PERSONAL DATA PROTECTION AUTHORITY Athens, 29-05-2019 Prot. No.: G/EX/3834/29-05-2019 DATE 14/2019 (Department) The Personal Data Protection Authority met in composition Department at its headquarters on 02-06-2019 at 10:00 a.m. upon the invitation of its President, in order to examine the case referred to in the present history. The Deputy President, G. Batzalexis, who was in the way of the President of the Authority, K. Menoudakos, and the alternate members of the Authority E. Papakonstantinou and P. Rontogiannis, as rapporteur, in place of the regular members K. Lambrinoudakis and Ant. Simvoni respectively, who, although legally summoned in writing, did not attend due to disability. The regular member of the Authority X. Anthopoulos and his alternate member Gr. Tsolias, although they were legally summoned in writing, did not attend due to disability. Present without the right to vote were G. Panagopoulou, special scientific auditor, as assistant rapporteur, who left after the discussion of the case and before the conference and decision-making, and E. Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: The Authority received the no. prot. C/EIS/8105/12-10-2018 notification of an incident of personal data breach by "Biomedical Diagnostic Center S.A." (hereinafter "controller") describing the accidental sending of medical examination results of an examinee to 1 third party . The sending channel was not clearly specified, it may have been sent by e-mail or by facsimile (fax). In this regard, the Authority has previously issued decision 164/2014 in which it issued a strict warning to the data controller to comply with the requirements of Article 10 of Law 2472/1997 on the privacy and security of processing, following a complaint that blood test results may to be sent by e-mail to a third party. Then, the Authority with no. prot. C/EX/8686/02-11-2018 call invited the controller to attend the meeting of the Department of the Authority on 21-11-2018, in order to discuss the above issue. During the hearing on 21-11-2018, A, Financial Director and B, IT Consultant, appeared on behalf of the data controller, while from the law firm Nikos Kanellopoulos – X. Zerva and Associates, which has been designated as the data protection officer of the data controller , Hara Zerva and Hera Hioni performed. After the opinions of the participants were developed orally, then the data controller submitted with no. prot. G/EIS/9631/31-10-2018 memorandum. The memorandum states that the specific incident concerns a single case of human error, with minor consequences, after an exam result was faxed to the wrong recipient with the same first and last name. The procedures applied for sending the results of medical examinations by e-mail are also described in their entirety, taking into account the recommendations addressed by the Authority with decision 64/2014. The Authority, after examining the elements of the file, the hearing and after hearing the rapporteur and the assistant rapporteur, who withdrew after the discussion of the case and before the conference and

decision-making, after a thorough discussion, CONSIDERED LAW 1. The GDPR, which replaced Directive 95/56/EC, has been in force 2 since 25 May 2018. Article 4 of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person (data subject)'. The same article also defines as processing "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or alteration, retrieval, retrieval of information, use, communication by transmission, dissemination or any other form of disposal, association or combination, limitation, deletion or destruction". Further, a controller is defined as anyone (the natural or legal person, public authority, agency or other entity) who, "alone or jointly with another, determine the purposes and manner of processing personal data". The same article defines a personal data breach as "the breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". 2. The principles governing the processing of personal data are defined in article 5 par. 1 of the GDPR - among them, as pointed out in article 5 par. 1 item in this, personal data are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or deterioration, using appropriate technical or organizational measures ("integrity and confidentiality"). Furthermore, in paragraph 2 of the same article, it is stated that the controller bears responsibility and is able to demonstrate compliance with paragraph 1 ("accountability"). 3. According to Article 32 of the GDPR, "taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and liberties of natural persons, the controller and processor implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, in case 3: (…) d) procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing". Furthermore, in paragraph 2 thereof, it is stated that "when assessing the appropriate level of security, the risks deriving from the processing are taken into account, in particular from accidental or illegal destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed'. 4. With regard to incidents of personal data breaches, the GDPR defines specific obligations for data controllers. Specifically, in article 33 thereof, it is defined that in the event of a personal data breach, the data controller shall notify the competent1 supervisory authority immediately and, if possible, within 72 hours of becoming aware of the personal data breach, except if the breach of personal

data is not likely to cause a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay. Paragraph 3 of Article 33 states that this notification shall at least: a) describe the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects, as well as the categories and of the approximate number of affected personal data files, b) announces the name and contact details of the data protection officer or other contact point from which more information can be obtained, c) describes the possible consequences of the personal data breach, d) describes the measures taken or proposed to be taken by the data controller to deal with the personal data breach, as well as, where appropriate, measures to mitigate its potential adverse consequences. In the event that it is not possible to provide the information at the same time, it can be provided gradually without 1 Taking into account Article 55 of the GDPR on the powers of the supervisory authorities, the Personal Data Protection Authority is responsible for the incident in question 4 unjustified delay . Pursuant to Article 34 of the GDPR, when the breach of personal data may put the rights and freedoms of natural persons at high risk, the data controller shall immediately notify the data subject of the breach of personal data.

This notice clearly describes the nature of the breach

personal data and contains at least the information and

the measures referred to in article 33 paragraph 3 items b), c) and d) (cf.

above). Notification to the data subject is not required if

any of the following conditions are met: a) the person in charge

processing implemented appropriate technical and organizational protection measures, and

these measures were applied to the data affected by the breach

of a personal nature, mainly measures that render 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 which

ensure that a high risk is no longer likely to arise for the

rights and freedoms of data subjects, c) assumes

disproportionate efforts (so, in this case, it is done instead

public announcement or there is a similar measure by which the subjects of

data are updated in an equally efficient manner).

5. In this case from the data of the case file

it follows that the data controller has complied with the obligations of

data controllers which derive from the aforementioned articles 33 and

34 of the GDPR regarding the management of data breach incidents

of a personal nature, given that:

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

from the moment he became aware of the incident,

b) the disclosure as a whole, as completed, provides all

information required under art. 33 of the GDPR,

c) immediately carried out a risk assessment for the affected subject

of the data due to the incident and updated it,

in accordance with the relevant provisions in art. 34 of the GDPR.

7. In view of the above, there does not seem to be any issue in relation to

management of the specific individual incident as well as with the

adaptation of the person in charge to the recommendations of decision 64/2014.

FOR THOSE REASONS

The Authority considers that for the case examined it is not required to exercise

some of the corrective powers provided for in article 58, paragraph 2 of the GDPR

her.

The Deputy President The Secretary

Georgios Batzalexis Irini Papageorgopoulou