GREEK EMPIRE

PRINCIPLE OF PROTECTION OF E OMEN

OF A PERSONAL CHARACTER

Athens, 09-11-2018

Prot. No.: G/EX/7022-2/09-11-2018

A P O F A S I NO. 67/ 2018

(Department)

The Personal Data Protection Authority met in composition

Department following an invitation from its President to its headquarters on Wednesday 7-11-2018,

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

They were attended by the Deputy President, Georgios Batzalexis, who was in his way

of the President of the Authority, Constantos Menoudakos, Constantos Lambrinoudakis,

regular member, and the alternate members Panagiotis Rontogiannis, as rapporteur, and

Grigorios Tsolias, replacing the regular members Antons Symvonis and

Charalambou Anthopoulos, respectively, those who, although only summoned in writing, did not

attended due to obstruction. The meeting was attended by the order of the President

Georgios Rousopoulos and Constantos Limniotis, expert scientists – auditors, as

assistant lecturer. Irini also attended, by order of the President

Papageorgopoulou, employee of the Administrative Department of the Authority, as secretary.

The Authority took into account the following:

It was submitted to the Authority by the company "DIMERA GROUP EMPORIO

SPORTING GOODS SOLE INDIVIDUAL LIMITED LIABILITY COMPANY"

(hereinafter, DIMERA) the no. prot. C/EIS/7022/27-08-2018 notification of incident

personal data breach, according to art. 33 of the General

of Regulation (EU) 2016/679 (General Data Protection Regulation - hereinafter, GDPR).

According to the notification in question, the incident involved a security attack or

which was the result of malicious external action ("hacking"). The one in question

incident, which was no longer ongoing at the time of its submission

disclosure, results in a breach of data confidentiality

of the company's customers. DIMERA submitted the above notification to the Authority within 72

hours from the moment he became aware of the incident. In this notice – the

its detailed information as described in its confidential appendix

present – describes the type of personal data of which n

confidentiality was breached, the number - approximately - of those affected by it

incident of individuals, the number of affected files with personal data, the

security measures that had been implemented before the said incident as well as the measures

which were taken immediately after the incident with the aim of its effectiveness

treatment. Furthermore, the notification describes the way in which

DIMERA became aware of the incident, the assessment made by DIMERA is recorded

acted as to the seriousness of this, while it is also stated that DIMERA will

inform the data subjects whose data has been leaked.

To this end, it is pointed out that the updating process has already started at the time

that the notification in question was submitted to the Authority and with its completion it will

followed by the submission of a supplementary notification.

Subsequently, DIMERA submitted the supplement no. first

C/EIS/7098/30-08-2018 notification about the incident in question. With this news

notification – the detailed information of which is further described in

confidential annex hereto – the number of which is specified

of affected persons, copies of the electronic messages are attached

mail with which the persons in question received personalized information from the

DIMERA for the incident in question as well as guidance on the actions to be taken

their turn to do so as not to be affected by the incident in question, while
also, it is presented with an enriched - in relation to the initial disclosure - in
technical measures adopted by DIMERA after the incident in question.
Based on the information contained in the above two notifications, the Authority
sent DIMERA the no. prot. C/EX/7022-1/21-09-2018 document requesting
clarifications on issues related to the measures that were in force before the incident
in order for such events to be detected in time, as well as
more specific topics of our specific treatment (such as what exactly was the
underlying information flow of DIMERA's customer data as follows
used its online service, clarification of various techniques

issues in relation to updated or non-updated versions of internet protocols
sure let's etc.). DIMERA replied to the Authority with the no. original G/EIS/7789/02-
10-2018 document, in which he provided clarifications on these issues.
More detailed information on the above documents is described in the confidential
annex hereto.
The Authority, after examining all the elements of the file, after listening to him
rapporteur and the clarifications of the assistant rapporteurs, who then left
before conference and decision, and after thorough discussion,
THOUGHT ACCORDING TO THE LAW
1. The GDPR, which replaced Directive 95/56/EC, has been in force since 25
May 2018. Article 4 of the GDPR states that "personal data" yes yes
"any information concerning an identified or identifiable natural person (subject
of data)". In the same article, it is also defined as processing "each act or series."
operations carried out with or without the use of automated means, in data
of a personal nature or in sets of personal data, such as collection,

record, organize, structure, store, adapt or change,

retrieval, information search, use, communication by transmission, dissemination

any other form of provision, association or combination, limitation, deletion or

destruction". Furthermore, anyone (the natural or

legal person, public authority, agency or other body) which, "alone or jointly with

another, determine the purposes and manner of processing personnel data

character".

In the second article, the breach of personal data is defined as "

breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorized disclosure or access to personal data transmitted,

stored or otherwise processed'.

2. The principles governing the processing of personal data are defined

in article 5 para. 1 of the GDPR – among them, as indicated in article 5 para. 1

item in this, personal data are processed

way that guarantees the appropriate security of personal data,

among others their protection from unauthorized or illegal processing and

accidental loss, destruction or damage, using appropriate techniques or

organizational measures ("integrity and confidentiality"). Further, in paragraph 2

of the second article, it is stated that the person in charge of processing shall bear the responsibility and yes to

position to accept compliance with paragraph 1 ("accountability").

3. According to article 32 of the GDPR, "taking into account the latest developments, the

implementation cost and nature, scope, context and purposes of

processing, as well as the risks of different possible outcomes and

seriousness for the rights and freedoms of natural persons, the person in charge

processing and the processor apply appropriate technical and organizational

measures to ensure an adequate level of security against risks,

including, among others, in case of: (...) d) procedure for t n tactics

testing, evaluation and evaluation of technical and organizational effectiveness

measures to ensure the security of the processing". Moreover, in paragraph 2

of this, it is stated that "according to the assessment of the appropriate level of security

the risks deriving from the processing are taken into account in particular, especially from accidental or

illegal destruction, loss, alteration, unauthorized disclosure or access

personal data transmitted, stored or submitted by

otherwise processed".

4. With reference to the incident of personal data breach, o

GDPR sets specific obligations for data processors. Specifically,

in article 33 thereof, it is stipulated that in the event of a personal data breach

nature, the controller shall notify us immediately and, if possible, within 72

hours from the moment it becomes aware of the fact of the data breach

of a personal nature to the competent1 supervisory authority, unless the data breach

of a personal nature may not cause a risk to the rights and

liberties of natural persons. When the notification to the supervisory authority does not

carried out within 72 hours, accompanied by a justification for the delay.

In paragraph 3 of article 33, it is stipulated that this notification as a minimum: a)

describes

the

nature

her

violation

data

personnel

character,

including, where possible, categories and approximate

number of affected data subjects, as well as the categories and

of the approximate number of affected personnel data records

1 Taking into account article 55 of the GDPR regarding the competences of the supervisory authorities, responsible for the

due to the incident yes the Personal Data Protection Authority

character, b) announces the name and contact details of the person in charge

data protection or other point of contact from which they may be obtained

more information, c) describes the possible consequences of the violation of

personal data, d) describes the received or proposed to

taking measures by our processor to deal with the violation of

of personal data, as well as, where appropriate, mitigation measures

of its possible adverse consequences. In case and since it is not possible to

information is provided simultaneously, it can be provided gradually without

unjustified delay.

According to article 34 of the GDPR, when the personal data breach

character may put their rights and freedoms at high risk

natural persons, our controller shall immediately notify the violation of

of personal data to the data subject. In this

notification clearly describes the nature of the personal data breach

character and contain at least the information and measures referred to in

article 33 paragraph 3 letter a b), c) and d) (see above). The announcement at

data subject is not required if any of the following are met

conditions: a) the person in charge of processing shall apply appropriate technical and organizational measures

protective measures, and those measures were applied to those affected by the breach

personal data, etc. as measures that make the data unintelligible

of a personal nature to those who do not have permission to access them, such as

encryption, b) the controller subsequently took measures to ensure

that it is no longer likely that a high risk will arise for the rights and

liberties of data subjects, c) requires disproportionate efforts

(in which case, in this case, a public announcement is made instead or there is

similar measure to which data subjects are informed about you

efficient way).

5. In this case, DIMERA was our processor, v

the meaning of art. 4 of the GDPR (see item 7 thereof). Further, from its elements

of the case file shows that DIMERA complied with its obligations

data processors that derive from the aforementioned articles 33 and 34 of

GDPR regarding the management of personnel data breaches

character, given that:

a) submitted the relevant notification to the Authority, within seventy-two (72) hours from

5

upon becoming aware of the incident,

b) the notification as a whole, as completed, provides all the information

required under art. 33 of the GDPR,

c) immediately carried out an assessment of the risks for the affected subjects

data due to the incident and updated them, in accordance with

what is provided in relation to art. 34 of the GDPR.

6. DIMERA described in detail to the Authority the new measures it took, after

incident, in order to counter the attack and create one

safer environment for the future. Besides, immediately as soon as DIMERA was informed

for the incident, took actions both to investigate the generative causes

of the incident as well as for taking appropriate measures in order to stop the

specific attack for sure. Also DIMERA, in the aforementioned no. first

C/EIS/7789/02-10-2018 her document, states that before the incident in question she had

deciding on the full adoption and implementation of technical and organizational measures, some

of those that have already taken place. Further, DIMERA states that similar

security attack, which was a new type of attack, other

large businesses in Europe, especially during the period of the attack

surely it also took place against DIMERA – mentioning some specific ones

cases.

From the analysis of the security measures that DIMERA has taken before

incident, compared to the measures taken after the incident, and taking

also taking into account the way in which he became aware of this2, it follows that DIMERA –

and he had already adopted technical security measures – he did not have the appropriate ones

mechanisms for early detection of such type of security attacks and, by extension,

to prevent them as effectively as possible. Furthermore, he has not received it

necessary care to update the software used and immediately

application of its security updates. It should also be noted that by nature

of our specific processing of personal data (as detailed in

confidential annex hereto), it appears that a possible data breach

may put the rights and freedoms of individuals at high risk

of persons – as was also the case in the present case – and, consequently, n

DIMERA owed as our editor, taking into account these high

2 All relevant information is described in the confidential annex hereto

risks, to implement

appropriate measures for

the treatment

their,

including the regular testing and evaluation of their effectiveness

technical and organizational measures for the security of our processing. Therefore, based on

of these, there was a violation of the provisions of art. 32 of the GDPR and, consequently, of

fundamental principle of data security (art. 5 par. 1 item f of the GDPR).

7. In view of the above violations found, and also taking into account

that, on the one hand, the data controller acted promptly in dealing with

of the incident in compliance with all the obligations arising from it

GDPR regarding incidents of personal data breaches, and

on the other hand, that the security attack in question was a new type of attack, the Authority considers

unanimously that he must exercise the right provided for in article 58 par. 2 sec. II GDPR

its authority, as stated in the operative part of the present, and the same is removed

with the gravity of the violations.

FOR THOSE REASONS

The Authority taking into account the above:

Addresses based on no. 58 par. 2 b' of Regulation (EU) 2016/679 attack

at DIMERA GROUP TRADE OF SPORTING GOODS SOLE REPRESENTATIVE COMPANY

LIMITED LIABILITY for the violation of the provisions of art. 32 of the Regulation

(EU) 2016/679 and, by extension, of art. No. 5 par. 1 item in this.

The Deputy President

The Secretary

George Batzalexis

Irini Papageorgopoulou