/2018, Official Gazette A 102/12.6.2018: "With the reservation

of article 20 and in particular paragraphs 8, 9 and 12 to 15 of this article, every provision is repealed

6. With article 2 par. 2 para. i' of the p.d. 114/2014 "Ministry Organization

of Education and Religions", (A' 181), as this was supplemented by

recent Law 4452/2017 (see below) defines "Self-employed Address

Private Education". With article 40 of the same as above p.d., like this

added by Law 4452/2017, the following are defined: "1. Business objective

of the Independent Directorate of Private Education is the supervision of

of private schools of primary and secondary education, h

ensuring the quality of the training provided to them, the handling

issues of the staff and their owners, as well as its supervision

operation of foreign schools, tutoring schools and centers for foreigners

languages. 2. The Independent Directorate of Private Education reports directly

to the General Secretary of the Ministry of Education, Research and Religions.

3. The Independent Directorate of Private Education is composed of

following organic units: a) Department A of private primary schools

and secondary education […]. 4. Section A of private schools

of primary and secondary education is responsible for: a)

supervision of all private primary and secondary schools

education, b) the granting, modification, updating, transfer and

revocation of the license of private primary and secondary schools

education, c) every issue related to the organization and operation of

of private schools of primary and secondary education, and d) the

handling any other relevant matter. 5. Department B of private personnel

of primary and secondary schools is responsible for: a)

the registration in the Yearbook, as well as the supervision of the issues

service status of private primary teachers and

of secondary education in accordance with the present provisions, b) the

disciplinary cases of private teachers, as well as owners

and legal representatives of

of private primary schools and

secondary education, and c) the handling of any other relevant matter.

[…].”.

7. Article 41 par. 2 of Law 4301/2014 "Organization of the legal form of

religious communities and their associations in Greece and others

which is in conflict with the provisions hereof and, in particular, the following: a) [...], b) the Chapters

A to C` of article 11 […].

18

provisions of the competence of the General Secretariat of Religions and others

provisions" (A´ 223) stipulates that "[…] 2. Paragraph 5 is added to article 2

of Law 682/1977 as follows: For disciplinary responsibility and in general

procedure and any other relevant matter concerning disciplinary proceedings and

penalties for teachers of private general education schools

the provisions of Law 3528/2007 shall be applied proportionally."

8. Article 41 par. 1 of Law 4351/2015 "Grassable lands of Greece and other

provisions" (A´ 164) provides regarding the high school diplomas of

of private schools that "1. The true meaning of the provision of the second paragraph

of paragraph 5 of article 16 of Law 3149/2003 (A' 141) is that the issued

Dismissal titles of the students of the private schools are considered by the

director of the relevant secondary education directorate, in addition to

high school diplomas of dismissal of the students awarded by the

recognized as equal to public private primary schools and

of secondary education".

9. Article 7 par. 1 a' of Law 4452/2017 "Regulation of matters of the State

Certificate of Language Proficiency, of the National Library of Greece and

other provisions" (A' 17), as applicable, provides that "1. a) One is established

Education Number, which is issued based on the Registry Number

of Social Security, is unchanged for every natural person and

is maintained even after the end of the studies. The Single Number

Education is attributed with the person's first entry into

any level of education in the country, public or private. THE

Single Education Number corresponds to a relevant personalized registration

of the relevant information system of the Ministry of Education, Research and

Religions. b) [...]."3.

10. the no. KYA 1493 (Government Gazette B 298/12-02-2016) interconnection is provided

of the "mySchool" Information System of the Institute of Technology

of Computers and Publications, (ITYE) "Diofantos", under the responsibility of the Ministry of Health, with the

central database of the Integrated Information System

National Census. specifically, in par. 1 and 2 of the article itself

as above KYA provides for the access of ITYE-Diofantos, as accredited

3 Paragraph 1 was replaced as above by article 18 of Law 4521/2018 (A' 38).

body, in the central database of the OP ED National Census for

the exercise of the responsibilities of the Ministry of Health, as well as the access of the system

"mySchool" on the above basis exclusively for the processing of the relevant

tasks with the registration and monitoring of students in Kindergartens -

Primary - Middle - High School. Also, in par. 3 of the above-mentioned article alone

KYA defines that "(...) The necessary information for the processing of

related tasks of registration and monitoring of students at

Kindergartens - Primary - Middle - High schools will be transferred digitally from

OP ED in the Information System "my school" of the ITU "Diofantos" for the

Ministry of Education, Research and Religions (…)"). In addition, in par. 4

it is stipulated that the administration of the ITU "Diofantos" must receive the appropriate

technical and organizational security measures. Furthermore, according to par. 7, the

services "under the competence of the Ministry of Health (exclusively:

Kindergartens - Primary - High Schools - High Schools)" and have access to

"mySchool" are looking for the required information to process them

procedures of their competence, through "mySchool", by the OP ED

National census and are not allowed to ask citizens to

proceed with the presentation of supporting documents which include the

information provided by the OP ED.

11. Security issues during the exercise of powers by its operators

public sector using ICT, during communication and transaction between them

public sector bodies using ICT, or between public bodies

sector and natural or legal persons under private law, as well as in terms of

the access of natural persons or legal persons under private law to

public documents and making them available for further use using ICT

are regulated in Law 3979/2011 (A' 138) on electronic government (see

in particular article 2, article 3,. article 17 par. 1 and 3, article 21 par. 2, article 22 par.

1, article 32 par. 4).

12. By authorization of articles 27 of Law 3731/2008 (A´ 263) and 17 par. 3 and

21 par. 2 of Law 3979/2011 was issued under no. YAP/F.40.4/1/989 decision of

Deputy Minister of Administrative Reform and Electronic Government,

(Government Gazette B´ 1301/12.04.2012) entitled "Sanction of Service Provision Framework

of Electronic Government" (hereafter PPYID). In particular, in PPYID

20

the rules and standards for registration, identification and

electronic identification of citizens in electronic public services

sector and specifically in its Annex III (Framework of Digital

Authentication).

a. according to the PPYID, the user authentication conditions

are determined by the level of trust, to which the

electronic services provided. The

flat

trust

are categorized according to the type of data they use

(personal, sensitive and financial), but also the possible effects

which may be caused in case of improper operation or

their management. In particular, they are included in confidence level 2

services that require the exchange of personal data, which do not

are sensitive, such as, for example, data concerning the

user's marital status, date of birth, gender, etc.,

while trust level 3 includes either services that

require the exchange of sensitive data, or electronic services

level 4 completion, where the user also performs the

financial transactions required electronically.

b. Also, according to the PPYID, the authentication mechanisms that

recommended for authentication level 1 include

passwords, one-time passwords (which are a form of

two-factor authentication) or a combination

of these. The authentication mechanisms proposed for the layer

authentication 2 use digital certificates, it is recommended

and exploiting soft or hard storage tokens.

c. the rules standardized at the end of Annex III thereof

PPYED is defined as the services that have joined the level

trust level 2 must adopt authentication level

at least 1 (K.Y. 9) and the services that have joined the level

trust level 3 must adopt authentication level

at least 1, while authentication level 2 (K.Y. 10) is recommended. The

services that have adopted authentication level 1 must

use as an authentication mechanism at least

21

passwords (K.Y. 11).

13. the processing in question, purpose of registering the data

of students/parents-guardians and teachers of the private schools in

"mySchool" system is the facilitation, but also the improvement of the exercise

graded and hierarchical supervisory authority of the Ministry of Health through the

by place and by material of the competent bodies of the administration of the First Degree and

private education, as provided for in the text

Second grade

legislation.

During the examination of the case it was found that the following apply:

A) Regarding teachers:

From the above provisions and more generally from the current legislation

it is concluded that the competent services of the Ministry of Health have the supervision of the organization

of private schools regarding the teaching staff working in

that's all. Besides, private schools already transmit to the Ministry of Education and Culture based on the text

legislation all categories of teachers' personal data that

are kept in the "mySchool"4 system for public schools, except for those that

are exclusively related to work in a public school, such as e.g. retrospective

appointment, voluntary resignation, intention to resign coc.

Consequently, the data of private school teachers who

is not necessary for the above purpose and by extension for the present case

registration in the system, in contrast to what applies to their teachers

public schools, are as follows: 1. Transfer Area/Organic Position, 2.

Received a Transfer, 3. More than 5 years Secondment to a school abroad, 4.

Five-year term in Standard Experimental Schools (P.P. .) and 5. End of term in

P.P. .. These categories of personal data are not required, according to

provisions of the current legislation, to be registered in the system for them

4 The 44 types of personal data contained in the "mySchool" system are as follows:

Surname, First name, Father's name, Mother's name, Registration number, A.F.M, AMKA Gender,

Date of birth, Employee status, employment status, Degree, Compulsory Education

Time, Gazette of Appointment = Number, Date, publication order, Retrospective Appointment (YES OR

NO), Specialties - Main Specialty, Education Level, Employee Status, MK,

Date of 1st Assumption of Service, Personal File Position, Organic/Temporary

placement, Organic Transfer Area, Supervising Agency, Voluntary Retirement

(checkbox), Intention to Resign (checkbox), Received Transfer (checkbox), Over-5-Year Posting

in a foreign school (checkbox), Five-year term in Standard Experimental Schools (P.P.).

(checkbox), Expiration of Term in P.P. , Address, Area, Postal Code, Municipal Unit, Landline, Mobile,

Other, Email addresses, reductions, Leave, Absences, Teacher assignments to

unit, Working hours details of the employee, Placements in other units.

22

private school teachers. After all, they are not necessarily judged for her

exercising the supervision of the Ministry of Health, the following information: 1. Address, 2. Area, 3.

Postal code, 4. Municipal unit, 5. landline, 6. other telephones and, therefore, the

their registration in the system contradicts the principle of proportionality.

The rest of the data already held in the "mySchool" system for them

public school teachers must, based on the aforementioned

provisions, to be observed also for the teachers of the private schools so that

supervision of the Ministry of Education and Culture to be effective. However, access to

specific users of the system and its manager must have these

of the school unit, the relevant education director, the regional one

director of education in the context of his responsibilities, as well as the central

service of the Ministry of Health. This last service should only have access to

information that is necessary for the issuance of administrative acts related to

the professional status of teachers.

According to the opinion of the member of the Authority K. Christodoulou, its principle

of necessity requires the examination by the Authority of the legality of the

registration in the above system should not be limited to the question of which data

are permitted to be disclosed and forwarded to the Ministry of Health, but to include the

medium of processing. That is, to examine whether the access to these data from

the competent bodies of the Ministry of Education and Culture should not be done through the system

"mySchool", but in other, safe ways, under the supervision of the relevant Administrator

Education.

B) Regarding students:

contrary to what applies to teachers, private schools

they transmitted only statistical data about the students to the Ministry of Education and Culture

they concern the number of departments per class and department, as well as the whole

number of students of each private school. purpose of this transmission is,

among others, the planning of the educational policy by the Ministry of Education.

During the examination of the present case, it was found that especially for the

panhellenic exams and, in particular, for the participation of students in them, from

start of operation of the system and up to now are registered by the

23

private schools in the system 13 of the 90 types of personal data of students

of public schools included in the system5.

Furthermore, a single pupil number has been established for the purpose of uniformity

his identification in order to monitor his course during the school years

of study, regardless of the units or the geographical regions in which

is studying According to the claims of I the purpose of identifying the student

is fully satisfied with the registration of 3 to 4 personal categories

student data: 1. Student's name 2. Student's last name 3. Father's name and 4.

Date of birth. On the contrary, the Ministry of Health claims that all the 90 data that

contained in the system is necessary for its supervisory competence and for

the above-mentioned purpose of establishing the uniform student number. Moreover,

after the start of operation of the system they are registered at the school level

unit (private school) in the system, while he has exclusive access to them

school principal. The central service of the Ministry of Health has access only to

statistical data.

according to the principle of proportionality, as defined above

article 4 of Law 2472/1997, the Ministry of Health must process only the data

are absolutely necessary for the realization of its intended purpose

processing, i.e. ensuring the transparency and reliability of all

from the procedures provided for by law through the unified and direct control by

the Central Administration, but also the better and unified supervision of the Ministry of Health

in all school units. Processing is therefore permitted

only those personal data of students of private schools, the collection

and compliance with which is specifically provided for by the current legislative regime or

is necessary for the exercise of the powers of supervision of the relevant services

of the Minister of State In addition, from the above-mentioned provision of article 4 par. 1 n.

4351/2015 clearly infers the will of the legislator to have the supervision

and the control of the issuance of all types of private degrees

schools by the head of the relevant Directorate of Primary Education.

It is, therefore, necessary to register the students' personal details

5 These are the following student data: 1. First name 2. Surname 3. Father's name 4. Mother's name

5. Date of birth 6. Registration number 7. Municipality of registration 8. Mother's gender 9. Address

student 10. Postal code 11. Telephone 12. school of origin 13. Specialist number

school of origin register.

in order to make it possible to identify their personal information

students when their dismissal certificates are considered by the competent Director

Education.

Against

the above

exposed, in the "mySchool" system legally

the details of the students of the private schools are registered

access to these data by the competent body in terms of material and location

Ministry of Health for the exercise of its supervisory authority, regarding: a) the

performance of the uniform student number, b) the conduct of the pan-Hellenic exams,

as well as c) the consideration of baccalaureate degrees. It goes without saying that the

above relate to the registration and access to the system and do not prevent

the exercise of the supervisory authority of the Ministry of Health, as well as the search

student data.

According to the opinion, however, of the member of the Authority K. Christodoulou, apart from

elements expressly provided for in the current legislation, there is none

other legislative provision, by which it becomes necessary and mandatory h

registration of the remaining data contained in the system. THE

and documentation from the Ministry of Health of the necessity of the registration under consideration

given the students of private schools in the system is general and

vague, despite his relative projected opinion that the entry in question

is inextricably linked to his supervisory competence.

C) Regarding security measures:

The Authority has already pointed out, with Decision 139/2014, that it becomes

it is imperative to maintain a high level of security because in the database

of the "mySchool" system, which is accessible via the Internet,

a large volume of personal data of students/parents is registered-

guardians and teachers of the country.

C1) Regarding the implementation of the 6th recommendation of Decision 139/2014 of the Authority

and the issue of TLS certificate security:

Recommendation 6a of Decision 139/2014, which concerns encryption

of the data of the "mySchool" system (at least the data

identification of the subjects) at the database level, has, according to

relevant response from the Ministry of Health and Welfare and the ITU-Diofantos, already implemented.

25

Regarding the TLS protocol, it is pointed out that it is used for

ensuring the confidentiality of the transmitted data between two

communicating nodes through the encryption of this data (see

Decision 121/2014 of the Authority, available on its website). The

this protocol is provided in versions 1.0, 1.1, 1.2 and 1.3 and is a successor

of the SSL protocol (which is provided in versions 1.0, 2.0 and 3.0). Each one

version of the TLS protocol fixes/mitigates vulnerabilities of the previous ones

publications. it is recommended to avoid using TLS version 1.0 because the

SSL 3.0 vulnerabilities can also be exploited in

case of using the TLS 1.0 protocol, which supports the version

SSL 3.06. Furthermore, the existence of known attacks (such as padding oracle attack,

BEAST attack, Lucky Thirteen attack) sets specific requirements regarding the

use of symmetric encryption algorithms in the TLS7 protocol.

according to the relevant answer of the Ministry of Health and the Ministry of Education and Culture-Diofantos, both

The

central

online

locus

of

system

"mySchool"

(https://app.myschool.sch.gr), as well as the website of the central service

certification of the P D (https://sso.sch.gr) have the protocol installed

TLS 1.2. In order to serve older browsers, who

are built into older operating systems as well which may

still exist in some schools, the corresponding "ciphers" are also supported

(cryptographic algorithms) or older protocols (TLS 1.0).

6 Cf. a) B. Moller, T. Duong, and K. Kotowicz., 2014, “This poodle bites: Exploiting the SSL 3.0

fallback. https://www.openssl.org/~bodo/ssl-poodle.pdf” and b) NIST Special Publication 800-52

Revision 1.

7 If block ciphers are used, the CBC encryption method should be avoided

due to padding oracle attack, BEAST attack and Lucky Thirteen Attack (cf. a) B.

Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux. Password interception in an SSL/TLS channel. In

Advances in Cryptology - CRYPTO 2003: 23rd Annual International Cryptology Conference, Lecture

Notes in Computer Science, vol. 2729, pages 583-599. Springer Berlin Heidelberg, August 2003, b) T.

Duong and J. Rizzo. Here come the xor ninjas. In Ekoparty Security Conference, 2011 and c) N. J.

Al Fardan and K. G. Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. In IEEE

Symposium on Security and Privacy, pages 526-540, May 2013).

Also, the RC4 algorithm should be avoided, because if used they can

other attacks take place, due to inherent weaknesses of RC4.

(see a) N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, and J. C. N. Schuldt. On the

security of RC4 in TLS. In Proceedings of the 22d USENIX Conference on Security, S, pages

305{320. USENIX Association, August 2013 b) K. G. Paterson, B. Poettering, and J. C. N. Schuldt.

Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited

Paper), pages 398{419. Lecture Notes in Computer Science, vol. 8873. Springer Berlin Heidelberg,

December 2014).

From a relevant overview, when examining the case at hand,

it seems that, both the above websites, and the websites

https://myschool.sch.gr/ (initial website that leads to the online

location of the central certification service without appearing to be taking place

through

his

processing

personal

data),

https://register.sch.gr/password/change_password/

(change website

password of P D) and https://register.sch.gr/password/reset_password/

(P D password recovery website), have

TLS 1.2 certificate. Additionally, the browser security reviews

Chrome reports for all of their websites above

designations "strong cipher" ("strong encryption") and "strong key

exchange" ("strong key exchange").

Recommendation 1: The HYPETH and ITYE-Diofantos, as far as the

accordingly, they must ensure that there is no possibility of support

of the previous versions of the TLS 1.2 protocol, i.e. 1.0 and 1.1 in

any of the websites that support the feature

of the "mySchool" system, as well as not to use the

cryptographic algorithms already blocked in its version 1.3

TLS protocol. The Ministry of Health must ensure the appropriate adjustment

of the computers of the school units and the administrative structures that

are used to log in to the "mySchool" system.

C2) Regarding the implementation of recommendation 6g of Decision 139/2014 of

Principle:

The Ministry of Health and the ITU-Diofantos clarified with the no. first

C/EI /7689/08-12-2014 document (which was sent to the Authority following the

Decision 139/2014), the no. prot. G/EI /8320/16-12-2016 document (which

sent after the no. original C/EX/7648/23-11-2016 of the Authority's document,

in the context of examining compliance with Decision 139/2014) and under

no. prot. G/EI /1964/10-3-2017 memo (concerning the

complaint) that the restriction on access (i.e. access to "mySchool"

only from IP addresses of Π D) set by the implementation of its recommendation 6g

of Decision 139/2014 is not a realistic option for the "mySchool" system

27

for the reasons set forth in these documents and listed in her history

present.

It is pointed out that electronic government systems, as indicative

the Electronic Prescribing system and the taxisnet system, in which

a huge amount of personal data is processed (in the first place

data of special categories related to health and the second data which

are protected by tax secrecy and are used for the provision

services for carrying out financial transactions electronically) and

which have common features with the "mySchool" system (such as

access the system via the internet using a TLS certificate and use

passwords as a user authentication mechanism), provide them

corresponding services without restricting users' access.

Furthermore, the personal data processed in

"mySchool" system, as it appears from the situations with the personal ones

data of students, parents/guardians and teachers sent to

Authority from ITYE-Diofantos, in accordance with Decision 139/2014 (which does not

allows the registration of his special category data in "mySchool".

student's individual health record), usually include "simply"

personal data, with the exception of the religion of students in specific,

cases provided for by law (see paragraph 4 of Decision 139/2014). e

each case, whether the services provided are included in the level

confidence level 2 ("simple" data) or at level 3 (expert data

categories), must be adopted, according to

the PPYEDN, level

authentication of at least 1 (which it must use as a mechanism

authentication

by

minimum

passwords),

while

the

level

authentication 2 is recommended for trust level 3. The system

"mySchool" implements authentication level 1, i.e. passwords, according to

provided for in the PPYID.

Recommendation 2nd: Following these and because the "mySchool" system implements

at least authentication level 1 and, as specified by the Ministry of Health and

the ITYE-Diofantos, it is not possible to limit access only to IPs

addresses of the P D for its proper operation and proper utilization

system, it is considered that two authentication implementation should be considered

factors (two-factor authentication), for the connections made

in the "mySchool" system from IP addresses outside of Π D and be updated

regarding the Authority. in case of non-application of this method

authentication, the reasons must be justified.

C3) For the additional issues raised by I with no. first

G/EI /2665/29-3-2017 his memorandum regarding the security of the system

"mySchool", the following are listed:

C3(a) regarding the authentication of users of the "mySchool" system:

The issues that were raised with the above memorandum regarding the

user authentication and trust level mapping

of the provided service and authentication level, (see its history

present), were examined in point C2 of the reasoning of this decision.

Regarding the encryption of users' passwords, in accordance with

responses of the Ministry of Health and the Ministry of Health and Welfare-Diofantos (see history of the present), the

passwords of the users of the "mySchool" system are encrypted by P D.

Additionally, from an overview of the website's login interface

https://sso.sch.gr/login when examining the case at hand, it seems not

CAPTCHA is used and it is possible to copy and paste them

codes in the respective fields. It is pointed out that the input interfaces of all

of websites mentioned, for comparative purposes, by I

(Eurobank bank - https://ebanking.eurobank.gr/ebanking/login.faces) and the

MINISTRY OF

and

ITYE-Diofantos

(banks

National

https://ibankretail.nbg.gr/sts/Account/Login/web, Alpha

https://www.alpha.gr/e-

banking, Piraeus https://www.winbank.gr/sites/idiwtes/el/Pages/default.aspx and

taxisnet https://login.gsis.gr/mylogin/pages/login.jsp), do not apply CAPTCHA

on the respective input interfaces and allow copying – pasting of them

codes (as seen after reviewing the above websites,

also, when examining the case at hand). In addition, it is noted that

according to reports8, Google disputed that CAPTCHA, which

8 Cf. indicatively http://tech.in.gr/news/article/?aid=1231368514, http://www.independent.co.uk/life-

style/gadgets-and-tech/news/google-captcha-re-robot-image-recognition-artificial-intelligence-website-

a7627331.html,

https://gizmodo.com/google-has-finally-killed-the-captcha-1793190374

29

generally considered annoying by the online community, it can now be

guarantee security, as there are algorithmic methods that yield the

garbled text with high accuracy and introduced the reCaptcha mechanism

(https://www.google.com/recaptcha/intro/invisible.html). In addition, it is noted that

the "mySchool" system provides for the "locking" of the account after one

number of repeated failed connection attempts.

Recommendation 3: Following these, the Ministry of Health and the ITU-Diophantos, according to

part that belongs to him, they must send in writing to the Authority documented

opinion on the issue of whether a) the user input interface to the system

"mySchool" is vulnerable to attacks because it does not have CAPTCHA and allows

the copy-pasting of the codes in the respective fields and b) is

necessary for the "mySchool" system to disable the possibility of

users' browsers to save the password when logging in,

taking into account that for connections other than Π Δ it is recommended to examine it

two-factor authentication application. If so, you must

ensure the implementation of the above.

C3(b) in relation to the 6g recommendation of Decision 139/2014 of the Authority:

The issue that was raised with the above memorandum of I regarding the

interception of their usernames and passwords

users, who connect to the "mySchool" system from IP addresses other than

of P D (from any computers infected with viruses with old

operating systems, which may be at home, in an internet cafe, with

use of free wi-fi as well as mobile phones and tablets) (see history

of this) is covered by point C2 of the reasoning of this decision.

Besides, the issue that was raised in the above memorandum of I, that the use

of the "mySchool" system outside standard working hours contravenes

labor legislation, escapes the competences of the Authority.

C3(c) regarding the Security Policy of the "mySchool" system:

I, based on the content of the Security Policy, with the above

his memo referred to shortcomings of the Security Policy and claimed

that the "mySchool" system is not properly designed to prevent

threats during the registration process and appears to be vulnerable to many

attacks, as these are not provided for in the Security Policy (see

history of the present). It is pointed out that, however, shortcomings (of the content)

of the Security Policy do not demonstrate/document without other application

of missing or insufficient security measures or that the system is vulnerable to

attacks.

Recommendation 4th: Therefore, the Ministry of Health and the Ministry of Education and Culture - Diophantos must

ensure the revision and updating of its Security Policy

of the "mySchool" system, so that the

rules and the procedures followed. Also, there must be

mapping between the procedures and rules reflected in

Security Policy and security measures applied to the system. THE

Security Policy must be reviewed on a regular basis and updated

about the users (such as by posting the Security Policy on the internet

site of the "mySchool" system). Especially for the procedures of creating a new one

account in the "mySchool" system and retrieving access information

care must be taken so that the account details

are sent exclusively to the users they concern (such as

individual email accounts of these users)

C3(d) regarding the education of the users of the "mySchool" system:

I claims with his memo that the users of the system

"mySchool" is not trained in security matters (see its history

present).

With the nos. prot. G/EI /8320/16-12-2016 and G/EI /1964/10-3-2017

documents, the Ministry of Health and the ITU-Diofantos informed the Authority that they have

programmed information days regarding the

operation of the "mySchool" system in all educational districts with

participation of the directors of the school units of each region and others

interested teachers. the said meetings were presented

issues of security and protection of personal data.

Also, the request to create a new account in the system includes

terms of use and confidentiality statement. the terms of use state that a)

the provided login account pertains to the specific user and

is used exclusively by him, b) disclosure to

and the use of the code by third parties and c) the electronic actions of users

are recorded with the aim of protecting the correctness of the data and

avoiding violation of legal rules. In addition, every user who logs in for

the first time the system is informed about the terms of use of the account and

must read the provisions of the confidentiality statement. Only then

can proceed to use the system. with next connection, the

pop-ups do not appear, but exist as links at the bottom

part

her

interface

of

system

("Terms of use",

"Declaration

Confidentiality").

according to the HYPETH and ITYE-Diofantos, since the platform does not

subject to changes affecting security issues, the updating of

users on matters of safe use of the application and the update regarding it

use of accounts, both during a user's application process and in

final rendering of the account by P D, is sufficient and substantial, so

managers and other users to be fully aware of their importance

security issues and the principles that should govern their preservation

accounts and their passwords. For these reasons, no guide was drawn up

users on security issues.

Also, it is stated that with a frequency of at least twice a year

there is an update to the users from the SSO service of P D in relation to him

password and its security and attached to answer one

such informational message.

The above attached informative message appears to contain

informing users to recognize and avoid misleading messages

"phishing" type and misleading password interception websites

access, management of unsolicited electronic communication messages

(spam), as well as information about the possible deception of users and

installing malware on their computers.

the website of the Central Certification Service of P. D

(https://sso.sch.gr/safetyInfo.jsp), which is used for authentication

of the users of the "mySchool" system, there are posted instructions

safe use of the services of P D, which concern authenticity

32

of the service page, the protection and non-disclosure of the password and

her

safe

log out

from

her

service. Also,

at

page

http://www.sch.gr/password of Π D for changing their passwords

users there is a "Safety and Protection" section, which includes

following user information sub-sections: protection against misleading

messages, security and virus protection instructions, virus protection

in mail, latest virus update, firewall

(firewall), spam protection, mail blocking

(rbl), internet security.

Recommendation 5th: Following these, the Ministry of Health and the ITU-Diofantos must,

at a minimum, to draw up a single guide, in which it can be found

gathered all the information required to inform users

of the "mySchool" system in matters of security and personal protection

of data and which must be easily provided to users (such as with

posting on the website of the "mySchool" system).

C3(e) regarding availability problems of the "mySchool" system:

I's reference to a single case of system failure

"mySchool", i.e. from 23.30 on 16.3.2017 until the morning of the following day, does not

substantiates his claim that this system presents problems

availability or general security issue.

7f) in relation to the lack of possibility of mass input of the data in

"mySchool" with xml files:

The provision of bulk import functionality/capability of

data from the information systems of the private schools in the system

"mySchool" with xml type files helps to facilitate its operation

of the "mySchool" system, and no protection issue is mentioned by I

and safe processing of personal data.

C3(g) regarding the ability to search and find in the "mySchool" system

of the data, including the AMKA, private teacher:

according to the above memorandum of I, the "mySchool" system provides

ability to search and find all private tutor details,

including this AKMA, with only the registration of the VAT number

of the teacher in the said system (see history of the present).

33

according to the user manual of the "mySchool" system, according to

using the functionality "Add new employees for private schools"

it is allowed to search for a teacher based on his tax identification number. the above manual

it is written that "(...) In your case the Educationist already has the PS

"mySchool", the site supports its components and you have the

possibility to recommend the unit to him (…) In case the Educator

"mySchool" does not exist, then fill in its details and

prefix the unit let (…)'. The details of the teacher, according to

upper handbook, include in terms of the basic elements the surname, the first name, the

father's name, mother's name, date of birth, VAT number, AMKA,

the gender and in terms of the official data the status of employee, the relationship

work, the hours of compulsory teaching hours at the institution and

the specialty.

Furthermore, according to the answer of the Ministry of Health and the ITU-Diofantos

to the Authority, based on the role assigned to him, the director of the school unit

has access to the data of teachers serving in the school unit

(and only in relation to the current service). However, it appears that

at least, when using the above functionality, it can have access

in data of teachers of the other school units. therefore must

examine whether, through the above search facility, it can and is

necessary to have access to the data of teachers of other schools

units.

Recommendation 6: Following these, the Ministry of Health and the Ministry of Education and Research - Diophantos must

to clarify, if the role of the director of the school unit has

access to the data of the teachers of other school units. e

affirmative case, it must be clarified why this is necessary

and to inform the Authority about the possibility of restricting access

only in the data of the teachers of the relevant school unit.

C3(h) in relation to recommendation 6b of Decision 139/2014 of the Authority:

the above note of I is mentioned, in relation to its 6b recommendation

Decision 139/2014, according to which the Ministry of Health must "(...) b) To

care is taken to include the possibility of creating individual

accounts of single users to be assigned by properly authorized persons

34

teachers of each school unit and employees of each administrative department

structure such as address or regional address, in order to avoid any common

use of my unique account attributed to the college director

unit or the administrative structure to carry out all the tasks that

the side of the "mySchool" (…) service is required, that it is known throughout

the educational community that "mySchool" is used by at least

three employees of each Education Directorate or each Regional Directorate,

except for the responsible Director. The result is that all of the above

user ID and password may be shared.

The above claim of I regarding the use of the manager's account

by other employees of the above education departments is not documented with

specific elements.

according to the response of ITYE-Diofantos to the Authority, in the school ones

units, an individual access account is assigned to the manager of each

unit and it is possible to assign an individual access account to

responsible teachers of departments, as they are designated by its director

of each school unit. Also, an individual access account is attributed to

Regional Directors of Education, as well as to the Directors

Primary and Secondary Education Directorate. The above

accounts have the access rights derived from the corresponding one

role they belong to.

From the above and from all the data provided

it appears that in the "mySchool" system there is no possibility of rendering individual results

access accounts to employees of the above education departments

(besides managers).

Recommendation 7th: Following these, the Ministry of Health and the ITU-Diofantos must,

due to recommendation 6b of Decision 139/2014 of the Authority, clarify a) whether

the ability to assign individual access accounts to

additional employees of the above education departments and b) in the affirmative

case why this possibility has not been implemented.

C3(i) regarding the connection of the "mySchool" system to the database

of the National Census:

35

in his above memo, I states that the interconnection of the base

data from the "mySchool" system based on the National Census (see

point B of the history of the present) creates questions regarding her

security and protection of personal data.

First of all, it is pointed out that the interface of the "mySchool" system with

the central database of the OP ED of the National Census is foreseen

in no. KYA 1493 (Government Gazette B 298 12-02-2016). Regardless, no

it turns out that there are risks to the protection of personal

data due to the connection with the database of the National Census,

the above claim of I is not substantiated..

7j) regarding the database and encryption codes:

I, in his above note, states that he was informed that the

only one person has database and encryption passwords.

The above

irrefutably.

I's claim is not substantiated and presented

C3(k) regarding the preparation of an impact assessment study:

Regarding I's proposal that the Authority request the Ministry of Health to

conduct an impact assessment on

data protection

it is pointed out that the obligation to carry out an impact assessment in a system that

already in operation is documented by the controller based on Article 35

par. 1, 2 and 4 of the GDPR. therefore, the Ministry of Health must examine the compliance

of with the above article.

FOR THOSE REASONS

The beginning:

1. Rejects I's complaint for the reasons detailed in

this decision.

2. Considers that:

A. It is legal to enter only the data in the "mySchool" system

of private school teachers deemed necessary for the purpose

the exercise of the hierarchical and graded supervision of the Ministry of Health, such as these

described above, with access to them only by users

referred to herein (see s. 13A).

B. It is legal to register their data in the "mySchool" system

of students/parents-guardians of private schools, the collection and observance of

which are specifically provided for by the current legislative regime or are necessary

for the exercise of supervisory powers of the relevant services of the Ministry of Health,

as these are described above, with access to them only from

the users referred to herein (see section 13B).

C. The HYPETH, as controller and ITYE-Diofantos, as executor

processing, they must also apply the recommendations mentioned

in point 13C of the rationale of this decision and to inform her

Authority within three months of its notification by submitting detailed

implementation schedule of these recommendations.

The president

The secretary

Konstantinos Menudakos

Irini Papageorgopoulou