DECISION 54/2022 Athens, 03-10-2022 Prot. No.: 2439 The Personal Data Protection Authority met, at the invitation of its President, in an extraordinary meeting via video conference on 21-

7-2022, following the postponement of its meeting from 19-7-2022 and following its meeting from 14-06-2022, in order to examine the case referred to in the history of the present. Konstantinos Menudakos, President of the Authority, the regular members Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur, Christos Kalloniatis, Aikaterini Iliadou and Grigorios Tsolias, as well as the alternate member Nikolaos Livos in place of regular member Charalambos Anthopoulos who, although invited, were present legally and in writing, he did not attend due to a disability. At the meeting, without the right to vote, the auditor Konstantinos Limniotis, IT specialist, as assistant rapporteur, and Irini Papageorgopoulou, an employee of the Department of Administrative Affairs, as secretary, attended the meeting, by order of the President. The Authority took into account the following: Following relevant complaints against the National Bank of Greece S.A. (hereinafter National Bank) and Piraeus Bank SA. (hereinafter Piraeus Bank), the Authority examined the issue of personal data processing through contactless debit/credit card transactions. The complaints in question concerned the mandatory replacement of debit/credit cards with new ones, which by default had the possibility of contactless transactions. The Authority, after examining the security issues of said processing as well as the related risks, and taking into account the international, during the disputed period, specifications regarding contactless debit and/or credit 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr cards based on the relevant information provided by the Mastercard and Visa companies, issued Decision No. 48/2018, with which it addressed a recommendation1 to the due to Banks, if a customer declares to them that he does not wish to have a card with the possibility of carrying out contactless transactions, either to provide the possibility of deactivating the contactless operation of such a card or to grant a new card without the possibility of contactless transactions. Further, in the context of examining the above complaints, the Authority found that in some cases of credit/debit cards, a history of recent transactions carried out using the card is kept on the chip of the card, which can also be easily read without contact. In particular, the said information related to the transaction history consists of the date of the transaction and the amount of money. For the feature in question found on Mastercard cards, the company in question informed the Authority that it is not a mandatory feature and it is up to the respective issuer whether or not to incorporate it into the corresponding banking product (credit/debit card) that it provides to the his client. Regarding this issue, which the Authority examined ex officio, the Authority, with the above Decision, addressed the following recommendation2 to the Banks in question. If a card issued to a

customer has the option of keeping a transaction history on its chip activated without having given his specific consent, the customer should be informed in any appropriate way (e.g. via e-mail, through a message when logging in to personalized electronic services of the data controller, through a postal letter, etc.) regarding this processing, giving him the possibility to stop this processing. Furthermore, in each new edition/grant, the feature in question should be deactivated from the beginning, and only be activated if there is a special 1 According to article 19 paragraph c' of Law 2472/1997 which was in force during the disputed period 2 In accordance with article 19 par. c of Law 2472/1997 which was in force during the disputed period 2 consent of the customer, as long as he has been previously informed about this processing. Subsequently, the Authority, with document no. prot. C/EX/6257/16-07-2018, forwarded the above Decision to all Greek Banks (with notification to both mentioned above), pointing out that, although the complaints submitted to the Authority and examined in the context of the above-mentioned Decision concerned two specific Banking Institutions, they should proportionally - to the extent that each Bank provides its customers with cards of the technology in question - take care to fulfill all that is perceived in said Decision. After all, the Authority had previously addressed all the Banks, with its letter No. C/Eξ/4943/27-06-2017, requesting, among other things, information as to whether they provided contactless debit/credit cards and with what characteristics (such as what information is stored on their chip). In this document, as also mentioned in Decision 48/2018, ALFA BANK SA. (hereinafter Alpha Bank) and EUROBANK ERGASIAS SA. (hereinafter Eurobank) had not responded to the Authority, while they also did not respond even after the relevant reminder documents with no. prot. C/EX/276/12-01-2018 and C/EX/275/12-01-2018 respectively. Subsequently, the Authority sent to National Bank, Piraeus Bank, ALFA Bank and Eurobank the document No. C/EX/4271/14-06-2019, with which it requested the said Banks to inform as to the actions they took in order to comply with the aforementioned recommendations of the Authority mentioned in Decision No. 48/2018. Piraeus Bank responded with the letter number C/EIS/5193/24-07-2019 document, stating the following: 1) If a customer states that he does not wish to have a contactless card, the Bank satisfies the relevant request given that it has completed all the relevant technical implementations required. 2) With regard to keeping the history of the latest transactions on the card chip, the Bank informed that a project was already underway to disable the relevant information for all the banking products it provides. This deactivation will apply to all new cards, regardless of the reason for their issue (loss, damage, etc.). 3) During the period in which the Bank's answer in question was submitted to the Authority, the latter informed that it had decided not to provide its customers with the possibility of maintaining the history

and that this particular possibility would be re-evaluated at a later time. Subsequently, the Authority, and given that there was a relevant document request from A (Authority's original no.: Γ/ΕΙΣ/6348/01-10-2021) who had submitted a relevant complaint to the Authority regarding the mandatory replacement of debit/credit cards with new contactless cards - to be informed whether the Banks have complied with the provisions contained in Decision No. 48/2018 of the Authority regarding the part of informing cardholders about keeping a history of transactions on this chip, pointing out that he himself did not receive such information, he sent to Piraeus Bank the document No. C/EXE/2602/15-11-2021, with which he asked the Bank to specifically clarify the actions it took regarding the issue of maintaining the history of the last transactions on the credit/debit card chip (for those cards that had the feature in question), clarifying in particular whether it has duly informed all holders of the above cards of the said processing, regardless of whether, in the meantime, their cards have already been replaced due to the expiration of the older ones. Piraeus Bank responded with document No. C/EIS/184/11-01-2022, stating the following: 1) The Bank initiated a project to deactivate the relevant information for all card products it provides, the which was gradually implemented for each product from the beginning of 2019 and was completed in its entirety at the end of the same year. Based on this, all new card releases regardless of the reason for issue (new card, loss, wear, renewal), which are issued from the date the relevant implementation for each product went into production, 4 have the said feature disabled as of today 65% of the card portfolio does not have the relevant information active. 2) The Bank has taken the necessary measures and launched all the required actions, in order to complete the gradual replacement of all cards – already a very large percentage has been done – and therefore to achieve the full circulation of cards, which will have the transaction history feature disabled. 3) There is no risk related to the personal data of customers, as the details of such a card (date, amount) do not lead to the identification of a natural person and, therefore, do not fall under the concept of personal data, while for the identification must have been preceded by illegal use of the card (e.g. theft of the card), combined with special knowledge or use of special technology. Therefore, these are data which, according to the Bank's claims, cannot be easily retrieved - even the owner himself cannot retrieve the relevant information - and therefore there is no risk to the rights and freedoms of the customers , nor does any leakage or breach of personal data occur. 4) With regard to the activation of the feature that consists in maintaining the history of transactions, at the request of the customers, the Bank, evaluating the data, decided not to provide its customers with this particular possibility. 5) In addition, Piraeus Bank, since it replaces the plastic cards of its cards with new ones, in which the maintenance of the history of transactions is deactivated and has decided not to provide customers with the possibility of

activating the maintenance of the said information, has not carried out and neither does it intend to inform its customers about it. As it states in its above document, the 5 relevant information of its customers would be equivalent not only to huge costs (both for carrying out the information, as well as for managing the issues that follow the information, such as monitoring information, responding to requests that related to information etc.), but it could damage the Bank's credibility and would cause unnecessary worry, concerns and distress to customers, given that there is no apparent risk to personal data, rights and freedoms in any way of customers. Subsequently, the Authority invited Piraeus Bank to a hearing, via video conference, at the Plenary meeting of 14-06-2022 (see call with prot. no. C/EXE/1336/02-06-2022). During the meeting of 06-14-2022, Ms. B, Director ..., Ms. C... Manager and Mr. D, Data Protection Officer, as representatives of Piraeus Bank. After the meeting, the data controller was given a deadline to submit a memorandum, which he submitted, within the set deadline, with document No. C/EIS/8665/08-07-2022. The following are mentioned in the memorandum in question: a) Piraeus Bank is in full compliance with all the provisions in point (a) of Opinion 9 of Decision 48/2018 of the Authority and has taken all the required systemic and operational actions so that, when the customers declare that they do not wish to have in their possession cards with contactless operation, Piraeus Bank shall proceed to deactivate the contactless operation of the cards in question, immediately, fully and without exception satisfying the relevant requests of the customers. In particular, after the issuance of the above Decision, Piraeus Bank immediately and effectively started the work of deactivating the cards, as long as relevant requests are submitted by customers, created the necessary infrastructure, made all appropriate adjustments and completed the required technical implementation for the all of its products in order to be fully harmonized with the Authority's requirements. In this context, as early as March 2019, Piraeus Bank, as soon as it receives requests for contactless functionality from 6 customers, with which the customers declare that they do not wish to have a card that supports contactless transactions or request the deactivation of contactless functionality , the Bank immediately satisfies the requests in question and deactivates contactless operation. Furthermore, the Bank, always having as its primary concern the support and service of its customers and the provision of full and transparent information on all issues concerning them, proceeds to inform its customers about the above possibility of submitting a request for deactivation contactless operation, through all service channels and specifically through the Bank's Branch Network, Winbank and the 24-hour Telephone Service. In fact, it notes that although from a business point of view it was expected that the percentage of its portfolio that would submit corresponding requests would be significantly small, nevertheless a strategic decision was made to complete the project in order to provide

the possibility of disabling contactless functionality, potentially at 100% of its portfolio. In continuation of the above and as an alternative, the Bank points out that today only 0.2% of its customers have chosen to make use of the above possibility. b) In continuation of the points contained in point (b) of Opinion 9 of Decision 48/2018 of the Authority, regarding the observance and transmission of the history of transactions on the chip of its cards, the Bank states that, on the one hand, analyzing the data in force for each scheme and taking into account that the maintenance and transmission of the transaction history concerns only Mastercard cards and not Visa cards and on the other hand taking into account the dispersion of its card portfolio between the two schemes (today the percentage of Mastercard cards amounts to 28% of all its cards), in view of its compliance with the above Decision and in order to shield its entire portfolio, it took a strategic decision concerning its entire portfolio. In particular, the Bank decided to start at the end of 2018 and prepare a project, which would be universal for all the card products it provides (46 in number), which provided for the deactivation of the relevant information from the cards' Chip. The project was implemented in stages 7 for each product from the beginning of 2019 and was completed in its entirety at the end of the same year. Based on this, all new card issues regardless of the reason for issue (new card, loss, wear, renewal), which are issued from the date the relevant implementation was brought into production for each product, have the said feature disabled and now 74 % of the product portfolio of its cards, does not carry the information in question. Furthermore, the Bank has taken all the necessary measures and initiated all the required actions, so that within a reasonable period of time the feature of maintaining the transaction history on the Chip of its cards will be deactivated for its entire portfolio in circulation, while already , as mentioned above, the above has already been achieved at a particularly high rate. In addition, the Bank points out that there is no risk related to the personal data of customers, as the details of the transactions kept and transmitted (date and amount) do not lead to the identification of a natural person and therefore do not fall under the concept of personal data data, while for identification there must have been previous illegal use of the card (e.g. theft of the card), combined with special knowledge or use of special technology. Therefore it is information, which cannot be easily extracted - even the owner himself cannot extract the relevant information - and therefore there is no risk to the rights and freedoms of the customers, nor any leakage or breach occurs personal data. The Bank also notes that the transactions recorded on Mastercard cards are the last ten (10) in number and not all are included, as electronic transactions - which as a result of the special conditions created due to COVID-19, make up a large percentage of them - are not recorded. Therefore, since the Bank replaces its plastic cards with new ones, in which the keeping of the transaction history is disabled and has decided not to provide its customers with the

possibility to activate it, 8 it did not inform the customers. Furthermore, the Bank states that such an update could damage the Bank's credibility, cause unwarranted concern in the market, confusion, concern and distress to customers, all the more so when the keeping and transmission of the data concerns only Mastercard holders cards and does not result in any leakage or violation of customers' personal data. In addition, the updating of the entire portfolio would create huge costs, both due to the action itself, and due to the issues that follow the update (monitoring of the update, responding to requests related to the update, etc.) The Authority, after after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteur, who (assistant) was present without the right to vote, after a thorough discussion DECIDED IN ACCORDANCE WITH THE LAW 1. In accordance with the provisions of articles 51 and 55 of the General Regulations Data Protection (EE) 2016/679 (hereinafter, GDPR) and Article 9 of Law 4624/2019 (Government Gazette A

137), 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. 2. According to article 4 par. 1 of the GDPR, personal data means "any information concerning an identified or identifiable natural person ("data subject")", while "the identifiable natural person person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors specific to the physical, physiological , genetic, psychological, economic, cultural or social identity of the natural person in question". And in introductory paragraph 26 of GDPR 9 it is stated that "in order to judge whether a natural person is identifiable, all the means that are reasonably likely to be used, such as for example separating him, should be taken into account, either by the person responsible processing either by a third party for the direct or indirect verification of the identity of the natural person. In order to determine whether any means is reasonably likely to be used to verify the identity of the natural person, all objective factors, such as the cost and time required for identification, should be taken into account, taking into account the technology that is available at the time of processing and technological developments". 3. According to article 4 par. 7 of the GDPR, a data controller is defined as "the natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and manner of personal data processing; when the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State". 4. According to article 5 paragraph 3 of the GDPR the data controller

bears the responsibility and must be able to prove his compliance with the processing principles established in paragraph 1 of the same article, which include legality, objectivity and transparency of processing in accordance with article 5 par. 1 item a' - i.e. the data must be processed lawfully and legitimately in a transparent manner in relation to the data subject. In other words, with the GDPR, a compliance model was adopted with the central pillar being the principle of accountability in question, i.e. the controller is obliged to design, implement and generally take the necessary measures and policies, in order for the data processing to be in accordance with the relevant legislative provisions and, in addition, he must prove himself and at all times his compliance with the principles of article 5 par. 1 of the GDPR. 5. Furthermore, Article 6 para. 1 of the GDPR provides, among other things, that the processing is lawful only if and as long as at least one of the 10 following conditions (legal bases of the processing) applies: "a) the data subject has consented to the processing of his personal data for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a party or to take measures at the request of the data subject prior to the conclusion of a contract , (...) f) the processing is necessary for the purposes of the legal interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that require protection of personal data (...)". 6. With reference to the principle of processing transparency, the GDPR imposes specific obligations on data controllers regarding the information they must provide to data subjects. In particular, in accordance with article 12 par. 1 of the GDPR, the data controller takes the appropriate measures to provide the data subject with any information referred to in articles 13 and 14 (which concern the information provided to the data subjects or the data is collected from the subjects themselves or not) and any communication under Articles 15 to 22 (which concern the rights of data subjects to object3 to data processing, including Article 21 processing) regarding the processing in a concise, transparent, comprehensible and easily accessible format. Furthermore, paragraph 2 of Article 12 of the GDPR provides that "the data controller shall facilitate the exercise of the rights of the data subjects (…)". of the right 3 According to Article 21 of the GDPR, "The data subject has the right to object, at any time and for reasons related to his particular situation, to the processing of personal data concerning him, which is based on Article 6 paragraph 1 point e) or f), including profiling based on those provisions. The controller no longer processes the personal data, unless the controller demonstrates compelling and legitimate reasons for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or support of legal claims claims". 11 7. In particular, in article 13 of the GDPR it is defined that "when personal data concerning a data subject is collected from the data subject, the

data controller, upon receiving the personal data, provides the data subject with all of the following information: a) the identity and contact details of the controller and, where applicable, the representative of the controller, (…) c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing , (…)" (see par. 1 of article 13 of the GDPR). 8. In this particular case, for the processing which consists in storing, on the Piraeus Bank debit/credit card chip, the history of the last ten (10) transactions carried out through it, which can be read intact, the said The Bank is the controller, in the sense of article 4 par. 7 of the GDPR. Indeed, as emerged from the initial examination of the said case with the Authority's Decision No. 48/2018, the said technological feature is provided as an optional option on cards by the Mastercard company - i.e. it is left to each issuer ("Bank") whether to activate it or not. Besides, Piraeus Bank actually started, as described in the present history, issuing cards without this technological feature, for which it further decided that it will not provide it even as an optional option, upon customer request. 9. For the processing in question, Piraeus Bank did not provide relevant information to the data subjects (i.e. to the holders of the cards in question). It should be pointed out that the Authority, already with Decision No. 48/2018 (which was based on the legal framework in force before the GDPR), identified the said deficiency and sent a recommendation to the data controller in order to remedy it – that is, it adopted the milder possible choice. 10. In the absence of the relevant information, which in any case is an obligation of the controller according to the above, the legal basis of said processing is not clear. Such processing could in principle 12 have as its legal basis consent4 (article 6 par. 1 letter a' of the GDPR), as long as the data subjects declare freely, in full knowledge and clearly (with a statement or a clear positive action) that they specifically and explicitly consent to the processing in question, but these conditions do not apply in this case. Also, the processing in question cannot be considered as necessary for the performance of a contract - and, therefore, the legal basis cannot be that of article 6 par. 1 item. b' of the GDPR - since there are, after all, a number of corresponding debit/credit/prepaid cards without the feature in question, which, moreover, as mentioned above, is implemented on an optional basis. Therefore, the only possible legal basis seems to be that of article 6 par. 1 item. at. And in this case, however, apart from the fact that the Bank has not documented what is the legal interest it seeks by storing this data on its customers' cards, it is required on the one hand that the processing be transparent, but this condition was not met for the specific case, and on the other hand that the data subjects know in particular about the existence of the right to object to the processing in question (Article 21 of the GDPR), while this condition does not apply in the case in question either. Regarding this issue, the Authority, with the recommendation it addressed with no. 48/2018 Decision, requested the Bank, in addition to

informing the data subjects, to give the possibility, to those of them who wish to do so, to express their opposition to the processing in question and, subsequently, to take care of the satisfaction of the right (either by disabling the specific technological feature or by issuing a new card). 11. Piraeus Bank, although it initiated procedures based on which every new card it issues does not carry the said characteristic and therefore, gradually stops said processing, it did not inform the card holders about this processing, therefore not complying with the above Decision of 4 See the definition of consent in article 4 para. 11 of the GDPR, as "any indication of will, free, specific, explicit and in full knowledge, by which the data subject expresses that he agrees, by statement or by a clear positive action, to be the subject of processing of the personal data concerning him ». 13 Authority. Therefore, there is a violation of article 13 of the GDPR which entails a violation of the article 5 par. 1 item. a' of the GDPR principle of transparency of processing. The arguments put forward by the Bank for the reasons for not informing are that, according to its claims, the costs would be high and it would cause disruption to its customers and damage to its reputation, without any substantial risk to said customers. , as the data kept regarding the last transactions carried out with the card (date, amount) do not lead to the identification of a natural person and therefore do not fall under the concept of personal data, while for identification there must have been previous illegal use of the card (e.g. theft of the card), combined with special knowledge or use of special technology. However, these claims are unfounded for the following reasons: a) The obligation to inform about the processing and more generally the fundamental principle of the transparency of the processing exists regardless of whether or not there is a risk from the processing for the data subjects5. b) Even if there is no high risk from the processing in question for the affected persons, the claim that there is essentially no risk is not sufficiently substantiated for the following reasons: i) The equipment required to read the data is readily available to anyone. Specifically, as already described in Decision No. 48/2018 of the Authority, any "smart" device (e.g. "smart" mobile phone) with appropriate software (which is freely available) is sufficient in order to read the data. ii) There is clearly a possibility - and even an easy one - to associate the data in question with the subject thereof. In fact, this possibility does not necessarily require a stolen/lost card. For 5 Restrictions on rights can be imposed by EU law or the law of a Member State under certain conditions and if appropriate safeguards are provided for, but this particular case clearly does not fall under them (see Article 23 GDPR). 14 of the third example, a close family/friend/professional environment of the data subject can, if found near the said card of the data subject, read the said data intact. In any case, the card itself mentions the name of its owner on its front side. Therefore, and taking into account Article 26 of the GDPR, the data in question clearly constitute personal data and are not anonymous

information, as the Bank incorrectly claims. c) The claim about the high cost required for the update is not substantiated. Already the Authority, with Decision No. 48/2018, had mentioned as indicative ways of information the sending of an email message or the posting of a message when connecting users to personalized electronic services of the Bank. Furthermore, the claim that such an update would entail a large number of card replacement requests cannot lead the controller to the conclusion that he is exempt from the obligation to update because the management of the requests and their monitoring, if they are indeed excessive in number, could lead to in appropriate procedures for their satisfaction. For example, it could possibly be judged that this replacement would not take place immediately, also taking into account the not particularly high risks of said processing. In any case, the obligation to inform which falls on the data controller is not removed in principle from its cost, since in this particular case, in terms of the obligation to inform, article 13 of the GDPR6, 6 Even if it had been applied Article 14 of the GDPR, as referred to in Article 14 para. 5 of the GDPR regarding information provided to data subjects if the personal data has not been collected from the data subject, "paragraphs 1 to 4 shall not apply if and if: a) the data subject already possesses the information, b) the provision of such information proves impossible or would involve a disproportionate effort, in particular with regard to processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, under the conditions and guarantees referred to in article 89 paragraph 1 or if the obligation referred to in paragraph 1 of this article is likely to make it impossible or to 15 which does not provide for any exception for the controller from the obligation to inform the data subjects . 12. The Bank additionally states that such information would cause concern to its customers and damage to its reputation. And with regard to this claim, however, the provisions contained in the above Opinion 11 regarding the non-exemption from the obligation to inform apply in principle. Furthermore, this claim is not sufficiently substantiated. This is because precisely because the risks from the processing are not high, it does not follow that a properly worded information about this processing would cause concern. However, it does not appear that the Bank thoroughly examined appropriate information texts in order to reach the above conclusion. 13. Based on the above, the Authority considers that there is a case to exercise its corrective powers according to article 58 par. 2 of the GDPR in relation to the violations found. 14. The Authority further considers that, based on the circumstances established, it should be imposed, pursuant to the provision of article 58 par. 2 sub. i of the GDPR, an effective, proportionate and dissuasive administrative fine according to article 83 of the GDPR both to restore compliance and to punish illegal behavior. Furthermore, the Authority took into account the criteria for measuring the fine defined in article 83 par. 2 of the GDPR and Guidelines

4/20227 of the European Data Protection Board (which are in public consultation) and in particular that: a. the established violation of article 13 of the GDPR is subject, in accordance with the provisions of article 83 par. 5 sec. b' GDPR, in the higher prescribed category of the classification system to a large extent harm the achievement of the purposes of said processing. In these cases, the data controller shall take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject, including by making the information publicly available." 7

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022- calculation-administrative_en

16 administrative fines8, b. the violation in question constitutes non-compliance by the data controller with Decision No. 48/2018 of the Authority, c. the violation concerns a large number of data subjects – specifically, all Piraeus Bank customers who had debited the old version Mastercard credit card, d. the violation is continuous, since it was already established by the Authority's Decision No. 48/2018 and continues to this day, e. the activity was wide-ranging, as it concerns every "movement" of a Mastercard debit/credit card (issued by the Bank) in a physical store, regardless of the geographical location of this or type of transaction, as long as it is an old-issue card that has not been replaced, f. the activity is related to the main activities of the data controller, regardless of the fact that the data in question held on the card chip, and which are already being legally processed, in a different context, by the Bank (since it is held in its systems information regarding the movement of the card), it does not appear that they were used by the Bank. g. the processing concerns data of an economic nature, for which there is a risk, in accordance with what is mentioned in the rationale of this present, of coming to the knowledge of third parties, h. the violation was intentional, since the Authority had already addressed with letter no. . 48/2018 Decision regarding recommendation to the Bank and the latter took a strategic decision not to

8 "More important" violations are characterized as those that may result in

maximum possible fine of 20,000,000 euros or, in the case of businesses, up to 4% of

of total worldwide annual turnover of the previous financial year, in

contrary to the other violations included in article 83 par. 4 of the same article

to comply with that recommendation but, instead, to start

gradually stopping said processing,

i. the information available on the internet9 about its financial income

Bank for 2021,

and also that:

a. This processing does not result in financial loss for the

data subjects,

b. the Bank would not obtain any financial benefit from the

due processing,

c. the Bank took actions for the gradual discontinuation of the aforementioned

processing.

15. Based on the above, the Authority unanimously decides that it should be imposed on

reported controller referred to in the ordinance

administrative sanctions, which are judged to be proportional to the severity of the

violations.

FOR THOSE REASONS

The beginning,

It imposes on Piraeus Bank S.A., as controller, the

effective, proportionate and dissuasive administrative fine which

appropriate in the specific case according to the special circumstances

thereof, in the amount of twenty thousand euros (20,000.00) euros, for the above established

violation of article 13 of Regulation (EU) 2016/679, according to article 58

para. 2 i' of the GDPR in combination with article 83 para. 5 of the GDPR.

9 See https://www.piraeusholdings.gr/~/media/Com/2021/Files/investor-

relations/Financials/Financial-Statements/2021/12M/2021-Annual-Financial-Report_Holdco_gr.pdf

(last access: 19/8/2022)

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou

19

20