Athens, 03-08-2022 Prot. No.: 1963 DECISION 36/2022 (Department) The Personal Data Protection Authority met at the invitation of its President in a Department meeting via video conference on Wednesday 06.08.2022 at 10:00, in order to examine the case referred to in the present history. Georgios Batzalexis, Deputy President of the Authority, and the regular members of the Authority, Konstantinos Lambrinoudakis and Grigorios Tsolias, were present as rapporteur. Present, without the right to vote, were Chariklia Latsiu, DN - legal auditor, as assistant rapporteur and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: With the complaint dated 31.05.2021 (and with no. prot. APD C/EIS/3559/31.05.2021) A informed the Authority that she submitted to the diagnostic center PRIVATE POLYSIS AND DIAGNOSTIC CENTER OF PYLIS AXIOU I.A.E the request from 08.02.2021, with which he requested to receive copies of the images included in the medical file of the Center and related to the digital mammography carried out on ...01.2018, in addition to its conclusion. The Center, with its reply dated 09.02.2021, informed A that: "it is not possible to reprint images from the machine you performed the exam in January 2018. This particular machine had the ability to store a 3-month file and for this reason we in his replacement". Following this, A complained to the Authority that the right of access to personal data concerning her was violated, and 1-3 Kifisias Ave., 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr 1 specifically , that she was not given copies of the imaging tests of the digital mammography performed on ...01.2018, highlighting, moreover, that this is an important gynecological examination, which serves, due to her age and state of health, as a reference examination. The Authority, during the examination of the above complaint, called under no. prot. APD C/EXE/1496/15.06.2021 document the PRIVATE POLYSIS AND DIAGNOSTIC CENTER OF PYLIS AXIOU I.A.E. (hereinafter diagnostic center) as it submits specific clarifications on the complainants. Subsequently, the diagnostic center with the request from 01.07.2021 (and with no. prot. APD C/EIS/4330/01.07.2021) asked to accept the postponement request for the submission of opinions on a different day. Following this, the Authority with no. prot. APD C/EXE/1717/15.07.2021 document accepted the request to postpone opinions, and called the diagnostic Center: "(...) if in the meantime the disputed digital mammogram from ...01.2018 is found, please proceed without delay to grant a copy of this to the complainant, in satisfaction of the right of access to her personal data". In response to the Authority's above documents, the diagnostic center informed the Authority, among other things, that: "(...) The machine with which the digital mammography examination of the complainant was carried out on ...01.2018, indeed, as we answered the complainant herself, does not have the ability to reprint images. The produced images were stored locally on the specific machine for a period of approximately three (3) months from

the date of their processing and were simultaneously stored on hard disk systems, which were kept in a warehouse within the diagnostic center. We searched for and located the hard drive system on which the complainant's digital mammogram image is stored. This is a NAS hard disk system, which contains images from CT scans, MRIs, mammograms and X-rays, which have been performed during the period from March 2017 to March 2018 in our diagnostic center (…)". In addition, the diagnostic center informed the Authority that it has approached Northwind Data Recovery and 2 Stellar security companies in order to, it claims, exhaust all the possibilities offered by technology to recover the files contained in the company's hard disk system in best possible form and quality. Subsequently, the Authority with sub. No. prot. C/EXE/263/02.02.2022 and C/EXE/264/02.02.2022 documents invited A and the diagnostic center, respectively, to be presented at a meeting of the Department of the Authority on Wednesday 09.02.2022, in order to discuss the aforementioned complaint. In addition, with the above under no. prot. C/EXE/264/02.02.2022 document the Authority informed the diagnostic center that in the context of examination of the complaint it is checked ex officio in relation to the fact of the lack of availability of the personal data of the complainant and its general compliance with the processing obligations, the obligation to notify or not of any personal data breach, and the obligation or non-disclosure of any personal data breach of articles 32-34 GDPR, respectively, in the context of the obligation to observe the principle of accountability no. 5 par. 2 GDPR. At this meeting, during which A, Stefanos Topalis as attorney-at-law and Dimitrios Ganakis, Managing Director of the diagnostic center, appeared before the Authority, the Authority accepted the request to postpone examination of the case submitted by the attorney-at-law and legal adviser of the diagnostic center, Angelos Georgiadis, with (and with no. prot. APD C/EIS/1933/08.02.2022)) his application and set a new meeting date for 02.03.2022 at 10:00. During the new meeting, A and Stefanos Topalis appeared before the Authority as attorneys for the complainant (AM..), as well as Angelos Georgiadis, attorney for the diagnostic center (AM..), while B, Protection Officer, also attended. Data from the diagnostic center. on 08.02.2022 During this meeting, those present, after developing their views, were given a deadline for submitting written memoranda. Following this, the diagnostic center with its memorandum dated 17.03.2022 (under no. prot. APD C/EIS/4475/21.03.2022) argued, among other things, that: a) it exhausted every possibility 3 of recovering the disputed imaging examination , which was not possible to recover, b) according to medical science, the crucial document is the result of the imaging examination, which was given to the complainant, and not the imaging examinations as such, c) he has informed the complainant in writing in a timely manner of the lack of the availability of the imaging examination, d) in any case, the complainant has been informed fully and in detail in the context of

the filing by ... (with General Number ... and filing number of the petition ...) of her action against him before the Magistrate's Court [region] X, while e ) submitted his views on the issues of his compliance with the obligations of Articles 32-34 GDPR. Accordingly, A, with her memorandum dated 15.03.2022 (and with no. prot. APD C/EIS/4423/16.03.2022), argued, among other things, that in addition to the violation of the right of access in the failure to grant the requested imaging examination there was also a violation of the right to information, as she was never informed by the diagnostic center about the definitive loss of her availability. The Authority, after examining the elements of the file, after hearing the rapporteur and the clarifications from the assistant rapporteur, who was present without the right to vote, after a thorough discussion, DECIDED IN ACCORDANCE WITH THE LAW 1. Because, from the provisions of articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) and Article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise the implementation of the provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. In particular, from the provisions of articles 57 par.1 item. f of the GDPR and 13 par. 1 item g´ of Law 4624/2019 it follows that the Authority has the authority to deal with A's complaint against the diagnostic center, since the alleged violation of the right of access constitutes automated processing of personal data, subject to the regulatory scope of articles 2 paragraph 1 of the GDPR and 2 of Law 4624/2019. In addition, from the provisions of articles 57 par. 1 item a and h GDPR and 13 par. 1 item n. 4624/2019, it follows that Authority 4 has ex officio the authority to check, in the context of the alleged violation of the complainant's right of access, the compliance of the complained center with the obligations of Articles 32-34 GDPR, based on its obligation that follows from the principle of accountability of article 5 par. 2 GDPR. 2. Because article 15 of the GDPR stipulates regarding the subject's right of access: "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if this is the case, the right to access the personal data and the following information: (…) . 3. The controller shall provide a copy of the personal data being processed.(…)'. Subsequently, article 14 of Law 3418/2005 (Code of Medical Ethics) provides: "1. The doctor is obliged to keep a medical record, in electronic or non-electronic form, which contains data that is inextricably or causally linked to the illness or health of his patients. For the maintenance of this file and the processing of its data, the provisions of Law 2472/1997 (Government Gazette 50 A) are applied. Furthermore, paragraph 3 of the same article provides that: "Clinics and hospitals shall keep in their medical records the results of all clinical and paraclinical examinations." Furthermore, paragraph 4 of this article states: "The obligation to maintain medical records applies: a) in private

clinics and other primary health care units of the private sector, for a decade from the patient's last visit (…)". Finally, paragraph 8 of the same article provides that the patient has the right to access the medical records, as well as to receive copies of his file. 3. Taking into account the above, the Authority finds that the complained diagnostic center owed, by virtue of article 14 par. 4 item. a' Law 3418/2005, to keep the complainant's requested imaging examination for a decade, from her last visit to the diagnostic center, and was obliged to provide a copy, satisfying the complainant's right of access pursuant to Article 15 GDPR . The above is agreed 5 by the complained diagnostic center, as in the personal data protection policy provided (with document no. prot. 5068/02.08.2021) it is provided in point 7 entitled "data retention period" that: "The data of a personal nature are kept for as long as the relevant legislation determines, according to the more specific information provided separately for each category of subject. In particular for patients, the retention time for the personal data of patients/examined persons is 10 years, in accordance with the obligation imposed by the applicable legislation, unless legal actions are in progress, in which case the retention period is extended until the issuance of an irrevocable court decision. After their retention period, the Company ensures that personal data is destroyed in a secure manner." 4. Because, in the recent Guidelines 1/2022 of the European Data Protection Board (hereinafter KG 1/2022 ESPD) regarding the rights of data subjects – right of access it is explained that the right of access consists of three components: a) the confirmation on whether or not personal data is being processed, b) accessing it and c) providing information about the processing1. It is further clarified that a critical time for the evaluation of the assistance of the first aforementioned element (i.e. the processing of personal data) by the controller is the time of exercise of the right and its satisfaction presupposes the existence of the personal data (availability) at the time this2. Besides, it is emphasized in CG 1/2022 ESPD that there is no lifting of the obligation to satisfy the right of access, when the data controller intentionally deletes or modifies personal data during the exercise of the right of access3. 1 See Guidelines 1/2022 on data subject rights - Right of access of the EDPS from 18.01.2022 under public https://edpb.europa.eu/our-work- consultation, sc. tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en 2 CG 1/2022 ESPD, sc. 37: 3 CG 1/2022 ESPD 1/2022, sc. 39. available on the website 3, 6 5. Based on the foregoing considerations, the Authority finds, in this case, that no violation of complainant A's right of access can be established, in accordance with the provisions of Article 15 GDPR. And this, because at the time of exercising the right of access the disputed data of the imaging examination from ...01.2018 had become - even if illegally (according to the above, but also in violation of the provisions of articles 5 par. 1 letter

f) and 32 GDPR, as discussed below) – not available. Furthermore, it is established that the complained diagnostic center informed the complainant in its response to her request dated 08.02.2021 about the loss of availability of the requested imaging examination. For this reason, the belatedly submitted with the under no. prot. C/EIS/4423/16.03.2022 memorandum of the complainant alleging that the right to information was violated (pp. 1-2), for the reason that the diagnostic center failed to inform her of the (fruitless) attempts to recover the disputed imaging examination through IT companies and the result thereof, as well as – and regardless of the independent obligation of the diagnostic center for its compliance in particular with the obligation of Article 33 GDPR vis-à-vis the Authority – the provision of information to the complainant, in response to the access request, that the requested imaging examination is no longer available it was sufficient to inform her regarding, on the one hand, the loss of the data concerning her (pursuant to the provisions of article 12 par. 3 and 4 GDPR and recital 58 GDPR) and on the other hand to mitigate the risk and to undo the damage suffered by her loss, through the repetition of the imaging examination. Finally, the claim of the complained diagnostic center in its memorandum dated 17.03.2022 (pp. 3-4), citing medical science that a critical document which is medically necessary for any medical evaluation and is requested by doctors of all specialties to be evaluated is the conclusion of an imaging examination and not the imaging is rejected as unfounded, as beyond and regardless of the correctness of this 7 claim, a crucial element for the satisfaction of the right of access, as mentioned above, is the existence of the personal data at the time of exercising the right and not the purpose of using them4. 6. Because, subsequently, Article 5 of the GDPR defines the processing principles that govern the processing of personal data. Specifically, it is defined in paragraph 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity, transparency"), (...), f) 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, Article 32 GDPR regarding the security of processing provides: "1. Taking into account the latest developments, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of different probability of occurrence and severity for the rights and freedoms of natural persons, the controller and the executor the processing implement appropriate technical and organizational measures in order to ensure the appropriate level of security against risks, including, among others, where applicable: (…) c) the possibility of restoring the availability and access to personal data in a timely manner in the event of a natural or technical incident, d) procedure for the

regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of the processing (…). 2. 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 to personal data that 4 See CG 1/2022 ESPD, sc. 13, as well as the Authority's decisions 23/2020, 2/2020, 16/2017, 98/2014, 149/2014, 72/2013 and 71/2013, available on its website. 8 transmitted, stored or otherwise processed. (…) 4. The controller and the processor shall take measures to ensure that any natural person acting under the supervision of the controller or the processor who has access to personal data processes them only on his instructions controller, unless required to do so by Union or Member State law'. It follows from the above that one of the requirements of the GDPR is that, using appropriate technical and organizational measures, personal data is processed in a way that guarantees the appropriate security of personal data, including its protection from illegal destruction, loss and alteration. Accordingly, a key feature of any data security policy is to provide the ability, where possible, to prevent a breach and, if it does hopefully occur, to respond in a timely manner.7. Taking into account the above, from all the elements of the case file, the Authority finds that the complained diagnostic center, as the controller, processed (observed) the controversial imaging examination of the complainant, in violation of the required technical and organizational measures to ensuring its availability, in accordance with the requirements of articles 5 par. 1 item f and 32 GDPR, so that it is possible to satisfy the complainant's right of access to this data within the time period of its legal retention as stated above. In particular, in fulfillment of the obligation to take the appropriate technical and organizational measures regarding the maintenance of medical records (imaging examinations), the complained center should, in particular: a) store/keep the data in an external storage unit, in such a way that their availability is ensured for the period of time provided for in the provision of article 14 par. 4 item. a' of Law 3418/2005, b) receives sufficiently updated backup copies of the 9 performed imaging tests - personal data5, and c) periodically tests, evaluates and assesses the technical and organizational measures taken in a way that ensures availability in the over a period of ten years, so that it is possible to reprint or retrieve them. In this case, from the evidence in the case file, it emerged that the complained diagnostic center did cure the creative vacuum created by the use of the particular imaging machine, which provided the possibility of storing the files produced in it (images) for a period of time three (3) months, through the observance of imaging examinations on hard disk systems that were kept in the diagnostic center. The fact, however, that the chosen way of observing the imaging examinations made the data unavailable (temporarily and/or definitively) and for their recovery additional actions were required

on the part of the diagnostic center does not remove its obligation for the Article 32 GDPR taking the appropriate technical and organizational measures to ensure the availability of specific personal data (imaging tests) in accordance with the general principle of article 5 par. 1 item. in the GDPR. The above is indirectly acknowledged by the complained diagnostic center, as recognizing the above deficit in ensuring the availability of the imaging tests produced by the specific imaging machine, it installed in March 2019 a medical image management and storage system (PACS), which – according to its claims – is capable of maintaining a complete and retrievable history of examinations (imaging and findings) for the statutory period of ten (10) years. Furthermore, it emerged that the complained diagnostic center did not even keep back-up copies of the imaging tests in question stored on external hard drives, in order to ensure the availability of the imaging tests through them 5 Cf. Opinion 3/2014 of the Article 29 Working Group on with the http://ec.europa.eu/justice/article- notification 29/documentation/opinion-recommendation/files/2014/wp213_el.pdf , p. 7. personal data breach 10 and to be able to satisfy relevant access rights , as in the examined complaint 6. 8. The Authority, in relation to the established violation of articles 5 par. 1 item. f and 32 GDPR regarding the loss of the availability of the disputed imaging examination of the complainant, due to the non-observance of appropriate technical and organizational security measures in order to ensure the appropriate level of security on the part of the complained diagnostic center deems it necessary, based on the circumstances were established, to impose, pursuant to the provision of article 58 par. 2 sec. i GDPR, effective, proportionate and dissuasive administrative fine according to article 83 GDPR in accordance with the Guidelines "for the application and determination of administrative fines for the purposes of regulation 2016/679" of the working group of article 29. According to evaluation of the data, in order to choose the appropriate and corrective measure, the Authority takes into account that the specific violation concerned, in addition to the complainant, a significant number of people, i.e. approximately 15,445 people based on the no. C/EIS/2973/01.03.2022 notification of a personal data breach incident (article 83 par. 2 letter a), that the diagnostic center failed to carry out periodic checks on the effectiveness of technical and organizational security measures to ensure the security of processing (article 83 par. 2 letter b), that the complained diagnostic center had not obtained an appropriate level of security in accordance with the provisions of article 32 GDPR (article 83 par. 2 letter d), that the observance/loss of the imaging examinations concerned health data, i.e. it constitutes the processing of a special category of personal data of Article 9 GDPR (Article 83 par. 2 letter g), while it assesses as a mitigating circumstance the fact that the complained center nevertheless made efforts through IT companies to the recovery of imaging tests that had been stored on external disk systems in order to

mitigate the damage suffered by the affected subjects of data (article 83 par. 2 item c'). 6 See CG 1/2022 of the ESPD on the right of access, sc. 108. 11 9. Because, subsequently, in accordance with the provisions of article 4 item. 12 GDPR defines a personal data breach as "the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access of personal data transmitted, stored or otherwise processed". This definition is explained in terms of the concepts of "destruction-damage-loss" in the Guidelines of article 29 regarding the notification of personal data breaches pursuant to regulation 2016/679 as follows: "(...) It should be absolutely clear what means "destruction" of personal data: this is the case where the data no longer exists or no longer exists in a form that can be used by the controller. The term "damage" should also be relatively clear: this is the case where personal data has been changed, altered or is no longer complete. Regarding the "loss" of personal data, the term should be interpreted as a case where the data may still exist, but the controller has lost control or access to it, or is no longer in his possession. (…) » 7. 10. Because, in the complaint under review, the loss of the disputed imaging examination of the complainant constitutes illegal destruction, deterioration and loss of personal data or, otherwise, based on the principles of information security in accordance with Opinion 3/2014 of the article 29 on the notification of a personal data breach8 and Article 29 Guidelines on the notification of personal data breaches under Regulation 2016/6799, breach of availability. 7 WP250rev.01 from 03.10.2017, as finally revised and issued on 6 February 2018, available on the website http://ec.europa.eu/justice/data-protection/index_el.htm, page 7. 8 See aforementioned Opinion 03/2014 of the Article 29 working group on the notification of a personal data breach. 9 WP250rev.01 from 03.10.2017, as finally revised and issued on 6 February 2018, available on the website http://ec.europa.eu/justice/data-protection/index_el.htm 12 11. Because, article 33 para. 1 GDPR provides: "In the event of a personal data breach, the data controller shall notify the supervisory authority competent in accordance with Article 55, unless 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"10. Moreover, it is clarified in the Guidelines on the notification of personal data breaches under Regulation 2016/679 of the Article 29 Working Party: "The question may be raised as to whether a temporary loss of availability of personal data should be considered to constitute a breach and, if so, a breach that must be notified. In Article 32 of the GDPR ("Security processing") it is explained that, when implementing technical and organizational measures in order to ensure an appropriate level of security against risks, consideration should be given, inter alia, to the ability to ensure the confidentiality, integrity, availability and reliability of systems and of the processing services on a continuous basis and the

possibility of restoring the availability and access to personal data in a timely manner in the event of a physical or technical event. Therefore, a security incident resulting in the unavailability of personal data for a period of time is 10 The importance of being able to detect a breach in order to assess the risk to persons and then to disclose it, if required, is emphasized in recital 87 GDPR: "It should be ascertained whether all appropriate technological protection measures and organizational measures have been put in place for the immediate detection of any personal data breach and the immediate notification of the supervisory authority and the data subject. It should be established that the notification was made without undue delay, taking into account in particular the nature and seriousness of the personal data breach, as well as its consequences and adverse results for the data subject. Such disclosure may lead to intervention by the supervisory authority, in accordance with its duties and powers set out in this regulation." 13 also a type of violation, since the lack of access to data can have a significant impact on the rights and freedoms of natural persons. For the sake of clarity, it is stated that when personal data becomes unavailable due to scheduled system maintenance, this does not constitute a "breach of security" as defined in Article 4 point 12). As in the case of loss or destruction of personal data (or, indeed, any other type of breach), a breach involving a temporary loss of availability should be documented in accordance with Article 33(5). This helps the controller to demonstrate that it is accountable to the supervisory authority, which may request to see these records. However, depending on the circumstances of the breach, notification to the supervisory authority and notification of affected persons may or may not be required. The controller should assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the unavailability of personal data. According to Article 33, the controller should make a notification, unless the breach is not likely to cause a risk to the rights and freedoms of individuals. Of course, this should be evaluated on a case-by-case basis11". Next, it is emphasized that a data controller should be considered to acquire knowledge when said data controller has a reasonable degree of certainty that a security incident has occurred which has the effect of compromising personal data. In addition, it is explained that: "(...) the emphasis should be placed on taking timely action to investigate an incident, in order to establish whether personal data has been breached and, in such a case, to take corrective measures and make a notification, if required (…)" 12. 11 See WP250rev.01 from 03.10.2017, p. 9. 12 See WP250rev.01 from 03.10.2017, p. 12. 14 12. Because, in this case, the complained diagnostic center notified the personal data breach incident on 01.03.2022 (with prot. no. APD 2973/01.03.2022 ), in which it is stated that it became aware of the said incident of loss of availability on 28.09.2021. (loss of notification of availability) 13. Taking into account the above, the Authority finds that the reported diagnostic center with

the from 01.03.2022 (and with prot. no. 2973/01.03.2022) of the above personal data breach incident which has as as a result of the loss of the availability of the imaging examinations carried out on the specific imaging machine, in which the disputed imaging examination of the complainant took place, he performed a delayed/overdue fulfillment of the obligation of article 33 par. 1 GDPR. In particular, the claim of the complained diagnostic center that it became aware of the fact on 25.09.2021, when the control of the received file was completed by the second IT company to which it was contacted for the recovery of the data, is rejected as unfounded. And this is because, already at the time of the submission of the relevant request for granting the controversial imaging examination on 08.02.2021 by the complainant, its preparation for the satisfaction of the above request within the deadline set by the provision of article 12 par. 3 GDPR. and in any case, at the latest upon receipt of the no. prot. C/EXE/1496/15.06.2021 of the Authority's document, the complained diagnostic center had to evaluate, based on the data protection impact assessment, the possible risk for the persons concerned, in relation to the specific circumstances of the specific breach of loss of availability and make a relevant notification to the Authority13. For this reason it is rejected and there is no need to examine the claim of the complained diagnostic center that it came to his attention that the notification had not been submitted to the Authority on 28.09.2021 or 04.10.2021, by the then Director 13 WP250rev.01 from 03.10. 2017, p. 13. 15 Adviser to the accused, who eventually left the accused Centre. The above finding of the Authority is supported by the fact that even the temporary loss of availability, i.e. from the point of time when its loss was detected by the diagnostic center during the exercise of the complainant's right of access and the request to receive a copy of the imaging examination in question until of the time control point from the diagnostic center of the received file from the second recovery company and the confirmation of the definitive loss of the imaging tests, constitutes – according to the extrapolations – also a type of violation14, which should have been notified at that time to the Authority. 14. The Authority, in relation to the late/overdue fulfillment of the obligation to notify the above incident of personal data breach in violation of the time frame set by the provision of article 33 par. 1 GDPR, decided that there is a case to exercise the 58 par. 2 GDPR corrective powers. In particular, the Authority, taking into account in recital 148 GDPR the degree of responsibility of the diagnostic center due to the object of its activity, addresses a reprimand in accordance with article 58 par. 2 item. b' GDPR for late fulfillment of the obligation of article 33 GDPR. 15. Because, finally, Article 34 GDPR provides in paragraph 1: "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 breach of personal data to the data subject (…) 3. The notification to the data subject referred to in paragraph 1 is not required, if any of

the following conditions are met: a) the data controller has implemented appropriate technical and organizational protection measures, and these measures have been applied to affected by the breach of personal data, mainly measures that make personal data unintelligible to those who do not have permission to access it, such as 14 WP250rev.01 from 03.10.2017, p. 9. 16 encryption, b) the controller has subsequently taken measures to ensure that the high referred to in paragraph 1 is no longer likely to occur risk to the rights and freedoms of the data subjects, c) requires disproportionate efforts. In this case, a public announcement is made instead or there is a similar measure by which the data subjects are informed in an equally effective way (…)". In addition, OE 29 of article 29 in the Guidelines on the notification of personal data breaches under Regulation 2016/679, taking into account recital 86 of the GDPR underlines, among other things, that: "Controllers should remember that notification to the supervisory authority is mandatory, unless it is unlikely to create a risk to the rights and freedoms of persons as a result of the breach. In addition, when the rights and freedoms of individuals may be at high risk as a result of a breach, individuals must also be informed. The threshold for reporting a breach to persons is therefore higher than for notification to supervisory authorities and, consequently, not all breaches will require notification to persons, which protects them from unnecessary burden fatigue notifications. The GDPR states that notification of a breach to individuals should be made "immediately", that is, as soon as possible. The main objective of the notice to persons is to provide specific information about the actions they should take to protect themselves. As stated above, depending on the nature of the breach and the risk posed, timely notification will help individuals take action to protect themselves from any negative consequences of the breach"15. 16. In this case, the Authority finds that the risk to the rights and freedoms of the affected persons from the loss of availability 15 See WP250rev.01 from 03.10.2017, pp. 23-24. 17 of the images carried out on the specific imaging machine is high16, first of all because its spillover is the result of the failure to take the appropriate technical and organizational protection measures, which in particular due to the object of its activity and the justified trust that every client/patient expects from this should have been received and they could remove the relevant notification obligation (article 34 par. 3 letter a' GDPR). Secondly, because the complained diagnostic center made belated - as judged above - efforts towards the recovery of the imaging tests that had been stored on external disk systems, in order to mitigate the damage suffered by the affected data subjects (Article 34 par. 3 item b GDPR). And thirdly, because the complained center in no way invokes or proves that the communication with the affected persons (the total number of which is about 15,445 persons based on the notification No. Prot. C/EIS/2973/01.03.2022 and is able ) would entail disproportionate efforts on his part (article 34 par. 3 letter c) GDPR).

Further, the Complainant Diagnostic Center's claim that the risk to affected data subjects was not high is rejected because all patients whose imaging tests were included on the hard drive in question have already received their imaging images on DVD with the receipt of their results, therefore they have them and it is very rare that they are requested again, as this claim is in complete contradiction to the obligation to respect the results of clinical and paraclinical examinations, in accordance with the provisions of articles 14 par. 3 and 4 par. 1 Law 3418/2005, but also the data protection policy provided by the diagnostic center. For the same reason, moreover, the second reason put forward by the complained diagnostic center in support of the claim that the risk was not high, i.e. the detailed findings of all the imaging tests of the patients of the diagnostic center are available and easily retrievable, is also rejected. from 16 See WP250rev.01 from 03.10.2017, p. 40 example viii. 18 his staff, as compliance with the relevant findings does not remove or absorb the relevant obligation to comply with the imaging tests as stated above. In addition, the third ground in support of the claim that the risk was not high, i.e. that 3.5 years have passed since the most recent imaging tests included in the hard drive, and that on the one hand the patients who with the tests they were monitoring some identified problem, it is most likely that they have repeated the test, and on the other hand, the patients who underwent the tests as a precaution are covered by this finding, as it is simply the possibility that the patients who presented a history that justified the procedure imaging examination, they performed a repeat imaging examination is not sufficient to eliminate the high risk, nor does the complained diagnostic center submit data proving that out of the total number of 25,346 files to which the notified (with the prot. APD no. C/EIS/2973/01.03.2022 notification) incident of violation, a sufficient number of files - visualizations have been repeated, so that it can be documented that the occurrence of the high risk has been mitigated. Finally, the claim that there is no high risk is rejected, for the reason that no other patient has requested to receive the imaging tests, which were carried out between 16.03.2017 and 02.02.2018 in the last five years, as the claim this does not indicate/imply a mitigation of the high risk, which may however lead to physical harm, nor does it imply the removal of the obligation to observe it for a decade as stated above. On the contrary, the Authority finds, taking into account recitals 75 and 85 GDPR, that the nature of the specific data (imaging tests), their categorization as a special category of data (Article 9 GDPR) and the failure to observe appropriate technical and organizational protection measures of the data, in particular due to the object of the activity of the complained center and the justified trust that every customer - patient expects from it, constitute sufficient evidence for the assessment that the violation of their availability may bring about a high risk to the rights and freedoms that 19 to result in physical as well as moral damage, in order to justify the obligation to notify the affected data

subjects of the data breach according to Article 34 GDPR. Furthermore, for the above reasons, it was incorrect and illegal for the diagnostic center to choose not to notify the affected data subjects in accordance with Article 34 of the GDPR. 17. The Authority, in relation to the established violation of the notification obligation on the part of the diagnostic center, as data controller, to the affected data subjects of the violation of the availability of the imaging tests that were stored on a hard disk in violation of Article 34 GDPR, decided that there is a case to exercise its corrective powers under article 58 paragraph 2 GDPR. In particular, the Authority, taking into account in recital 148 GDPR the degree of responsibility of the diagnostic center due to the object of its activity, as well as the fact that the attempts to recover the disputed imaging tests after the assistance of the two IT companies were mostly unsuccessful Akarpes gives an order, according to article 58 par. 2 item. e' GDPR, in the diagnostic center, as controller, to announce the breach of personal data (availability of the imaging tests held in the diagnostic center) to the affected data subjects, in order to be evaluated by the affected persons (customers - patients) the need to repeat missed imaging tests. FOR THESE REASONS, the Authority a) rejects as unfounded the complaint of A against the diagnostic center PRIVATE POLYTRY AND DIAGNOSTIC CENTER PYLIS AXIOU I.A.E., as data controller, regarding the violation of the right of access for the reasons that are thoroughly set forth in paragraphs 3-5 hereof, 20 b) finds that the loss of availability of the disputed imaging examination of A constitutes a violation of the principle of article 5 par. 1 item. f GDPR, due to the failure to take appropriate technical organizational measures in order to ensure the appropriate level of security according to article 32 GDPR and imposes an administrative fine of thirty thousand on the PRIVATE POLYSTERY AND DIAGNOSTIC CENTER PYLIS AXIOU I.A.E., as controller (30,000) euros for this violation, for the reasons that are thoroughly analyzed in paragraphs 7-

8 hereof, c) finds that the notification of a personal data breach to the Authority was made late/overdue in violation of Article 33 GDPR and issues a reprimand in accordance with Article 58 para. 2 item. b' GDPR at the PRIVATE POLYCLINIC AND DIAGNOSTIC CENTER PYLIS AXIOU I.A.E., as controller, for the reasons that are thoroughly analyzed in paragraphs 11-14 of this present and d) gives an order, pursuant to article 58 par. 2 item e GDPR, to the PRIVATE POLYSTERY AND DIAGNOSTIC CENTER PYLIS AXIOU I.A.E., as data controller, to announce the breach of personal data to the affected data subjects, in accordance with the provisions of article 34 GDPR, for the reasons that are thoroughly are analyzed in its paragraphs 15-17present.

The Deputy President

George Batzalexis

The Secretary

Irini Papageorgopoulou

21